Universidade de Brasília

Instituto de Relações Internacionais (IREL)

Programa de Pós-Graduação em Relações Internacionais (PPGRI)

Eduardo Arthur Izycki

CYBER OFFENSIVE CAPABILITIES: A GLIMPSE ON A MULTIPOLAR DIMENSION

Brasília

2021

EDUARDO ARTHUR IZYCKI

CYBER OFFENSIVE CAPABILITIES: A GLIMPSE ON A MULTIPOLAR DIMENSION

Dissertação apresentada no âmbito do Programa de Pós-Graduação em Relações Internacionais (PPGRI) do Instituto de Relações Internacionais (IREL) da Universidade de Brasília (UnB) como requisito parcial para a obtenção do título de Mestre em Relações Internacionais.

Área de Concentração: Política Internacional e Comparada

Orientador: Prof. Dr. Antonio Jorge Ramalho da Rocha

Brasília

2021

Eduardo Arthur Izycki

Cyber Offensive Capabilities: a Glimpse on a Multipolar Dimension

Dissertação apresentada no âmbito do Programa de Pós-Graduação em Relações Internacionais da Universidade de Brasília (UnB), como requisito parcial para a obtenção do título de Mestre em Relações Internacionais.

Área de concentração: Política Internacional e Comparada.

COMISSÃO EXAMINADORA

_____

Prof. Dr. Antônio Jorge Ramalho da Rocha
Instituto de Relações Internacionais – UnB
Orientador

_____

Prof. Dr. Alcides Costa Vaz
Instituto de Relações Internacionais – UnB
Membro

_____

Prof. Dr. Eduardo Wallier Vianna
Programa de Pós-Graduação em Ciência da Informação – UnB
Membro

_____

Prof. Dr. Juliano da Silva Cortinhas
Instituto de Relações Internacionais – UnB
Suplente

Para minha família.

RESUMO

Um dos aspectos mais notáveis no Século 21 é a adoção da tecnologia da informação em múltiplos aspectos do cotidiano de indivíduos, da sociedade e de estados nacionais. A crescente interconectividade irá se ampliar exponencialmente nos próximos anos com a adoção de redes 5G, a internet das coisas, grandes volumes de dados (Big Data) e o uso de aprendizado de máquina. Como consequência, atividades econômicas e a vida concreta estarão ainda mais expostas a ameaças cibernéticas ofensivas. Se comparado a outras dimensões como terra, ar, mar e espaço, o espaço cibernético tem características únicas, pois pode ser modificado por cliques e configurações - oceanos e montanhas são mais difíceis de se mover. Além disso, o relativo anonimato, a irrelevância de distâncias geográficas, o baixo custo de aquisição e desenvolvimento de artefatos ofensivos e a possível negação de atribuição tornaram essa dimensão em um novo teatro-de-operações para os estados. Ao contrário de estudos pregressos que focaram em análises orientadas ao pior cenário possível, o presente estudo pretende apresentar uma análise empírica dos conflitos cibernéticos. Para tanto, um algoritmo de coleta e processamento de dados empíricos foi elaborado para testar as hipóteses deste estudo. Como resultado, foram identificados 29 países que realizaram ações cibernéticas ofensivas, além de 85 países que adquiriram capacidades cibernéticas ofensivas de provedores privados. Os montantes desafiam a tradicional percepção de que apenas alguns atores teriam essa capacidade ofensiva. Isso indica que o espaço cibernético, como um teatro de operações, favorece a difusão de poder entre estados nacionais. A maioria das ações ofensivas correspondem a instrumentos tradicionais como espionagem, vigilância e desinformação, potencializados pelas características peculiares do espaço cibernético. Nesse sentido, as capacidades cibernéticas ofensivas oferecem alternativas para a competição entre os estados abaixo do uso da força. Com isso, atores estatais têm alcançado resultados estratégicos que influenciam o equilíbrio de poder relativo sem que seja necessário se expor ao risco de respostas militares convencionais ou nucleares de seus oponentes.

Palavras-chave: Espaço cibernético; conflitos cibernéticos; capacidades cibernéticas ofensivas; patrocínio estatal; guerra cibernética.

ABSTRACT

One of the most striking features of the 21st century is the widespread adoption of information technology in every aspect of the modern life of individuals, society, or nation-states. The growing interconnectivity will increase exponentially in the years to come with the adoption of new 5G networks, the internet of things (IoT), large volumes of information (Big Data), and the use of machine learning (artificial intelligence). As a result, economic activity and ordinary life will be even more exposed to the threat of cyber offensive actions. When compared to land, sea, air, and space, cyberspace has unique features. Its “geography” is easily modified, oceans and mountains are hard to be changed, but entire cyberspace regions can be turned on or off with a button click. Additional features such as the relative anonymity, the irrelevance of geographical distances for some processes and purposes, the low cost of acquiring or developing offensive capabilities, and the plausible deniability of actions have turned this dimension into a theater of operations for nation-states. Many scholars focus their analysis on the worst-case scenario where cyber offensive actions will revolutionize war, but fail to provide enough evidence to support it. This research intends to provide empirical analysis regarding cyber conflict. For that purpose, an algorithm to collect and process the empirical data was built and used to examine hypotheses. As a result, this research gathered evidence of 29 different countries engaging in cyber offensive actions and 85 nations acquiring cyber offensive technologies from private vendors. The numbers challenge the average perception of concentration of cyber capabilities in a few "traditional" actors. This entails that cyberspace, as an operational theatre, favors the diffusion of power among nation-states. The majority of the cyber offensive actions are a variation of traditional instruments of statecraft such as surveillance, espionage, and disinformation, potentialized by cyberspace's peculiar characteristics. In this sense, cyber offensive capabilities are providing alternatives for the bargaining and interactions to nation-states below the threshold of the use of force. Actors are able to achieve strategic outcomes and influence the balance of power without having to resort to an armed attack and minimize the risk of a military or nuclear response from their targets.

Keywords: Cyberspace; cyber conflict; cyber offensive capabilities; state-sponsored actions; cyberwar.

FIGURES

TABLES

Contents

1. INTRODUCTION

This research delves into the current state of cyber conflict and its consequences for nation-state competition. The study does not intend to present conceptual innovations, instead it focuses on empirical evidence to present its conclusions regarding the use of cyber offensive capabilities. With this approach this research will avoid inflating threats by considering hypothetical cases where devastating consequences could be achieved through offensive cyber offensive operations.

One of the most striking features of the 21st century is the widespread adoption of information technology in every aspect of the modern life of individuals, society, and nation-states. This process is referred to as the "Fourth Industrial Revolution," and the internet is its iconic expression (J. Nye 2010).

The internet went from innovation to one of the essential pillars of the modern economy. According to the United Nations, since 2014, all countries possess a digital footprint, though it varies in sophistication and scale (2020). A previous study also demonstrated that security is a major concern regarding cyberspace, as more than eighty countries have published national strategies for cyber security (Izycki and Colli 2019).

Moreover, the growing interconnectivity will increase exponentially in the years to come with the adoption of new 5G networks, the internet of things (IoT), large volumes of information (Big Data), the use of machine learning (artificial intelligence) and the use of quantum computing. As a result, economic activity and ordinary life will be even more exposed to the threat of offensive cyber operations (Kello 2017).

When compared to land, sea, air, and space, cyberspace has unique features. Its "geography" is easily modified, oceans and mountains are hard to be changed, but entire cyberspace regions can be turned on or off at the click of a button (Kramer 2009).

Additional features such as the relative anonymity, the irrelevance of geographical distances for some processes and purposes, the low cost of acquiring or developing offensive capabilities, and the plausible deniability of actions have turned this dimension into a theater of operations for nation-states (J. Nye 2010). Further, the collective perception is that the number of incidents and the number of actors will increase in the future (Geers and Lewis 2015).

Cyberspace can be conceptualized in different manners, but a straightforward approach defines it as a hybrid composed of physical and logical layers. Its infrastructure - servers, submarine cables, internet exchange points, internet connection providers - is oriented by economic laws, limited resources, and increasing marginal costs. The logical layer - content providers, web applications, data, information - allows for economies of scale given its intangible nature (J. Nye 2010).

These features have generated high frequency and low-intensity offensive actions (Rid and Buchanan 2015), potentialized by the absence of clear framing regarding international law application.

The actors in cyberspace vary from individuals to nation-states. Individuals (Edward Snowden and Chelsea Manning), hacktivists groups, and public disclosure services (such as WikiLeaks and Cryptome) have not displayed the same sophistication as nation-states. However, their actions caused worldwide political impacts (Coleman 2014).

The core of cyberspace infrastructure is owned and managed by multinational companies and organizations such as Amazon, Apple, Facebook, Google and Twitter –, an Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the domain name system (Domain Name System - DNS) and the Internet Engineering Task Force (IETF) is responsible for establishing the internet protocols globally.

Private actors also have a market share of offensive actions. Indeed, a noticeable number of them are the providers of cyber capabilities to state actors (Kello 2017). By 2018, at least 60 countries acquired some cyber offensive artifacts (Izycki and Brandão 2019).

This panorama prompts the following questions: what is the current state of affairs regarding nation-state cyber conflict? Will firing bits and bytes become more, or as frequent as, throwing bombs and firing bullets?

The debate regarding cyberspace and cyber conflict needs to be based on evidence and not extrapolations of the worst-case scenarios (Valeriano and Maness 2018). Threat inflation is a scourge of cybersecurity, in part due to private vendors because it is good for business and also for governments to take advantage of discourse to enhance their prerogatives and powers in cyberspace.

Following the steps of Valeriano and Maness (Valeriano and Maness 2018), this research intends to analyze empirical data about cyber offensive actions performed by - or that can be attributed to - nation-states, instead of focusing on high-profile hypothetical cyber-attacks. The purpose of this research is to provide a clear picture of the stakeholders and their behavior so that future policy decisions are based on accurate observations of cyberspace.

This research has two main goals for the fields of international security and international relations.

The first is a methodological contribution. This research built an algorithm to collect and process the empirical data used to examine its hypothesis. The extensive use of Python3 and Natural Language Processing (NLP) can be adjusted to different subjects within social sciences by preparing a customized ontology.

The second contribution of this research is to gather evidence of 29 different countries engaging in offensive cyber actions and 85 nations acquiring offensive cyber technologies from private vendors. The numbers challenge the average perception of concentration of cyber capabilities in a few "traditional" actors. This implies that cyberspace, as an operational theatre, favors the diffusion of power among nation-states.

To summarize, this master's research will provide an innovative contribution with an unprecedented dataset gathered from open source and official data. Besides the raw data, this

research will provide a unique perspective by addressing the nation-state stakeholders, their behavior, and their goals when conducting cyber offensive actions.

2. Conceptual Framework

To address such a complex issue as conflict in cyberspace, it is necessary to define the issue before engaging in analysis. The first item for the scope definition regards what conflict means in the context of this research.

There is a great divide regarding the nature of cyber conflicts. A host of authors consider that cyberspace introduced a revolution to state affairs, and there is an equally engaged group that claims that it is mere technological evolution.

The revolutionary faction began with the seminal work of Arquilla and Ronfeldt (1993) - Cyberwar is coming! - and continuously assert that cyberspace conflict will eventually escalate to the level of war (Kello 2017). Similar thinking was presented in the "cyber–Pearl Harbor" scenario by Leon Panetta, Central Intelligence Agency Director (2012). Influential works by Clarke and Knake (2010) also evaluate countries according to their cyber capabilities to wage war.

To this group, there is little doubt that the coming changes will be dramatic enough to induce structural transformations in the framework and pattern of states' mutual relations. If this is the case, current concepts and dynamics will become unfit to assess and predict future conflicts.

On the other side of the spectrum, evolutionists consider that cyberspace's intrinsic characteristics will prevent a purely cyber conflict. According to Thomas Rid This realm's engagement will be a variation from countries influencing each other, through espionage and sabotage (Rid 2011), a silent and persistent battle.

Rid (2011), Lindsay (2013), and Gartzke (2013) assert that cyber offensive actions lack the kinetic effects (destruction and loss of human lives) to be an autonomous instrument to pursue political goals. Rid goes as far as to say that cyberwar will never take place, given that conflict without death and violence to achieve a political goal (Clausewitz) is not war.

In this sense, Nye points out that it is unlikely that cyber conflicts provoke escalation, because states face constraints in cyber offensive actions (2018). This, in turn, would convert the so-called "offensive's advantage" into a myth (Valeriano, Jensen and Maness 2018).

This theoretical schism appears unsolvable given the currently available evidence. Perhaps only time will settle this dispute, with the emergence of conclusive concrete cases. However, both sides agree that there is an increase in cyber engagements, and further studies about the subject are necessary.

It should be highlighted however, that offensive cyber capability applications as a support for conventional weapons are very promising. Their use for command and control, remote sensoring, terrain monitoring, enhanced communications systems, and increased striking precision is already in place and improving.

The case of the 2008 Georgian War in which intense offensive cyber actions preceded the Russian invasion is a real example of the supportive nature to conventional engagement. Several attacks against government services and denial of service attacks were seen during the confrontation (Georgia 2009).

Another interesting example where cyber actions have displayed a supporting role to conventional actions is the Russian-Ukrainian conflict (ongoing since 2014). The cases of BlackEnergy (Kaspersky 2016) and Industroyer (Cherepanov 2017) campaigns are additional evidence that cyber actions are used to degrade the opponent's morale and infrastructure as part of an ongoing broader conventional conflict.

In fact, the use of new technology in conventional operations is inexorable and constant throughout history and is accelerating with the possibilities presented by cyberspace. This, however, should not be understood as cyberwar itself, as Rid clearly stated. Despite the relevance of cyber actions as support to the conventional military operations, this subject is not going to be addressed further in this study.

To avoid trying to solve this complex theoretical issue, this research will consider a broad idea of cyber conflict that can be achieved through offensive cyber actions. According to Valeriano and Maness (Valeriano and Maness 2016), it means "the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions."

This definition includes both Computer Network Attacks (actions from cyberspace that produce effects beyond the digital realm) and Computer Network Exploitation (actions and results remain contained in cyberspace) equally relevant. This vocabulary is often used by the United States government (Kramer 2009).

It is also relevant to incorporate the idea brought by Kello (2017), referring to cyberspace as a dimension in a state of *unpeace*. The concept portrays cyberspace as an intermediate where states can engage aggressively without crossing the armed attack threshold, thus not provoking war. However, at the same time, their actions are extremely detrimental to their targets.

It is assumed that to perform cyber actions, states need power, that they derive from capabilities and intent to perform actions (Voo, et al. 2020). The concept of power is used often, however there are various definitions of power.

There are at least three dimensions of power. The first, introduced by Robert Dahl, is the ability to enforce a third-party to do as you desire, something that they would not otherwise do. The second dimension of power proposed by Peter Bachrach and Morton Baratz addresses the notion of agenda-setting or framing, without necessarily any coercion instruments. Steven Lukes created the third face of power as he indicates that ideas and beliefs can shape a desirable outcome to the one exercising it (J. Nye 2010).

The three facets of power were later reorganized by Joseph Nye between the dichotomy of hard power (coercion and material retribution induce third parties' behavior) and soft power (persuasion, ideological attraction, and agenda-setting in a cooperative fashion induce behavior).

There are examples of soft and hard power applied through cyberspace: cyber actions with kinetic consequences and cyber actions with cybernetic effects (J. Nye 2010).

Nye (2010) provides a few examples to synthesize the concepts of Soft and Hard power and its effects within and beyond cyberspace:

Table 1 – Physical and Virtual Dimensions of Cyber Power

		Cyber Effects	Kinetic Effects
Kinetic Action	Hard Power	Government controls over internet/telecom companies	Bomb internet exchanges, cut submarine cables, or bomb threat actors HQ
	Soft Power	Providing infrastructure to human rights activists	Criminally prosecuting alleged state-sponsored hackers
Cyber Action	Hard Power	Wiper attacks (data destruction), denial of service attacks	SWIFT system heists, attacks against Critical Infrastructures
	Soft Power	Set norms and standards (5G), data privacy laws (GDPR)	Disinformation campaigns, public diplomacy in social networks

Source: Nye, Cyber Power, pg. 5, 2010

To address such a complex issue as conflict in cyberspace, it is necessary to define the issue before engaging in analysis. The first item for the scope definition regards what conflict means in the context of this research.

There is a great divide regarding the nature of cyber conflicts. A host of authors consider that cyberspace introduced a revolution to state affairs, and there is an equally engaged group that claims that it is mere technological evolution.

The revolutionary faction began with the seminal work of Arquilla and Ronfeldt (1993) - Cyberwar is coming! - and continuously assert that cyberspace conflict will eventually escalate to the level of war (Kello 2017). Similar thinking was presented in the "cyber–Pearl Harbor" scenario by Leon Panetta, Central Intelligence Agency Director (2012). Influential works by Clarke and Knake (2010) also evaluate countries according to their cyber capabilities to wage war.

To this group, there is little doubt that the coming changes will be dramatic enough to induce structural transformations in the framework and pattern of states' mutual relations. If this is the case, current concepts and dynamics will become unfit to assess and predict future conflicts.

On the other side of the spectrum, evolutionists consider that cyberspace's intrinsic characteristics will prevent a purely cyber conflict. According to Thomas Rid This realm's engagement will be a variation from countries influencing each other, through espionage and sabotage (Rid 2011), a silent and persistent battle.

Rid (2011), Lindsay (2013), and Gartzke (2013) assert that cyber offensive actions lack the kinetic effects (destruction and loss of human lives) to be an autonomous instrument to pursue political goals. Rid goes as far as to say that cyberwar will never take place, given that conflict without death and violence to achieve a political goal (Clausewitz) is not war.

In this sense, Nye points out that it is unlikely that cyber conflicts provoke escalation, because states face constraints in cyber offensive actions (2018). This, in turn, would convert the so-called "offensive's advantage" into a myth (Valeriano, Jensen and Maness 2018).

This theoretical schism appears unsolvable given the currently available evidence. Perhaps only time will settle this dispute, with the emergence of conclusive concrete cases. However, both sides agree that there is an increase in cyber engagements, and further studies about the subject are necessary.

It should be highlighted however, that offensive cyber capability applications as a support for conventional weapons are very promising. Their use for command and control, remote sensors, terrain monitoring, enhanced communications systems, and increased striking precision is already in place and improving.

The case of the 2008 Georgian War in which intense offensive cyber actions preceded the Russian invasion is a real example of the supportive nature to conventional engagement. Several attacks against government services and denial of service attacks were seen during the confrontation (Georgia 2009).

Another interesting example where cyber actions have displayed a supporting role to conventional actions is the Russian-Ukrainian conflict (ongoing since 2014). The cases of BlackEnergy (Kaspersky 2016) and Industroyer (Cherepanov 2017) campaigns are additional evidence that cyber actions are used to degrade the opponent’s morale and infrastructure as part of an ongoing broader conventional conflict.

In fact, the use of new technology in conventional operations is inexorable and constant throughout history and is accelerating with the possibilities presented by cyberspace. This, however, should not be understood as cyberwar itself, as Rid clearly stated. Despite the relevance of cyber actions as support to the conventional military operations, this subject is not going to be addressed further in this study.

To avoid trying to solve this complex theoretical issue, this research will consider a broad idea of cyber conflict that can be achieved through offensive cyber actions. According to Valeriano and Maness (Valeriano and Maness 2016), it means "the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions."

This definition includes both Computer Network Attacks (actions from cyberspace that produce effects beyond the digital realm) and Computer Network Exploitation (actions and results remain contained in cyberspace) equally relevant. This vocabulary is often used by the United States government (Kramer 2009).

It is also relevant to incorporate the idea brought by Kello (2017), referring to cyberspace as a dimension in a state of *unpeace*. The concept portrays cyberspace as an intermediate where states can engage aggressively without crossing the armed attack threshold, thus not provoking war. However, at the same time, their actions are extremely detrimental to their targets.

It is assumed that to perform cyber actions, states need power, that they derive from capabilities and intent to perform actions (Voo, et al. 2020). The concept of power is used often, however there are various definitions of power.

There are at least three dimensions of power. The first, introduced by Robert Dahl, is the ability to enforce a third-party to do as you desire, something that they would not otherwise do. The second dimension of power proposed by Peter Bachrach and Morton Baratz addresses the notion of agenda-setting or framing, without necessarily any coercion instruments. Steven Lukes created the third face of power as he indicates that ideas and beliefs can shape a desirable outcome to the one exercising it (J. Nye 2010).

The three facets of power were later reorganized by Joseph Nye between the dichotomy of hard power (coercion and material retribution induce third parties' behavior) and soft power (persuasion, ideological attraction, and agenda-setting in a cooperative fashion induce behavior).

There are examples of soft and hard power applied through cyberspace: cyber actions with kinetic consequences and cyber actions with cybernetic effects (J. Nye 2010).

Nye (2010) provides a few examples to synthesize the concepts of Soft and Hard power and its effects within and beyond cyberspace:

Table 2 – Physical and Virtual Dimensions of Cyber Power

		Cyber Effects	Kinetic Effects
Kinetic Action	Hard Power	Government controls over internet/telecom companies	Bomb internet exchanges, cut submarine cables, or bomb threat actors HQ
	Soft Power	Providing infrastructure to human rights activists	Criminally prosecuting alleged state-sponsored hackers
Cyber Action	Hard Power	Wiper attacks (data destruction), denial of service attacks	SWIFT system heists, attacks against Critical Infrastructures
	Soft Power	Set norms and standards (5G), data privacy laws (GDPR)	Disinformation campaigns, public diplomacy in social networks

Source: Nye, Cyber Power, pg. 5, 2010

This research focuses on the bottom line: Cyber Actions taken through Hard and Soft Power. Whether that entails Cyber, Kinetic, or both effects are part of the analysis.

Regarding offensive capabilities that fulfill cyber actions, this research adopts the position of Rid and McBurney (2012) that these are "computer codes that are used or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."

Cardenal et al. (2017) suggest that some facets of cyber actions should be granted the status of sharp power since they are not coercive (military or economic) nor cultural/attractive (positive appeal and values). The idea is to frame actions such as censorship and disinformation (misinformation included) as exercises in sharp power.

In a similar fashion, Lopes proposes an alternative for that dichotomy called *software power*. The concept conveys alternative uses for power in cyberspace. It entices academics because it offers a view of power that allows projection without space-time conventional restraints while it is conditioned by the anarchical international order (Lopes 2016).

As a theoretical proposition, both concepts are very interesting. However, the elements that transform "public diplomacy" (soft power) into a "disinformation campaign" are, at best, murkier to be spotted in a real case. Lopes' concept is very promising, but it will not be addressed further in this dissertation. It merits a study of its own as a lens to interpret the data presented here.

Regarding the tactics in which cyber action takes shape, Ciaran Martin (2020), former Chief of the National Cyber Security Center and currently a professor at King's College, proposes a five-tier offensive cyber action level.

- Hacking: computer operations in pursuit of specific national defense objectives
- Adversarial infrastructure destruction: targeted destruction of adversary digital infrastructure
- Counter-influencing: promoting unhelpful info or 'prepositioning' on adversary critical infrastructure
- Kinetic: offensive cyber-operation to achieve significant and painful disruption in adversary country
- Systems wide: an all-out attack on military and civilian networks in the context of conflict

A similar approach is proposed by the Belfer Center for Science and International Affairs (Harvard Kennedy School) in its National Cyber Power Index 2020 – NCPI (Voo, et al. 2020). With the concept of national objectives that countries pursue with cyber means, the NCPI lists seven capabilities to be developed by nations:

- Surveilling and Monitoring Domestic Groups;

- Strengthening and Enhancing National Cyber Defenses;
- Controlling and Manipulating the Information Environment;
- Foreign Intelligence Collection for National Security;
- Commercial Gain or Enhancing Domestic Industry Growth;
- Destroying or Disabling an Adversary's Infrastructure and Capabilities; and,
- Defining International Cyber Norms and Technical Standards.

Based on these two sources, this research considered the following goals to identify offensive cyber capabilities as the wielding of cyber power:

- Surveillance - ability to surreptitiously access the digital communication, location of users (online or offline), data usage, and metadata produced (United Nations 2019)
- Disinformation - the adoption of the information disorder theoretical framework, which includes false information (inadvertently or deliberately) or genuine information or opinion to cause harm (Wardle and Derakhshan 2017)
- Espionage - unauthorized access into a system to collect information for immediate use or to manipulate the decision-making process in the long-term (Valeriano, Jensen and Maness 2018)
- Sabotage/Degradation - attempts to physically compromise the target's ability to operate properly (Valeriano, Jensen and Maness 2018)

Through soft or hard power, nation-states engage in offensive cyber actions and pursue particular national strategic objectives. None of these cyber-enabled actions are unprecedented, but their impact, scale, and low costs make this approach advantageous.

Policymakers tend to assess opponent’s behavior based on the information available about capabilities and intentions (Jervis). This research aims to present an overview of offensive cyber capabilities and their use by nation-states.

3. Literature Review

A significant number of previous researchers devoted time and effort to gather and analyze offensive cyber actions. Their objectives and methodologies are somewhat different from the ones undertaken in this research. However, they provided invaluable lessons regarding successes and pitfalls.

The book "A fierce domain conflict in cyberspace, 1986 to 2012", by Healey and Grindal (2013), is one of this research's precursors. The book collects a vast number of historical records

related to cyber conflict. It is an extensive data collection that includes actions from State and non-state actors. A few incidents are also included without acknowledgment of their occurrence.

In that same year, the United Nations Institute for Disarmament Research (UNIDIR) published a study about national cyber capabilities. The document pointed to 67 countries with civilian cybersecurity programs and 41 countries with units or military doctrines for cyber defense (2013). The document was based on National Strategies, Military Doctrines, and national legislation. It provided an official outlook of countries' intentions towards cyberspace, but it did not consider actual offensive cyber actions undertaken by nation-states.

The Wall Street Journal published an article that cataloged the world's cyber forces. The research was based on open-source material, interviews with cybersecurity experts, and historical data gathered to portray the 'new arms race' (Valentino-DeVries, Thuy Vo and Yadron 2015). The article did not discern state and non-state actors, often presenting private vendors and hacking groups as evidence of nation-state offensive cyber capabilities. The lack of rigorous criteria in classifying information weakens the conclusions regarding the countries' actual offensive cyber capabilities.

Another interesting project that collected information regarding offensive cyber capabilities is the Cyber Operations Tracker (2020), maintained by the Council on Foreign Relations (CFR). It is an ongoing database of over 300 records. The collection is a product of open-source monitoring of offensive cyber actions claimed by a nation-state. The dataset also proposes a taxonomy of incidents, origins, targets (nation and sector), and if the action is supported from the targeted country (2019). This project heavily influenced the collection proposed in this research.

Lindsay (2014) produced an interesting collection and analysis of historical records of offensive cyber actions attributed to China. The prominent cases are addressed in the study, and the conclusion is that espionage and intellectual property theft are the main objectives of Chinese offensive cyber actions. The drawback is the limitation of scope to only Chinese cases.

The collective research spearheaded by Florian Roth provided additional inspiration for this research. It is a project that gathers information regarding Advanced Persistent Threats (APT) executed or sponsored by nation-states (Roth 2019). This project is extensive in it’s special attention to attribution (normalizing different threat actors' names), the origin of threat groups (evidence that supports claims, not mere finger-pointing), and the collection of additional incident characteristics. Several of these paradigms were observed when modeling the methodology for this research.

Several other relevant works could be mentioned: Richardson (2011), Farwel and Rohozinski (2011), Bencsáth et al. (2012) and Jorge (2017). They are relevant because of the rigorous analysis of offensive cyber actions attributed to nation-states. However, the articles focus on particular incidents or campaigns - the first two address the Stuxnet case and the last two Flame, Duqu and Gauss. This limits the possibilities to extrapolate a global perspective based on a few selected cases that are considered outliers in terms of offensive actions (Valeriano and Maness 2014).

The most relevant works for this dissertation are the studies done by Valeriano and Maness in several papers and books. In the paper, '*The dynamics of cyber conflict between rival antagonists, 2001–11'*, the authors gathered over 110 incidents within interstate rivalry between 2001 and 2011. Later in their book, their collection increased to 192 incidents that covered and analyzed interstate rivalry (2014).

Their research is prolific and challenges the popular perception that cyberspace is on the brink of a global conflict. They provide solid evidence to support the claim that cyber conflicts are regionally oriented and usually involve countries with a prior geopolitical interest in the dispute.

According to Valeriano and Maness (2018), nation-states' use of offensive cyber capabilities is constrained, and there are no escalatory patterns identified so far. The most common goal for countries is to conduct espionage or create low severity disruption of their targets' online services.

There are several works regarding empirical analysis of offensive cyber actions. However, few of them delve into a broad comparative analysis. Inquiries regarding the causes or objectives of cyber actions are rare. These previous studies are relevant as they present interesting strategies regarding analytical tools and methodology. Thus, they have influenced this research.

An additional concern is the use of frameworks that only address actions associated with destruction and death, given that these events, albeit possible, have not happened. This is the reason to create an analytical framework to understand the lower-intensity conflicts.

4. Research Questions

The combination of the low cost of entry, the relative anonymity (plausible deniability), and the fact that cyberspace enhanced traditional means of statecraft has turned cyberspace into an attractive theater of operations for countries.

This research`s focus will not be on the potential consequences of cyber actions but the actual usage by nation-states during the last twelve years. Arguably, countries can destroy each other through conventional nuclear weapons, but they choose not to do so. Thus, one should not consider the potential damage of a cataclysmical offensive cyber action but base the analysis on empirical grounds.

The main objective is to deliver an in-depth portrait of offensive cyber capabilities and actions by nation-states over the last decade. The overarching results will allow the academic community to better understand different behaviors, strategies, and objectives that countries display when engaging in cyberspace.

To achieve the main objective the research will collect, classify and describe the goals of cyber offensive actions, its protagonists, and its targets.

As a secondary goal, this research intends to use the available data to enquire if there is a presence of a hegemon in cyberspace, with capabilities to act across the globe in an unmatched manner. Or if there is a bipolar confrontation where the United States and China strive for

leadership. As a third scenario, if there is a multipolar cyberspace where several regional actors display similar capabilities to act and engage.

Finally, the volume of data will allow the uncovering of trends associated with cyberspace and nation-state behavior. This will be useful for future researchers, to highlight subjects that were not fully explored in this dissertation for the sake of brevity.

5. METHODOLOGY

There are a few previous works that engage in cyber-attack historical analysis such as Healey and Grindal (2013), the UNIDIR (2013), a study published by the Wall Street Journal (Valentino-DeVries, Thuy Vo and Yadron 2015), the Council of Foreign Relations (2020), several open-source projects available at code sharing platforms (Bandla 2020), the Mitre Corporation (MITRE 2019), and Malware Information Sharing Platform – MISP (2019). They are all relevant because of the prior collection of data regarding cyber-attacks and how to process them. However, they have not delved into the motivations, the goals, and the intended targets of the attacks.

Despite the numerous references of cyber-attacks in traditional media outlets, rarely do they present technical remarks or concrete evidence supporting their stories. They are often the product of human sources that disclose details about a cyber-attack, such as the attribution of authorship, techniques employed, and the target's compromise level. However, without backing it up with data and concrete evidence, a story can be told to serve a political purpose, whether to be detrimental to the victim or the alleged perpetrator of the cyber-attack.

Thereby, to evaluate the current condition of cyber conflicts, this research sought objective data concerning cyber-attacks and Nation-State offensive capabilities. The goal is not to rely solely on conventional news, instead, the research identified sources of technical reports that could withstand a rigorous analysis. As a result, this research relied on four major sources:

- technical reports by cybersecurity private companies and national incident response teams (CSIRTs);
- independent studies by non-governmental organizations and universities;
- information leakage suffered from private vendors of spyware and governmental agencies;
- reports from export controls of European countries.

The four different sources of information provide insight into distinct features of Nation-State offensive cyber capabilities.

The first two – technical reports and independent studies – are clustered together for collection and processing. They usually describe complex campaigns that are frequently referred to as Advanced Persistent Threats (APT). They display detailed information about sophisticated long-term campaigns conducted or sponsored by Nation-States. The data provided by these

documents is strong evidence of both offensive cyber capability and intent, given that they analyze actual cyber-attacks.

This research gathered 1,885 technical reports describing cyber-attacks from 2008 to 2020. The research organized the documents into campaigns or groups based on who the attacks were attributed to, which resulted in 461 different threat-actors.

The technical reports and independent studies gathering process is described in the next session.

5.1. *Research Limitations*

This research sets ambitious goals for itself, but some limitations regarding the methodology will be explicitly addressed in this subsection.

The data gathering is dependent on the publicizing of cyber offensive actions and cyber capability acquisition. Therefore, there are unknown state-sponsored cyber actions that were not publicly disclosed and remained beyond this research's reach (Voo, et al. 2020). That does not mean that the data is not representative, but that it is only a fraction of the whole.

Another limitation to consider are the data sources. This research went to great lengths to gather a host of sources. Nevertheless, 80.6% of the dataset is provided by cybersecurity companies' technical reports. Given the nature of their services, some details might not be shared because of confidentiality clauses (Egloff and Wenger 2019). Alternatively, the analysis might be considered skewed for marketing purposes (Valeriano and Maness 2014).

Conversely, market competitiveness creates a balance that can be used by private companies to challenge fragile assumptions or conclusions once a technical report goes public. This reduces the possibility of inaccurate reports (Eichensehr 2020).

Western sources are predominant (73%), from which 48% are from American companies. This suggests that most of the targets of the cyber offensive actions are from western countries (customers of those companies).

Finally, the technical knowledge of the author is another limitation. Technical reports often delve into details that could not be validated or refuted by the author. Thus, the content is assumed to be accurate or questioned by another technical report (market competition).

Despite these limitations, the research data represents a significant sample from cyber offensive capabilities and actions from 2008 to 2020, allowing their use as projections on a global scale.

5.2. *Technical Reports and Independent Studies*

The technical reports and independent studies collection process was made possible by creating and maintaining automated scripts, specially developed for this purpose. This was done through several scripts built with the Python programming language.

The starting point was a sample-dataset provided at GitHub, the repository kbandla/APTnotes. This repository contained over 300 reports (from 2008 to 2016) from 20 different providers who described cyber-attacks considered APTs. Most of the reports were about offensive actions conducted by Nation-States and directed against other countries.

The first step was creating a model for identifying new documents that contained information about similar cyber-attacks, preferably conducted or sponsored by Nation-States.

Among the 20 different providers originally collected by the kbandla/APTnotes repositories were cybersecurity vendors, CSIRTs, and NGOs. From these categories, this research undertook an effort to identify companies and institutions with similar profiles.

The search for private cybersecurity vendors was the easiest task since most private companies advertise their products by publishing blog posts and white papers that describe APT threat actors. Nation-States are high-profile and first-tier actors facilitated the search because the reports received traditional media coverage.

The Forum of Incident Response and Security Teams (FIRST) was an important source to CSIRTs. The FIRST gathers 531 incident response teams across the world. Most of the CSIRTs have a webpage where they share content about cyber-attacks relevant and within the scope of this research.

To look for NGOs and independent cybersecurity researchers was more challenging. The fact that there is no equivalent to FIRST demanded a decentralized search across open-source data. Cybersecurity conferences – such as DefCon, Black Hat, Virus Bulletin – were excellent places to find NGOs and independent researchers publicizing their findings.

The tracking of technical reports and independent studies was a fundamental step towards the dataset for this research. Once those sources were identified, they were put into a daily monitoring routine. The Python scripts automatically "visited" the APT source's web pages to look for new reports or blog posts. Once the script found a new piece of information, they retrieved the content (e.g., web scraping). They sent an alert to notify a human supervisor in order to validate the collected item.

This process is operated incrementally. Thus, a new source can be included in the script, and the news reports are collected as they are published. The previous APT reports or blog posts are also collected retroactively to increase the dataset.

By the end of this dissertation's collection – December 2020 – 234 different sources were being monitored daily by the proprietary Python scripts.

5.3. *Data Breaches*

This research also gathered data from private vendors and state-sponsored APT threat actor's data breaches. The leaks have granted unprecedented access to the restricted private market and the development of offensive cyber capabilities.

There have been two major data breaches from offensive capabilities in private vendors from offensive capabilities: from Gamma Group in 2014 (WikiLeaks 2014), from Hacking Team in 2015 (WikiLeaks 2015). Both of the private vendor's data breaches are not clearly attributed to a state-actor. However, the sheer volume of information disclosed is remarkable. The Gamma Group breach amounted to 40 GB and included customer information, manuals, training materials, and source code for the spyware sold. The Hacking Team leak included more than a million emails exchanged from the Italian branch, overseas offices, and government customers.

The attack on the CIA became known as Vault 7. The agency suffered a cyber-attack from a non-governmental group, and its cyber weapons were published online (WikiLeaks 2017). The leak was claimed by the Shadow Brokers, an alleged hacktivist group that wanted to sell the exploits and later publicize the tools used by the American intelligence agency. There is a suspicion that the Shadow Brokers were, in fact, a hacking group working for the Russian government, but no evidence supporting this was presented (Risk Based Security 2016).

An Iranian state-sponsored APT threat-actor also suffered a data breach. A group called Lab Dookhtegan (Cimpanu 2019), allegedly composed of dissidents from the Iranian Revolutionary Guard cyber branch, leaked information about Iranian hackers' personal identities, details about their attacks, and source code of offensive cyber capabilities. Lab Dookhtegan remains active to this day, publishing new information monthly.

WikiLeaks gathered a massive amount of information from the data breaches and, through its web interface at www.wikileaks.org facilitated the collection for this research. By simple queries to WikiLeaks' online platform, data regarding offensive capabilities acquisition and government tools could be gathered and downloaded. In some cases, it was possible to infer if the entity responsible for the purchase was a military branch, law enforcement, or an intelligence agency based on the information released during the breaches.

5.4. *Report from Exports Controls*

The fourth source for this research was reports collected from export controls publicized – the countries in which some private vendors have their headquarters. This data was available for only a few countries: the United Kingdom, Switzerland, Germany.

A third-party (McGrath, Novak and Gallagher 2016) gathered and indexed the open-source project called Transparency Toolkit. The data is available for download and online queries.

The reports did not identify the private vendor selling, nor the exact software being sold. However, they identified the country for whom the export license was issued. That helped as additional evidence of intent from the acquiring country.

5.5. *Processing the data collected*

The collected information comprises two datasets relevant for this research but with distinct characteristics. The technical reports provided information about actual offensive cyber capabilities. The second set was collected from the data breaches and granted information about countries' intent by developing or acquiring offensive cyber technology from private companies.

Both sets provided invaluable information about Nation-States offensive cyber capabilities. The first gave insights into 34 countries that have displayed offensive capabilities. The second set of information provided a detailed overview of the 85 countries that acquired offensive capabilities, though the dataset lacks evidence for their actual use.

The first dataset was analyzed with Natural Language Processing (Spacy – Python 3.7). Spacy is a Python library that enables text processing and entity extraction without the loss of syntactical meaning. This processing step required more customized Python scripts for the adequate use of Spacy.

In the next section, the natural language process is described.

5.6. *The Classification and Entity Recognition*

Python scripts for natural language processing were applied into the first dataset. This process included building custom dictionaries (Appendix D), removing stop-words from the text, word lemmatization, phrase matching, and text extraction.

The overarching goal of the scripts was looking for cyber-attack attribution (whether it was state-executed, state-sponsored, or a non-state actor), information on the victims (if it was a government and/or which industry it targeted), the countries affected by the attack, and the purpose of the cyber-attacks/campaigns (e.g., financial gain, espionage, sabotage). It was also possible to collect and classify MITRE Attacks Techniques and CVEs employed during the offensive actions.

The entity recognition was entirely done using Spacy and its Large English library (a total of 65,000 English words), with the inclusion of few additional particular expressions. Since most of the documents were originally written in English (over 95%), this facilitated the use of Spacy's text extracting features. This research used the free service provided by Google Translator to translate all documents into English.

Initially, this research selected a random sample of documents to submit it to human classification and text extraction. Thus, creating a dictionary of words associated with the classification criteria. For example, for identifying a state-directed or state-sponsored cyber-

attack, the dictionary included the following words: state-sponsored, state conducted, state-led, and state support.

The dictionaries used for classification were a preparatory measure done before the automated text extraction. Nevertheless, it was common to append new words to the dictionaries as more documents were submitted to the next phase. This was done during Python scripts human supervision.

The text extraction automation process had two preparatory steps performed with Spacy: the exclusion of stop-words and the word lemmatization.

Stop-words are broadly defined as common words that do not interfere with the natural language process. Thus, as the 362 words – provided by Spacy's English Library default feature – do not help clarify the meaning of sentences, they are automatically excluded from the process.

The next step was the lemmatization of the text. This process reduces the words of the text into their radical form (e.g., the words processing and processed are understood by the script as "process"). Despite the reduction to their radical, the text still retains its syntactic meaning, so the original sentence's purpose is not lost during the script execution.

After removing stop-words and the lemmatization, the text is ready for phrase matching and text extraction step.

The phrase matching iterated the dictionaries built in the preparatory step aforementioned. Spacy automatically classifies the processed text according to its syntactical meaning. Thus, the comparison of dictionary words to the main-text had an improved performance because it was oriented to their meaning. Nationalities' adjectives and countries' names were only compared to the GPE word category provided by Spacy. The hacking group and victim's names were solely compared to the ENTITY word category.

Once the processing script matched a dictionary's word to the main text, it was stored in the database as an attribute for the document. Thus, every document processed was compared to every dictionary, and when a match was found, the information was added in a database. This allowed for multiple classifications of each document.

An additional classification was performed to cluster the reports into campaigns/threat actors. According to the myriad of names that private vendors use to refer to. Therefore, sources were classified as known APT groups base on the numerous names used by vendors. the, sources classify known APT groups according to the myriad of names that private vendors use. This was instrumental in performing analysis regarding the capabilities and intents of Nation-States.

The result was a dataset that classifies each document regarding authorship, if nation-affiliated, which group was attributed, the target's nature, and the duration of the cyber-attack/campaign.

5.7. *Parsing Structured Data*

The second dataset was built from structured data. The data breaches from Hacking Team, Gamma Group, Vault 7, and Lab Dookhtegan consisted of a huge volume of files. Wikileaks successfully indexed the files with a user friendly interface. It allowed queries to search for countries that developed cyber weapons and those that acquired offensive cyber capabilities from private vendors. There was evidence to attribute the spyware purchase to a military force, law enforcement, or intelligence agency in some cases.

The evidence provided by both leaks is abundant. Besides commercial information about how the spyware operates; the e-mail communication, invoices from the purchases, and even spreadsheets detailing the buyers provided a full picture of this share of the cyber-weapons market.

On a few occasions, the second dataset's information was successfully correlated to the information collected in the first dataset (the intent was materialized in actual capabilities). This was the case for reports from The Citizen Lab and Amnesty International that corroborated the purchases of cyber offensive capabilities from Morocco, United Arab Emirates (UAE), Saudi Arabia, and Bahrain.

Based on the available information, this research considered a set of twelve private vendors as providers of offensive cyber capabilities: Amesys, Area SpA, Cyberbit, Dreamlab, Elbit, FinFisher, Hacking Team, Sandvine, NICE Systems, NSO Group, SS8, and Trovicor (Teach 2020).

Thus, the parsing of data searched for evidence of commercialization of cyber capabilities from those twelve providers to any Nation-State. Once the script identified a match to both conditions, it added the database's information to further analysis.

5.8. *Threat actors and document clustering*

A factor that improved attribution is the increase of evidence accumulated over the years. Threat actors have been monitored for long periods of time, and information is shared among multiple stakeholders in the cybersecurity community (Roth 2019). In most cases, only the correlation from different malware and campaigns over long periods of time allowed an attribution with a higher confidence level.

One additional variable must be explained about attribution and its consequences for this research. The attributed attacks can describe a threat group, intrusion sets, and campaigns. The clustering of documents within the same threat actor based on different methodologies is the minimal analytical unit for this research (MITRE 2019).

Despite significant improvements, attribution remains a challenge in cyberspace. Those mainly responsible for it are research institutions and private cybersecurity vendors, but even

nation-states also attribute offensive cyber actions more often in the last few of years than during the early 2000's (Egloff and Wenger 2019).

The plausible deniability is also a concern because no state actor accepted or claimed responsibility for a particular offensive cyber action attributed to another country. It should be noted that the authorship of even kinetic actions might remain unclear. Recent examples of those are the Malaysian Flight 17 (shot down over Ukraine, likely by militias armed with Russian equipment) and the Abqaiq–Khurais refinery attacks in Saudi Arabia (allegedly by Houthi rebels armed with Iranian drones). Neither of these attacks were clearly attributed.

Each document is processed individually and, if possible, is indexed to a threat actor (based on different methodologies provided by its original author). This set of documents allows the threat actors profiling: motivations, resources, targets, preferred sectors, and state-affiliation. It also allowes for the cross-checking of references from multiple vendors, increasing confidence in the analytical process.

Hence, the set of documents provides attributes to the threat actors, and its affiliation to a country is the object of the analysis for Nation-State behavior in cyberspace.

An additional challenge is faced and created by the cybersecurity vendors. A myriad of vendors addresses the same threat actor with different names within the cybersecurity industry. It occurs due to human, technical and operational reasons (Roth 2018).

Due to the "human factor", cybersecurity vendors name threat actors after operations (e.g., Electric Powder) or malware used (e.g., NetTraveler). Also, vendors do not relate to threat actors (e.g., TEMP.Zagros and MuddyWater).

As for technical reasons, threat actors often share tools and infrastructure (e.g., Winniti) and split or join forces. Most importantly, vendors see different pieces of the same puzzle (different malware samples, C2 infrastructure, TTP, and IoCs).

Finally, the ability to conduct forensic investigations in ways in which other vendors might disagree with, is a strong reason for the multiplicity of threat actor names. A second operational reason is market competitiveness. By creating their own names, vendors do not implicitly recognize their competitor's research as better, more thorough, or precedent setting.

In order to avoid double-counting the same threat actor, the threat actors' synonyms are compliant with Roth (2018), MISP (2019), and MITRE Corporation (2019). This means that the most accurate landscape of threat actors available by the end of 2020 was taken. As new information is uncovered, groups with no established affiliation certainly will be tracked.

5.9. *Merging the Datasets*

Since the main goal of this research is to portray a clear picture of the cyber offensive capabilities of Nation-States. To achieve that goal, it was necessary to combine the two datasets.

Whenever available, the information collected was associated with a country (purchase, origin, or target), a date/period (acquisition or attack), and the victim's characteristics.

The compiled dataset is the basis for the Nation-State behavior analysis accomplished in this research. It was possible to identify which demonstrate intent (acquired technology that enables them to perform cyber-attacks) and which states displayed actual offensive cyber capabilities (performing cyber actions).

In the next section, we will perform a comprehensive analysis of the dataset. We will go deeper into the cases of documented cyberattacks attributed to Nation-States. The origins and targets of the attacks, their relation to each other, and regular geopolitical issues will be the subject of analysis.

6. Overarching Results

The data gathering process collected over 3000 documents. After the analysis, 1,885 documents remained describing APTs campaigns/threat actors. The analysis performed a classification of each document concerning the support of state-actors.

As mentioned before, the attribution process is a complex endeavor. Nevertheless, 1,034 documents (54.9%) establish some level of authorship. In most cases, the technical analysis identified the threat actor, its idiom, country, or origin region.

In some cases, there is the attribution of a threat-actor nationality, but there is no evidence that it had the support, sponsor, or acquiescence of the hosting country. In light of this, it became important to undertake this dichotomous classification within documents: state-sponsored attacks and independent threat actors acting from a particular country or region.

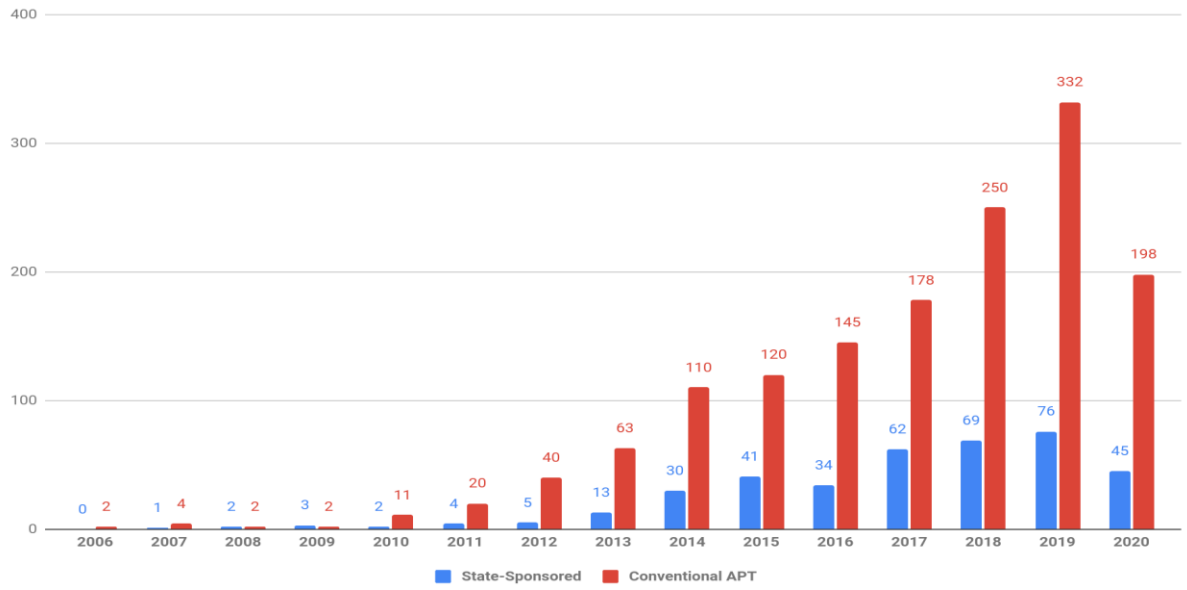
This research adopts Tim Maurer's notion of proxies acting on behalf of governments, i.e., when an intermediary conduct or contribute to a offensive cyber action that is enabled knowingly by a beneficiary (2018). Three forms of state-sponsored relationships are defined:

- Delegation: the principal grants authority to an agent to act on its behalf
- Orchestration: providing support (ideational or material) and directing them at particular targets
- Sanctioning: tolerates the actions of the threat-actor despite having the capabilities to stop it

From the documents with attribution, a total of 389 documents presented evidence of state-sponsored cyber offensive activities. The number represents 20,6% of the 1,885 documents and is equivalent to 37.6% of all documents with some attribution. It is an impressive figure, especially in light of the common idea that attacks remain anonymous on the internet.

Another interesting feature provided by the dataset is the increase of cyber-attacks during the 2006 and 2020 period.

Figure 1 – Number of reported APTs attacks (2008-2020)



Source: Izycki, Eduardo

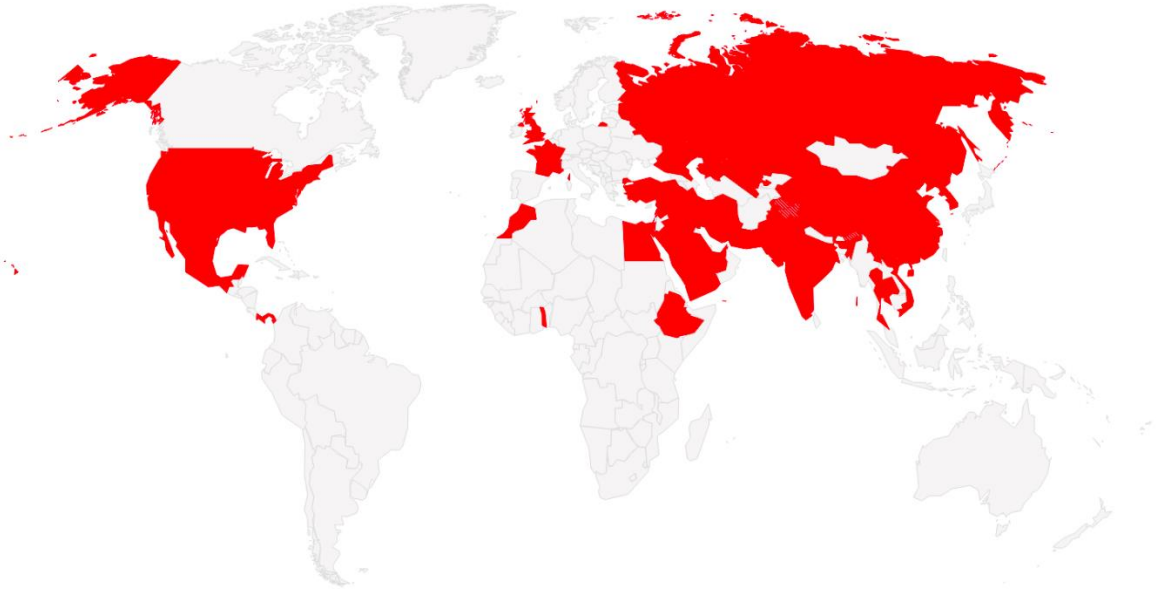
The reports are systematically increasing over the years. The 2020 apparent drop is probably due to the natural delay in producing reports as they refer to activities from the weeks and months before.

The results of the research also validate an established idea: multiple actors are engaging in offensive actions in cyberspace. However, the figures and the countries involved might come as a surprise. There is evidence that 29 different nations have already performed offensive cyber actions, either directly or by supporting a threat actor.

The list goes well beyond the traditional cyber powerhouses: China, Russia, Iran, Israel, North Korea, and the United States. It includes the likes of Bahrain, Egypt, Ethiopia, France, India, Iraq, Lebanon, Mexico, Morocco, Kazakhstan, Pakistan, Panama, South Korea, Syria, Saudi Arabia, Thailand, Togo, Turkey, the United Arab Emirates, the United Kingdom, Uzbekistan, Vietnam, and Yemen.

The 29 countries have proven offensive cyber capabilities and have demonstrated the intent to act within cyberspace.

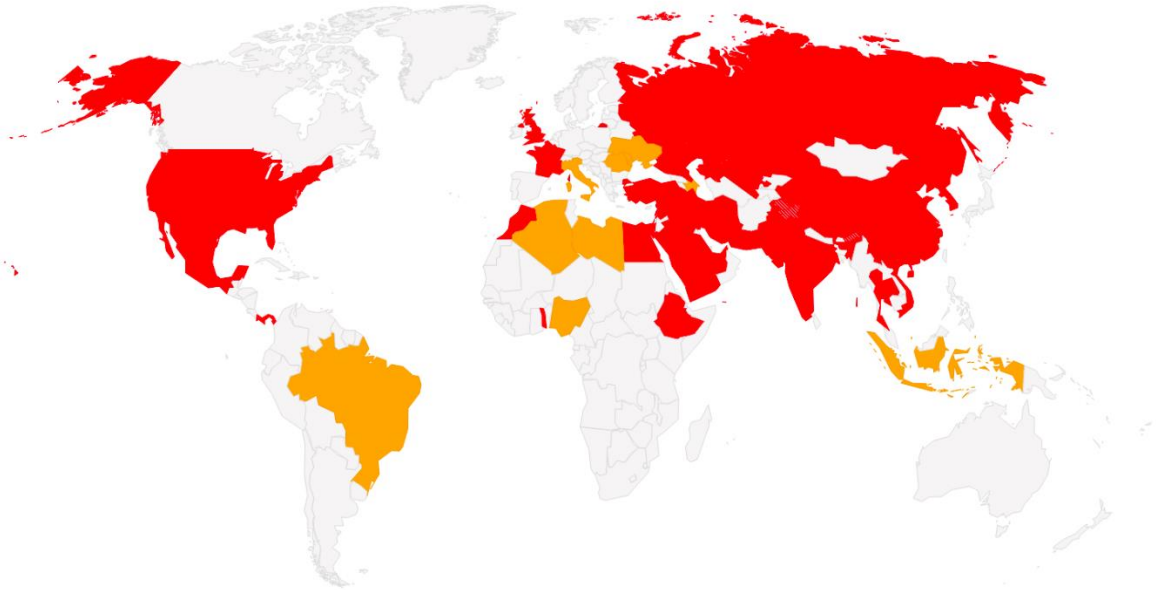
Figure 2 – Countries with state-sponsored APT activity (2008-2020)



Source: Izycki, Eduardo

The figures became even more impressive for the cases of native threat actors identified without evidence of state support. A total of 40 countries were shown to have indigenous human resources to perform sophisticated cyber offensive actions.

Figure 3 – APT activity attributed to a country without evidence of state support (2008-2020)



Source: Izycki, Eduardo

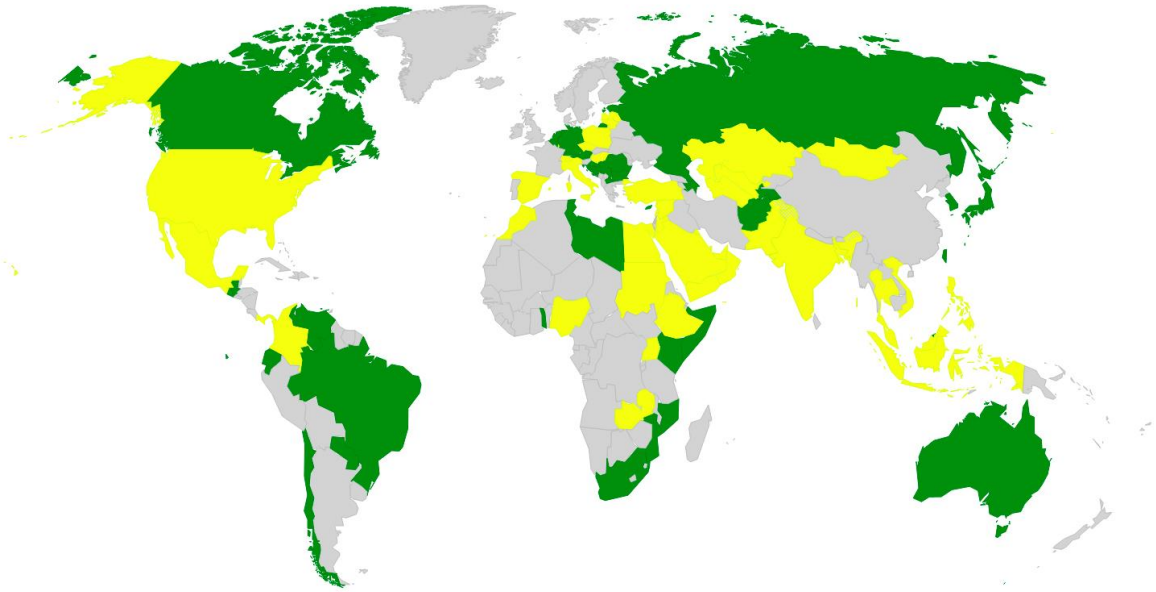
The included countries with APTs originating from its borders are Brazil, Ukraine, Indonesia, Italy, Romania, Azerbaijan, Algeria, Nigeria, Palestine, Libya, and Moldova.

The 11 aforementioned countries are considered to have proven indigenous offensive cyber capabilities despite no evidence of allocation to their local government.

The dataset also portrays a host of 85 countries that acquired offensive cyber capabilities from the private sector, although no concrete evidence of its use has been provided. This staggering number coupled with the sophistication level presented by each software acquired suggests that offensive capabilities are widespread in cyberspace.

Moreover, the purchasing of state-of-the-art offensive cyber capabilities was not a one-time deal; 45 countries (52,9%) acquired offensive solutions more than once. It consists of an additional confirmation of intent by Nation-States to be assertive in cyberspace.

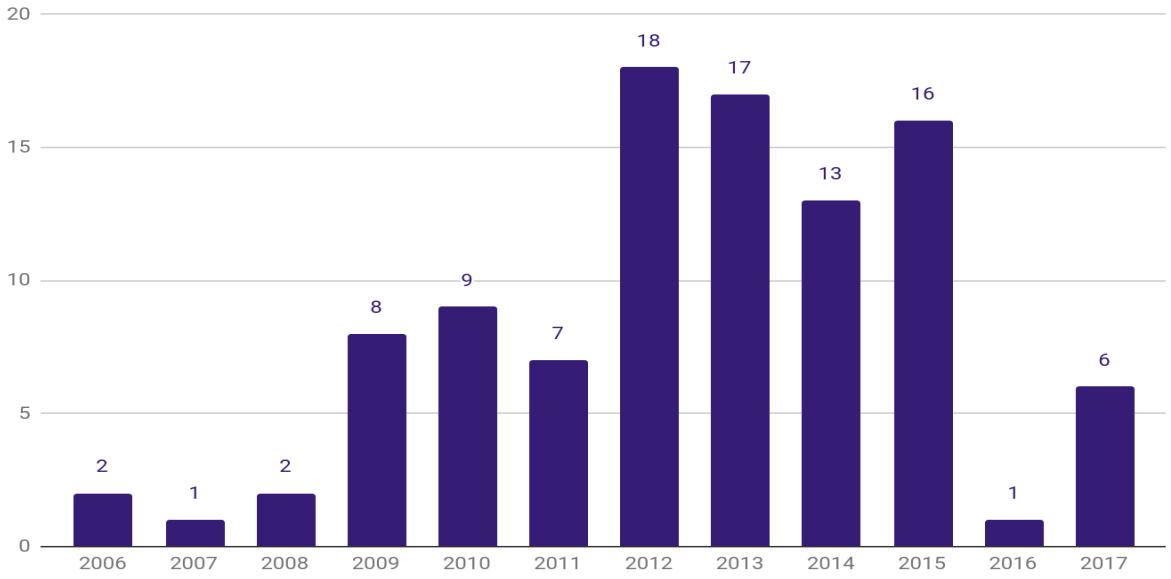
Figure 4 – Cyber offensive acquisition from third party vendors (2008-2020)



Source: Izycki, Eduardo

The purchasing of cyber offensive capabilities presents a similar pattern of increases over the years compared to APTs. Unfortunately, the acquisition data is unknown in several cases. Furthermore, this information was dependent on data breaches and public reporting, both of which occur with a considerable delay.

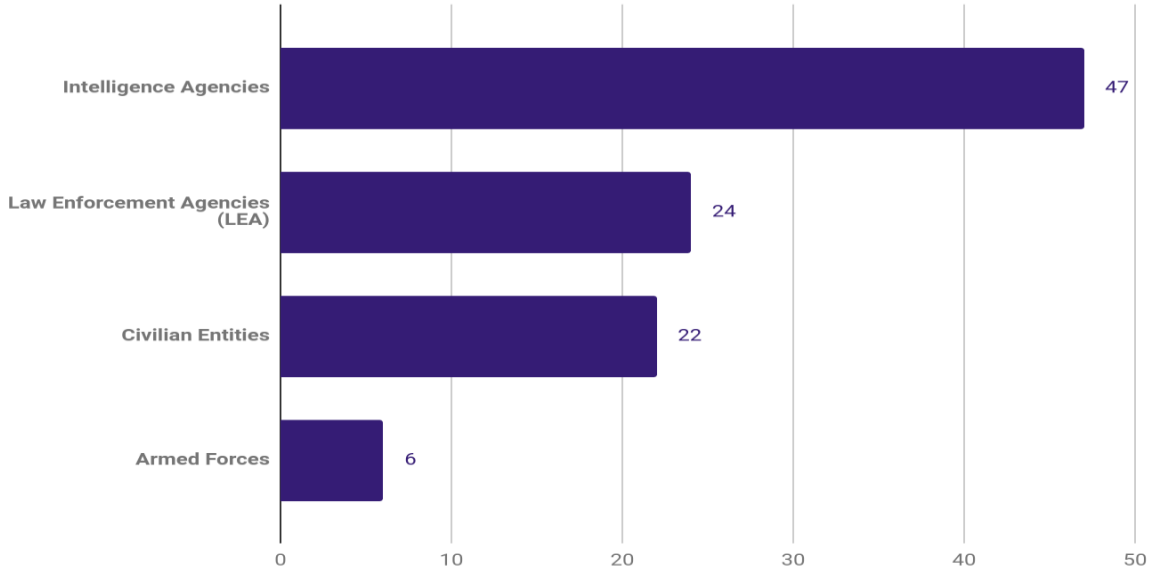
Figure 5 – Cyber offensive acquisition yearly distribution (2008-2020)



Source: Izycki, Eduardo

The dataset also provides evidence that allows us to speculate about the intent of offensive cyber capabilities acquisition. In 99 cases, it was possible to identify the national entity responsible for the purchase. This research classified entities in four categories: Law Enforcement Agencies (LEA), Intelligence Agencies, Armed Forces, and Civilian Entities.

Figure 6 – Cyber offensive acquisition customer distribution (2008-2020)



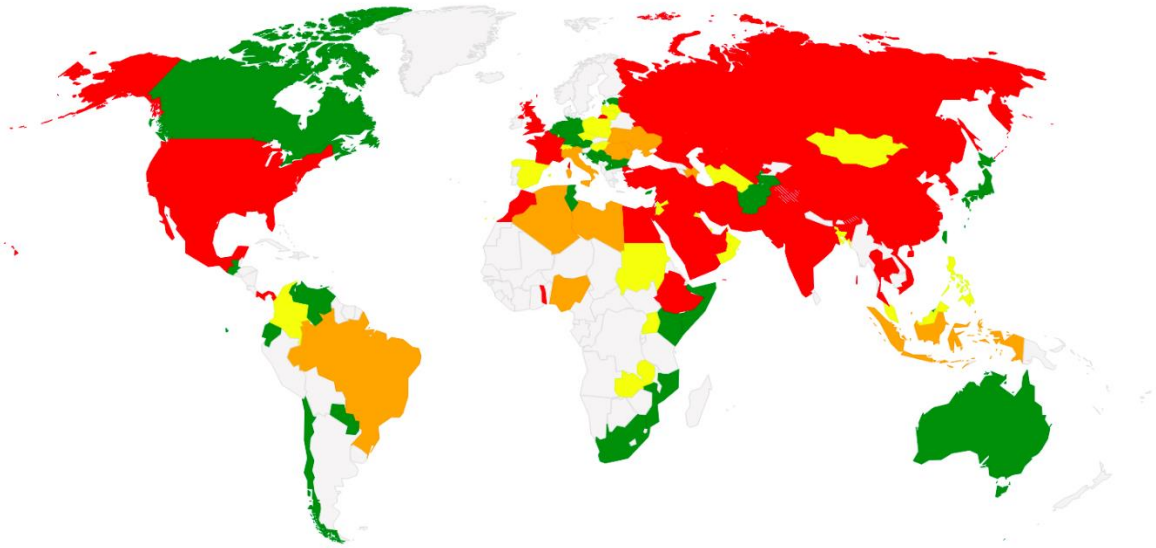
Source: Izycki, Eduardo

Intelligence Agencies (47) and Armed Forces (6) are purchasing offensive cyber capabilities which strongly suggest the extraterritorial use of those assets. Arguably, even LEA could operate outside their own borders. However, that is less likely given the judicial oversight regarding their use (at least nominal).

The civilian entities that acquired offensive cyber capabilities are mostly related to ministries of telecommunications, finances, and local governments. Therefore, it is unlikely that their regular use would result in extraterritorial consequences.

The following picture portrays a map where all the 95 countries identified by this research data are presented. The countries with at least one state-sponsored APT (red), countries with at least one APT from a domestic threat-actor (orange), countries with multiple purchases (yellow), and countries with at least one acquisition (green). In the cases where countries fit in more than one category, the country is presented by the color scale (from red to green).

Figure 7 – Global summary of Nation-State cyber offensive capabilities (2008-2020)



Source: Izycki, Eduardo

The landscape displays an abundance of Nation-States with offensive cyber capabilities. Over the last decade, the number of players, capacity, and intent has become more noticeable. The next sections will address different phenomena (such as targeting, objectives and complexity).

7. Nation-State Cyber Offensive Actions

This section is dedicated to an in-depth analysis of offensive cyber actions attributed to Nation-States. The state-sponsored threat actors, target geographical dispersion, the preferred sectors, the actions complexity, and the purpose of the attacks will be addressed in detail.

7.1. *Threat Actors*

As explained in the methodology section, threat actors are classified based on different methodologies. They represent groups of intrusive activities that may occasionally overlap but are useful for analytical purposes.

The following table illustrates the number of state-sponsored threat-actors identified (first column) within the dataset and the total documents indexed to each country (second column). The proportion of threat-actors and documents indicates the available information regarding threat-actors, i.e., the bigger the number of documents, the more details regarding that country's offensive cyber actions.

The numbers display the traditional countries occupying the top of the table (China, Iran, Russia, United States, North Korea, and Israel). There are 14 countries in an intermediate position that display more than one active threat actor supported by a few documents. The last 9 countries have a single threat actor identified, and the documents all relate to a single deployed campaign.

Table 3 – Number of threat actors and documents related (2008-2020)

Country	Threat Actors	Documents
China	42	75
Iran	12	38
Russia	12	48
United States	6	13
North Korea	4	32
Israel	3	6
Kazakhstan	3	3
Ethiopia	3	5
Lebanon	3	3
Egypt	3	4
Pakistan	3	8
United Arab Emirates (UAE)	2	4
India	2	3
South Korea	2	2
Syria	2	3
Turkey	2	5
United Kingdom	2	6
Vietnam	2	5
France	1	3
Uzbekistan	1	2

Source: Izycki, Eduardo

The number of state-sponsored threat actors is the first key indicator regarding countries' behavior in cyberspace. It signals the offensive diversity displayed by the country since they represent different intrusions techniques. Thus, countries with a bigger number of threat groups are considered offensively more capable.

It should not be taken as an absolute measure because it depends on uncovering a threat-group in action. The numbers reflect only the known threat-actors and those that were attributed as state-sponsored. Thus, other countries may be on the list, and the actual number of actors is much higher for the countries already on the list.

7.2. *Indigenous Technology or Outsourcing*

Another difference regarding the state-sponsored threat-actors is the deployment of indigenous technology or outsourced offensive capabilities.

A cluster of countries whose threat-actors develop or adapt publicly available artifacts to perform cyber offensive actions. The decision to use public tools often shared with cybercriminal non-state actors is a conscious decision to conceal the threat-actor origin. Using the same backdoors and malware, state-actors intend to blend in, using false-flags and a more challenging attribution process (Bartholomew and Guerrero-Saade 2016).

The second group of countries deployed acquired solutions from private vendors and later self-made cyber offensive technology. Countries first acquired and then developed their own tools suggesting that there is a maturing process regarding the use and development of cyber offensive capabilities among nations.

The third tier comprises countries that deployed offensive capabilities from private vendors or completely outsourced the offensive actions performed on their behalf. This is the case in Kazakhstan (Hunter 2016), UAE (Bing and Schectman 2019), Iraq (Senft, Dalek, et al. 2014), Yemen (2018), and Thailand (CitizenLab 2014).

Table 4 – Indigenous or outsourced cyber offensive capabilities (2008-2020)

Indigenous	Both Uses	Outsourced	
China,	Lebanon,	Kazakhstan,	Iraq,
Russia,	India,	Ethiopia,	Yemen,
United States,	Pakistan,	Egypt,	Bahrain,
North Korea,	Vietnam,	Morocco,	Thailand,
United Kingdom,	Turkey,	UAE,	Panama,
Iran,	South Korea,	Mexico,	Togo
Israel,	Syria,	Saudi Arabia,	
France	Uzbekistan		

Source: Izycki, Eduardo

This three-layer level suggests that there is a difference regarding the autonomy of offensive cyber capabilities. The development of local technology suggests that these countries

would customize their tools to engage particular targets. Moreover, they could sustain trade embargos or hostilities and continue to engage in offensive cyber actions. The lower level is dependent on third-parties, most of the western nations, that could disable the necessary infrastructure for the deployment of offensive tools, rendering them inoperative.

7.3. *Target's Geographical Dispersion*

A second key indicator extracted from the dataset of state-sponsored APTs is the target's geographical dispersion. With the use of natural language processing, the research produced a list of threat actor's targets.

By grouping threat actors to their state-sponsored government, the research accomplished/created a target geographical dispersion landscape. The following table illustrates the total of unique targeted countries, the most frequently targeted country, and the region most targeted by each country (the sum of referenced attacks against multiple countries).

Table 5 – State-sponsored geographical distribution (2008-2020)

Country	Country's Region	Unique Targets	Most Frequent	Prevalent Region	Total Targets
Russia	Europe	74	Ukraine	Europe	204
United States	Americas	68	Iran	Europe	121
North Korea	Southeast Asia	64	South Korea	Southeast Asia	175
China	Southeast Asia	61	China	Southeast Asia	316
United Kingdom	Europe	61	China	Europe	86
Iran	MENA	47	Iran	MENA	179
Ethiopia	Africa	25	Ethiopia	Africa	31
Lebanon	MENA	23	Lebanon	MENA	24
Israel	MENA	21	Iran	Southeast Asia	31
Syria	MENA	21	Syria	MENA	24
France	Europe	19	Iran	MENA	26
Turkey	MENA	16	Syria	MENA	23
Pakistan	Southeast Asia	15	India	Southeast Asia	28
Vietnam	Southeast Asia	13	Vietnam	Southeast Asia	40
Saudi Arabia	MENA	12	Saudi Arabia	MENA	22
UAE	MENA	11	UAE	MENA	17
South Korea	Southeast Asia	9	North Korea	Southeast Asia	9
Kazakhstan	Central Asia	7	Kazakhstan	Europe	10
Mexico	Americas	5	Mexico	Americas	14
India	Southeast Asia	4	Pakistan	Southeast Asia	5
Bahrain	MENA	2	Bahrain	MENA	2
Egypt	MENA	2	Egypt	MENA	4

Morocco	MENA	2	Morocco	MENA	4
Panama	Americas	2	Panama	Americas	2
Yemen	MENA	1	Yemen	MENA	2
Iraq	MENA	1	Iraq	MENA	2
Thailand	Southeast Asia	1	Thailand	Southeast Asia	1
Togo	Africa	1	Togo	Africa	1
Uzbekistan	Central Asia	1	Uzbekistan	Central Asia	2

Source: Izycki, Eduardo

The top 6 countries attacked more than 45 unique countries, displaying a global distribution of targets and an impressive number of total attacks (over 85 targets). They are Russia, the United States, North Korea, China, the United Kingdom, and Iran.

A second cluster of countries is discernible. Their most frequent targets are foreign countries, an indication of extraterritorial behavior. Despite that, their behavior appears regionally oriented as their prevalent region is the one in which they are located. They are Lebanon, Israel, Turkey, Pakistan, France, Vietnam, India, and South Korea. France and Lebanon are the only two countries that attacked more frequently outside their region (MENA and Europe, respectively).

The third tier of countries are internally oriented, i.e., the most common target is located within their borders, and when the attacks were extraterritorial, the person/institution targeted was national. That is Ethiopia, the UAE, Syria, Mexico, Kazakhstan, Bahrain, Egypt, Morocco, Panama, Yemen, Iraq, Thailand, Togo, and Uzbekistan.

Additional insight is the strong correlation (25/29 - 86%) between the attacker's origin and its preferred target region.

If focused on the target, the results are somewhat similar. Considering the origin of the target and its most frequent attackers, in 51/82 countries (62.2%), most attackers are from the same region. And 11 of those countries have threat-actors from their own country as the most frequent attacker. The own state-sponsored attacks are the most common.

This evidence suggests that offensive cyber actions appear to be heavily influenced by geography and geopolitical imperatives.

7.4.*Preferred Targeted Sectors*

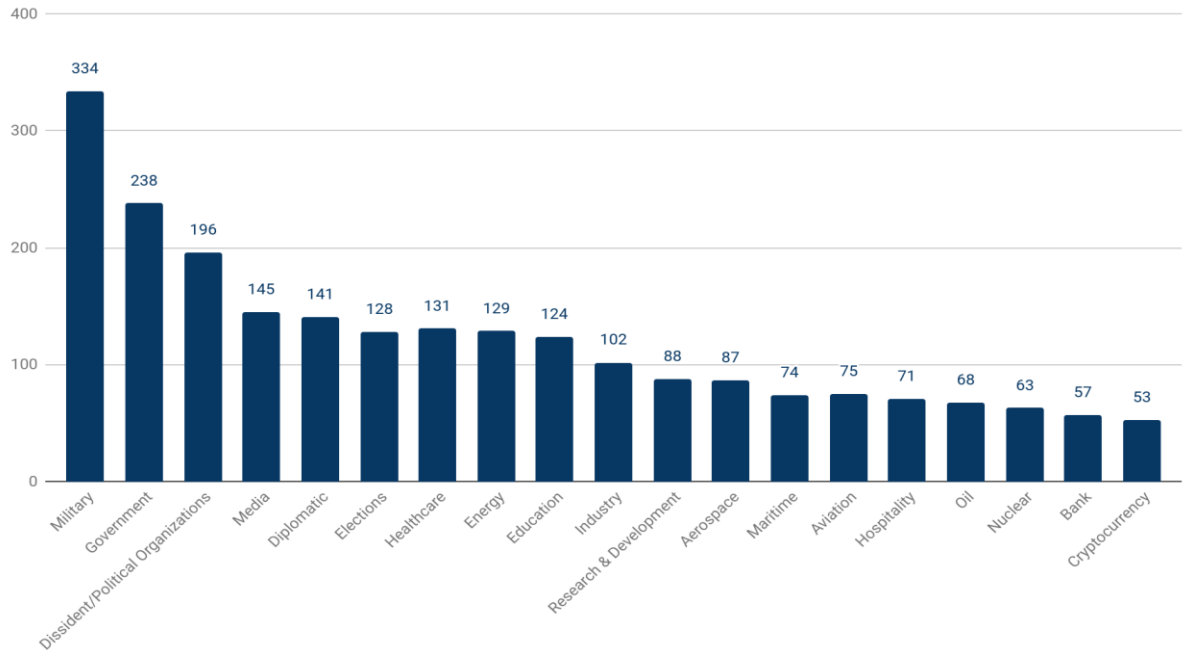
The third key indicator produced from the dataset of state-sponsored APTs is the most targeted sector. Once again, with natural language processing, the research produced a list of economic and organizational sectors most frequently the target of state-sponsored APTs.

The Malware Information Sharing Platform (MISP), an initiative carried out by the Computer Incident Response Center Luxembourg (CIRCL), was the basis for the classification of APTs attacks regarding its preferred sectors. MISP is an open-source framework used by more

than 6000 entities, and it is a benchmark for information sharing of threat intelligence, including cybersecurity indicators.

The most frequently targeted sectors are represented in the following table. The fact that Military, Government, Diplomatic, and Elections are at the top 6 targeted sectors illustrates how nation-states APTs target other government functions.

Figure 8 – State-sponsored APTs targeted sector distribution (2008-2020)



Source: Izycki, Eduardo

Delving into data extracted from the state-sponsored APTs dataset, the following table aggregates the sectors most commonly targeted per country.

Table 6 – Preferred targeted sectors distributed by country (2008-2020)

Countries	Preferred Sectors (Referenced Documents)
Russia	Government (62), Dissident (43), Military (98), Diplomatic (51), Elections (46)
United States	Government (4), Military (8), Energy (4), Research & Development (4), Nuclear (7)
North Korea	Government (15), Military (32), Aerospace (14), Cryptocurrency (18)
China	Government (62), Dissident/Political Organizations (52), Military (89), Healthcare (50)
United Kingdom	Government (3), Military (4), Nuclear (3)
Iran	Government (30), Military (32), Energy (23)
Ethiopia	Dissident/Political Organizations (4), Media (3)
Lebanon	Ten sectors tied (2)
Israel	Military (7), Industry (9), Nuclear (8)

Syria	Government (3), Dissident/Political Organizations (3)
Turkey	Government (5), Military (4)
Pakistan	Government (7), Military (15), Diplomatic (7)
Saudi Arabia	Government (4), Dissident/Political Organizations (5), Media (4)
UAE	Government (6), Dissident/Political Organizations (9), Military (6), Media (7)
South Korea	Dissident/Political Organizations (2), Elections (2)
Kazakhstan	Dissident/Political Organizations (3)
France	Hospitality (2), Media (3), Oil (2)
Vietnam	Dissident/Political Organizations (7), Maritime (6)
Mexico	Government (9), Dissident/Political Organizations (11), Healthcare (9), Media (10)
India	Military (10), Diplomatic (4), Education (4), Energy (4), Media (4), Elections (4)
Bahrain	Dissident/Political Organizations (2), Media (2)
Egypt	Dissident/Political Organizations (5)
Morocco	Dissident/Political Organizations (4), Media (3)
Panama	Dissident/Political Organizations (1), Military (1), Maritime (1), Elections (1)
Yemen	Twelve sectors tied (2)
Iraq	Government (2), Education (2), Oil (2), Elections (2)
Thailand	Dissident/Political Organizations (2), Media (2)
Togo	Dissident/Political Organizations (1)
Uzbekistan	Dissident/Political Organizations (2)

Source: Izycki, Eduardo

The sector's target is an interesting variable to relate to targets' geographical dispersion and attacks' purposes to identify Nation-State patterns in cyberspace.

7.5.*Actions Complexity*

Another key indicator resulted from the state-sponsored APTs analysis is the action complexity. It is based on the CVE (Common Vulnerabilities and Exposures), the Common Vulnerability Scoring System (CVSS), and the use of zero-day exploits.

The MITRE Attack is a knowledge base built as an open-source project to describe tactics and techniques observed in real-world attacks. The framework describes threat-actors behavior to prepare for a robust security process (MITRE Corporation 2017). This research uses the number of different tactics and techniques performed by threat-actors as an indicator of their ability to perform multiple actions. Thus, the bigger the number, the more versatile the threat actors are and more capable of offensive cyber actions.

The CVE is a database of publicly disclosed cybersecurity vulnerabilities. The vulnerabilities are classified according to a CVSS. The vulnerability ratings (Critical, High, Medium, and Low) are commonly used to prioritize vulnerability remediation activities.

The CVSS considers the attack vector, attack complexity, privileges required, user interaction, scope, and impact metrics (availability, integrity, and confidentiality). The less complex the attack and the more damage it causes, the higher its CVSS score.

This research uses the vulnerabilities ratings to measure threat actors' ability to leverage their offensive capabilities to conduct offensive cyber actions.

The third factor considered is the reference of the use of zero-day vulnerabilities in cyber offensive actions. A zero-day (also referred to as 0-day) is a vulnerability (a software or hardware flaw) that is only known by a threat-actor. The threat-group can be identified or purchased in the thriving exploit market, usually at a prohibitive cost. This research considers the reported use of a zero-day to indicate sophistication level or financial resources availability.

After identifying those indicators in the original report sources, the threat actors were grouped according to their state-sponsored country. Countries with more identified threat-groups tend to have more CVE's explored over time. Thus, simply counting is not enough. An additional layer to the analysis is the proportion of the most severe CVE's being exploited. Threat-actors that exploit unique vulnerabilities are more versatile, and the ones that explore more severe vulnerabilities are considered more capable of offensive attacks.

The following table displays the proportion of CVE according to their rating by CVSS standards. This evaluation is performed by NIST (National Institute of Standards and Technology).

Table 7 – Countries CVE rating count (2008-2020)

Country	Critical	High	Medium	Low
Russia	101	36	7	0
China	82	31	12	3
North Korea	45	28	0	0
India	20	10	0	0
United States	14	3	5	0
Israel	10	3	3	0
Ethiopia	8	0	0	0
Turkey	8	3	2	0
United Kingdom	7	0	0	0
Kazakhstan	6	0	0	0
Mexico	5	0	0	0
Saudi Arabia	5	0	0	0
Morocco	5	0	0	0
South Korea	5	0	0	0
Panama	5	0	0	0
Egypt	5	1	0	0
UAE	5	2	1	0

Uzbekistan	5	3	0	0
Pakistan	5	4	0	0
France	3	0	0	0
Iran	3	11	1	1
Vietnam	0	3	0	0
Yemen	0	2	1	1

Source: Izycki, Eduardo

Moreover, the average difference between reported exploitation and the CVE registry year is also similar across countries. New CVE's tend to be explored by sophisticated actors, given that an exploit needs to be created for exploitation.

Table 8 – Total number of CVE's and average age (2008-2020)

Country	CVE's	Average
Russia	145	2,05
China	134	2,63
North Korea	74	2,61
India	31	2,10
United States	22	2,55
Iran	19	1,74
Israel	16	1,94
Turkey	13	2,77
Pakistan	9	3,67
Ethiopia	8	2,75
UAE	8	1,63
Uzbekistan	8	1,63
United Kingdom	7	3,00
Kazakhstan	6	2,33
Egypt	6	3,00
Mexico	5	2,60
Saudi Arabia	5	2,60
Morocco	5	2,60
South Korea	5	2,60
Panama	5	2,60
Yemen	4	8,75
France	3	3,67
Vietnam	3	1,33

Source: Izycki, Eduardo

This suggests that offensive actions are performed by exploiting recent CVE's in a reproduced pattern among countries (except for Yemen).

All countries showed a tendency to explore Critical or High-level CVE's. This evidence suggests that despite differences in the number of threat-groups and volume of CVE's explored, the offensive cyber actions are similar regarding their severity.

7.6. *Attacks Objectives*

The final key indicator concerns the attack's objectives. This indicator addresses the offensive cyber actions impact: espionage, surveillance, disinformation, sabotage, and financial purposes.

The same offensive cyber techniques can produce different outcomes. A threat-group can perform an offensive technique against a target that equally enables espionage, surveillance, and sabotage. In fact, discerning what exactly happened after an offensive cyber action requires extensive forensic work.

The following table presents the consequences of the attacks as observed in each technical report. The same threat-actor performed attacks with different goals given a long time of activity. The threat-actors are grouped according to their country of origin.

Table 9 – State-sponsored APTs objectives dispersion by country (2008-2020)

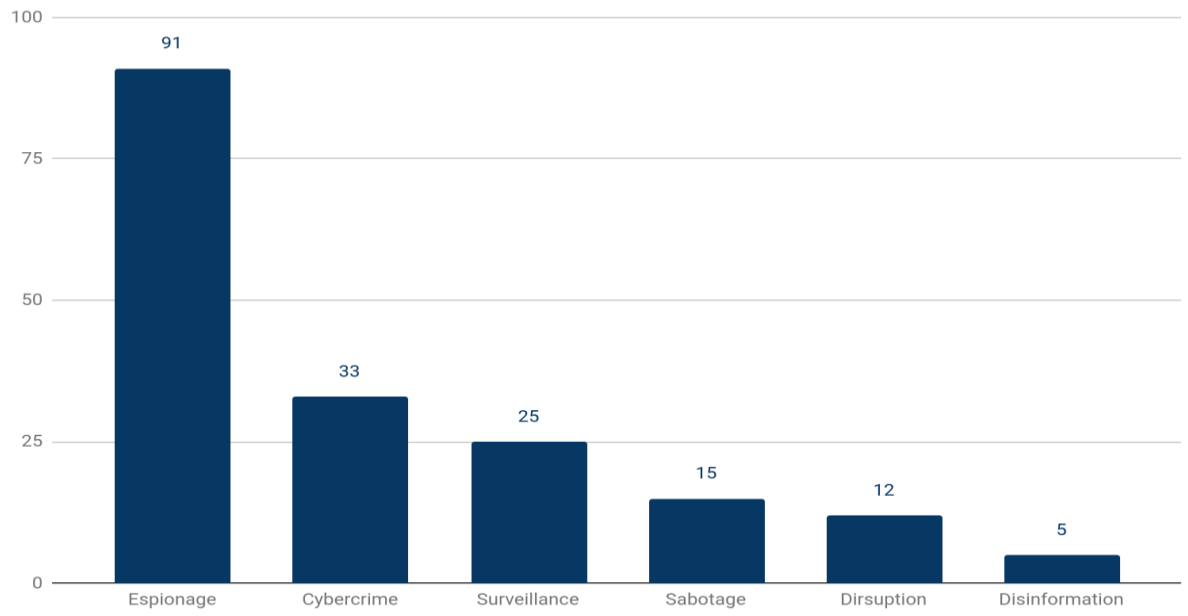
Country	Espionage	Surveillance	Disruption	Disinformation	Sabotage	Cybercrime
China	23	5	4	1	0	10
Iran	13	2	1	2	1	3
Russia	12	0	3	2	6	9
North Korea	6	0	3	0	5	7
United States	6	0	0	0	1	0
United Kingdom	5	0	0	0	0	0
Pakistan	4	0	0	0	0	2
Turkey	3	0	0	0	0	1
France	3	0	0	0	0	0
UAE	2	1	0	0	0	0
Lebanon	2	1	0	0	0	0
Mexico	1	1	0	0	0	0
Vietnam	1	1	1	0	0	0
Ethiopia	1	1	0	0	0	0
Kazakhstan	1	1	0	0	0	0
Saudi Arabia	1	1	0	0	0	0
Bahrain	1	1	0	0	0	0
Uzbekistan	1	1	0	0	0	0
Israel	1	0	0	0	2	0

India	1	0	0	0	0	1
South Korea	1	0	0	0	0	0
Yemen	0	2	0	0	0	0
Egypt	0	1	0	0	0	0
Syria	0	1	0	0	0	0
Morocco	0	1	0	0	0	0
Iraq	0	1	0	0	0	0
Thailand	0	1	0	0	0	0
Togo	0	1	0	0	0	0
Panama	0	1	0	0	0	0

Source: Izycki, Eduardo

Acts of espionage (91) are more frequently observed among countries. Followed by cybercriminal activities (33) and surveillance (25). The two outcomes related to "real-world" consequences: sabotage (15) and disruption (12) represent a small number of threat-actor's actions. Finally, disinformation (5) is not frequently related to APTs attacks, thus there are a small number of occurrences.

Figure 9 – State sponsored APTs distribution according its objectives



Source: Izycki, Eduardo

The data provides a first insight regarding offensive cyber actions. Threat-actor's objectives are mostly related to cyber consequences, whereas results that produce some effect in the "real-world" are less common (14,9%). The results are backed up by previous research

undertaken by Izycki and Vianna (2021), where they demonstrated that kinetic results are unusual in offensive cyber actions.

8. Cyber Offensive Capabilities Acquisition

This section focuses on the acquisition of offensive cyber capabilities by Nation-States from private providers. The dataset was built from reports, vendors' data breaches and national export controls issued licenses.

This research considered a set of 12 private vendors as providers of offensive cyber capabilities: Amesys, Area SpA, Cyberbit, Dreamlab, Elbit, FinFisher, Hacking Team, Sandvine, NICE Systems, NSO Group, SS8, and Trovicor. A brief analysis of each provider is available in Appendix A

Table 10 – Cyber offensive capabilities private vendors and distribution by region (2008-2020)

	Africa	Americas	Central Asia	Europe	MENA	Southeast Asia
Amesys	0	0	0	0	2	0
Area SpA	0	0	0	0	2	0
Cyberbit	2	0	2	0	0	2
Dreamlab	0	0	1	0	1	0
Elbit	1	0	0	0	0	0
FinFisher	7	6	3	18	10	11
Hacking Team	5	21	4	13	13	6
Sandvine	2	0	1	0	7	2
NICE Systems	2	1	2	0	0	0
NSO Group	4	3	2	5	5	0
SS8	0	2	0	0	1	1
Trovicor	1	0	1	0	6	1
TOTAL	**24**	**33**	**16**	**36**	**47**	**23**

Source: Izycki, Eduardo

The table reflects 179 identified purchases from private vendors from 2006 to 2017. The most prolific sellers are Hacking Team (Italy), FinFisher (UK/Germany), and NSO Group (Israel). In Appendix A, there is a further profiling on each provider and its advertised services.

The providers of offensive cyber capabilities are all from western countries. This contradicts the dominant narrative that Chinese technology is the enabler for digital authoritarianism. The evidence points to western companies providing the tools for offensive cyber actions against the civilian population and foreign governments (in some cases, including their own country of origin).

Table 11 – Cyber offensive capabilities sales according to the private vendor's origin (2008-2020)

Country Name	Total
Germany	64
Italy	63
Israel	31
Canada	12
United Kingdom	11
United States	4
Switzerland	2
France	2

Source: Izycki, Eduardo

These results do not deny the use of Chinese technology to engage in surveillance operations, there are frequent publications by Amnesty International and other ONGs describing human rights violations in the Xinjiang province. For instance, the Australian Strategic Policy Institute has research that lists 164 sales of technology from Chinese companies abroad (2019). These results were not incorporated into this research because the definition of surveillance adopted by the Australian institute does not match with our own.

A total of 85 different countries purchased at least one piece of software or service provided by one of the aforementioned private providers. The complete list of each country's purchases is included in Appendix B.

8.1. *Multiple Acquisitions*

One of the most striking figures is the number of countries that acquired more than a single offensive solution. The 45 countries are listed below with the respective number of purchases observed.

Table 12 – Countries with cyber offensive capabilities multiple acquisition (2008-2020)

Nome	Region	Purchases
Mexico	Americas	13
UAE	MENA	8
Egypt	MENA	7
Saudi Arabia	MENA	6
United States	Americas	5
Kazakhstan	Central Asia	5
Bahrain	MENA	5
Nigeria	Africa	5
Oman	MENA	5

Ethiopia	Africa	4
Uzbekistan	Central Asia	4
Hungary	Europe	4
Pakistan	Southeast Asia	3
Turkey	MENA	3
Syria	MENA	3
Morocco	MENA	3
Thailand	Southeast Asia	3
Panama	Americas	3
Qatar	MENA	3
Singapore	Southeast Asia	3
Spain	Europe	3
Malaysia	Southeast Asia	3
Italy	Europe	3
Sudan	Africa	3
Lebanon	MENA	2
Vietnam	Southeast Asia	2
India	Southeast Asia	2
Philippines	Southeast Asia	2
Zambia	Africa	2
Yemen	MENA	2
Indonesia	Southeast Asia	2
Mongolia	Central Asia	2
Bangladesh	Southeast Asia	2
Switzerland	Europe	2
Kuwait	MENA	2
Czechia	Europe	2
Lithuania	Europe	2
Uganda	Africa	2
Luxemburg	Europe	2
Latvia	Europe	2
Turkmenistan	Central Asia	2
Honduras	Americas	2
Jordan	MENA	2
Poland	Europe	2
Colombia	Americas	2

Source: Izycki, Eduardo

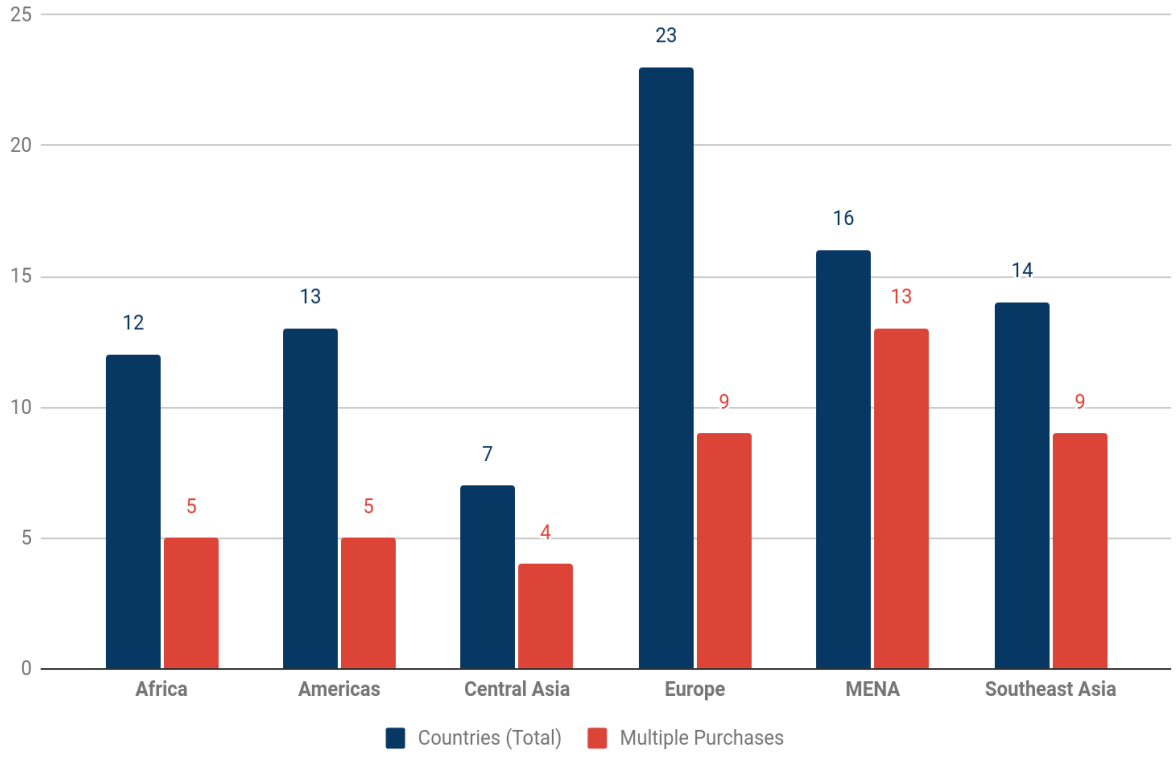
This research assumes that the repeated purchases are evidence of the intensive pursuit of offensive cyber capabilities within countries. In three regions, there is a concentration of multiple acquisition countries: Central Asia, MENA, and Southeast Asia.

The acquisition of multiple offensive cyber solutions suggests that the countries acquiring them intend to expand their repertoire since private vendors have different strategies to compromise targets and explore different vulnerabilities (Teach 2020).

Thus, even advanced offensive cyber capabilities - exploring a zero-day vulnerability - might not be useful against the desired target if it is not vulnerable or does not have a particular hardware or software set-up. Hence, the willingness of countries to acquire offensive artifacts from more than one private vendor is considered as evidence of intent to perform offensive cyber actions.

Unlike conventional weaponry, where interoperability is a requirement, offensive cyber capabilities can and often operate independently. Moreover, a threat-actor can use one artifact to compromise the target and another (from a different provider) to extract information (espionage) or send disruptive payloads (ransomware).

Figure 10 – Cyber offensive capabilities acquisition by region (2008-2020)



Source: Izycki, Eduardo

The cost of acquisition varies from the extension of services acquired. Still, the Remote-Control Service (also known as Galileo), provided by Hacking Team, cost less than 1 million dollars and yearly maintenance was lower than 200 thousand dollars (on average - reference to 2013/2014). This indicates that the cost of acquisition for a state-of-the-art offensive cyber solution is negligible for a nation-state.

8.2. *Customers*

The sources gathered during this research allowed for the identification of customer acquisition on 99 occasions. The Hacking Team (WikiLeaks 2015) and FinFisher (WikiLeaks 2014) data breaches provided a colossal amount of information regarding commercial activities (e-mails exchange, balance spreadsheets, customers list).

The Citizen Lab reports (Munk School of Global Affairs & Public Policy, University of Toronto) were another instrumental resource for identifying the customer and stocktaking offensive cyber capabilities.

This research classified entities in four categories: Law Enforcement Agencies (LEA), Intelligence Agencies, Armed Forces, and Civilian Entities.

Table 13 – Cyber offensive capabilities acquisition distribution according customer (2008-2020)

Entities	Purchases
Intelligence Agencies	47
Law Enforcement Agencies (LEA)	24
Civilian Entities	22
Armed Forces	6

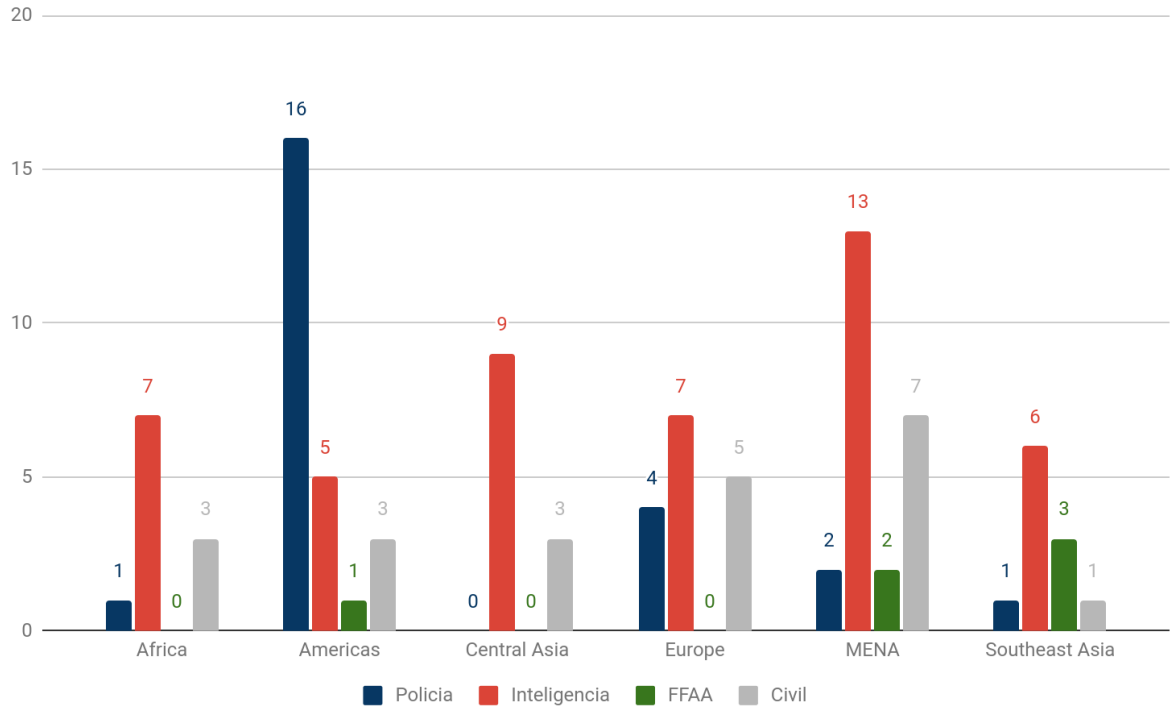
Source: Izycki, Eduardo

Intelligence agencies are the top customers in every region, except in the Americas where Mexico LEA made purchases on 13 different occasions (J. e. SCOTT-RAILTON 2017) (SCOTT-RAILTON, et al. 2017). This is an indication of intent to surreptitiously use the acquired offensive cyber capabilities.

Moreover, generally, intelligence agencies do not have extensive oversight from the Judicial branch and Attorney General in most countries, which is an additional cause for concern over its use.

Further, intelligence agencies and armed forces are focused on external targets. This suggests that the proliferation of offensive cyber capabilities over time increases the likelihood of extraterritorial use and the risk of cyber skirmishes.

Figure 11 – Acquisition distribution according customer and region (2008-2020)



Source: Izycki, Eduardo

Most customers' profile indicates that the use of offensive cyber capabilities is an expression of intent to project power externally.

9. DISCUSSION

The data presented in the last section is the empirical evidence that supports the discussion and analysis presented in this section. The data concerning state-sponsored APT is a reliable indicator of intent and capability. The data gathered from offensive cyber capability acquisition is trustworthy evidence of nation states' intent.

This section presents conclusions based on the empirical data gathered. The first point is that there is an unprecedented diffusion of power among the countries compared in regard to their offensive capabilities in a conventional conflict. Moreover, offensive capabilities are not constrained to six "traditional" cyber powers but a roster of over twenty countries (Voo, et al. 2020).

9.1. *Diffusion (not equality) of Cyber Offensive Capabilities*

Conventional wisdom suggests that there are only a handful of countries with meaningful offensive cyber capabilities. Four variables from this research demonstrate that there is unprecedented diffusion of offensive cyber capabilities:

- The existence of state-sponsored threat-actors in 29 different countries
- The small role of countries with indigenous capabilities
- The similar complexity displayed in cyber attacks
- The acquisition of cyber offensive solutions by additional 66 countries

This research demonstrates that there is evidence that 29 countries are already engaged in state-sponsored offensive cyber actions. Though their complexity is similar (in terms of CVE's), only a small group of countries displayed autonomous capabilities of developing or customizing their own offensive cyber tools.

The complexity of the offensive actions is evidence that countries possess similar capabilities in terms of vulnerabilities exploited during state-sponsored APTs. All countries exploited 50% or more CVE's considered critical or high.

Table 14 – CVE's severity according to country (2008-2020)

Country	Critical	High	Medium	Low
Russia	70,1%	25,0%	4,9%	0,0%
China	64,1%	24,2%	9,4%	2,3%
North Korea	61,6%	38,4%	0,0%	0,0%
India	66,7%	33,3%	0,0%	0,0%
United States	63,6%	13,6%	22,7%	0,0%
Israel	62,5%	18,8%	18,8%	0,0%
Ethiopia	100,0%	0,0%	0,0%	0,0%
Turkey	61,5%	23,1%	15,4%	0,0%
United Kingdom	100,0%	0,0%	0,0%	0,0%
Kazakhstan	100,0%	0,0%	0,0%	0,0%
Mexico	100,0%	0,0%	0,0%	0,0%
Saudi Arabia	55,6%	44,4%	0,0%	0,0%
Morocco	62,5%	25,0%	12,5%	0,0%
South Korea	83,3%	16,7%	0,0%	0,0%
Panama	100,0%	0,0%	0,0%	0,0%
Egypt	100,0%	0,0%	0,0%	0,0%
UAE	62,5%	37,5%	0,0%	0,0%
Uzbekistan	100,0%	0,0%	0,0%	0,0%
Pakistan	100,0%	0,0%	0,0%	0,0%
France	18,8%	68,8%	6,3%	6,3%
Iran	100,0%	0,0%	0,0%	0,0%
Vietnam	0,0%	100,0%	0,0%	0,0%
Yemen	0,0%	50,0%	25,0%	25,0%

Source: Izycki, Eduardo

Thus, offensive cyber actions can be deployed by multiple countries. However, only 16 countries are not constrained by external factors: China, Russia, the United States, North Korea, the United Kingdom, Iran, Israel, France, Syria, Lebanon, India, Pakistan, Vietnam, Turkey, South Korea, and Uzbekistan.

This is evidence that the conventional powers will not dominate this dimension as they have done in others, such as air, sea, or land (Nye 2010).

The remaining 79 countries displayed or acquired capabilities to perform offensive cyber actions. Still, they are highly dependent on private providers or third parties responsible for executing the actions themselves.

To have a world-class Navy or Air Force, a country must spend 100 million on a plane, a satellite system over 1 billion, 3 billion on a single combat ship. The cost of offensive cyber capabilities is negligible compared to that (Kramer 2009).

The number of countries capable of engaging in cyberspace is impressive. A comparison with different dimensions would result in a restricted number of potential protagonists at the global level, rendering an unprecedented nation-state competition with a relative reduction of power differentials (Nye 2010).

The preeminence of the United States regarding conventional forces is not observed within offensive cyber capabilities. Even the idea of complete superiority or dominance in this field is highly doubtful.

As the table above displays, countries like China, Russia, North Korea, Turkey, and India display similar CVE severity. This suggests that it is not significant in qualitative terms of offensive capabilities.

There is a level of power diffusion, but in a belligerent scenario where there are trade embargos or hostilities, it is reasonable to conclude that the vast majority of countries would only be able to retain their offensive cyber capabilities if the original provider allowed it to continue. The dependence on private vendors can also be subject to a suspension order by the third-party host nation, in a similar fashion to suspension of ammunition or equipment during a conflict.

Therefore, there is power diffusion but there is not power equality among the several players in cyberspace.

9.2. *Geography Matters*

One of the most singular characteristics of cyberspace is its disregard for borders. This allows any engaging country to mount an offensive cyber action against targets which are physically far from its own territory.

While this allows for a more diverse set of strategic options, this research's empirical evidence suggests that geopolitical goals are a dominating factor for offensive cyber actions. It is ironic that the virtual space is still in large part determined by real-world constraints.

Two variables from this research support this conclusion: the target's geographical dispersion and the acquisition of offensive cyber capabilities.

Considering the countries that performed state-sponsored offensive cyber actions, 86% (25/29) of most of their targets were countries within the same geographical region.

The countries that do not display this behavior are the United States (targeting Europe and Southeast Asia), Israel (Southeast Asia and Europe), France (MENA and Europe), and Kazakhstan (Europe and Central Asia). However, the last two focused their actions on targets in their vicinity: France (Germany, Luxembourg, and Algeria) and Kazakhstan (Russia and Kazakhstan).

Building the relation from the target's perspective ushers similar results. There are 124 countries identified as targets of state-sponsored offensive cyber action. In 41 of them, 3 or fewer actions were registered. Thus, they were not counted for this particular relationship. Considering the remaining 82, in 66% of countries (54), most of the actions are sponsored by a country in the same region.

Table 15 – Geographical distribution of targets related to its attributed origin (2008-2020)

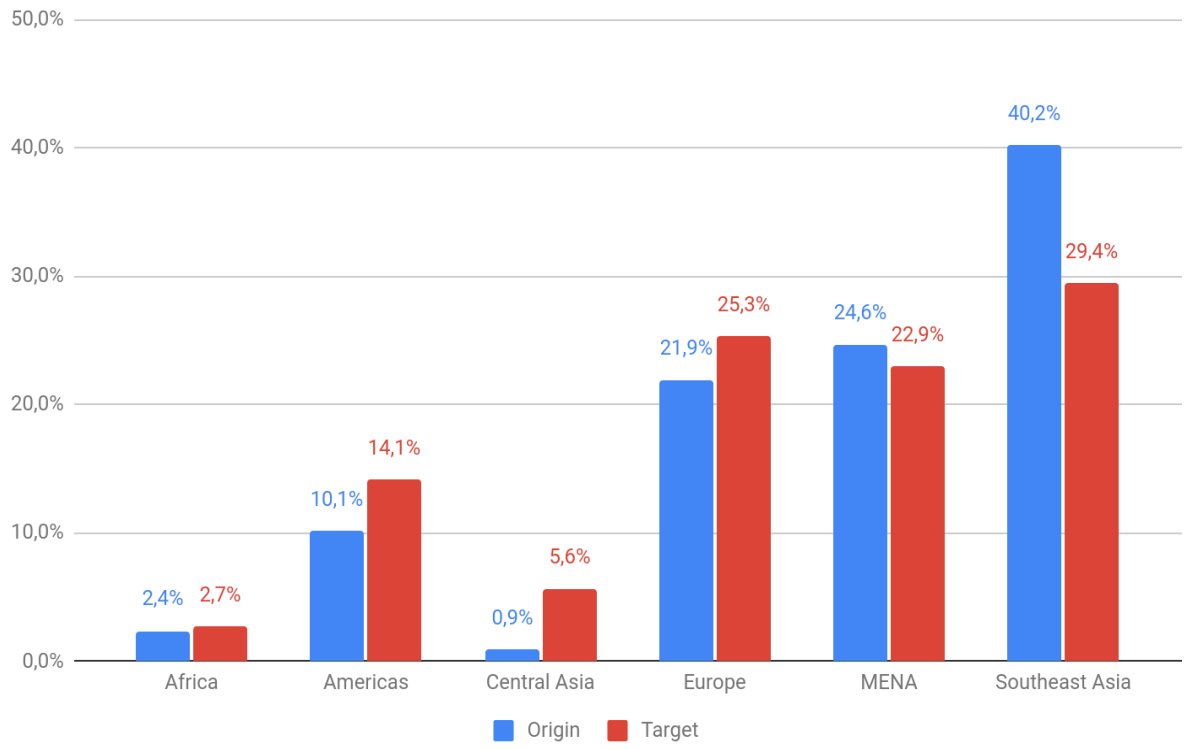
		Targets					
		Africa	Americas	Central Asia	Europe	MENA	Southeast Asia
State-Sponsored Actions	Africa	11	4	0	10	2	5
	Americas	7	31	9	31	29	30
	Central Asia	0	1	5	4	1	1
	Europe	10	37	27	119	53	50
	MENA	0	37	15	63	174	45
	Southeast Asia	8	81	20	116	52	268

Source: Izycki, Eduardo

Further evidence of geopolitical orientation is produced by building a relational matrix from the state-sponsored actions to its preferred targets.

Except for the Americas (two regions tie for first place), every region displays a preference to engage in offensive cyber actions against targets within its own region.

Figure 12 – APTs targets and origins distributed according region (2008-2020)



Source: Izycki, Eduardo

It is important to emphasize that 204/297 of European offensive cyber actions are attributed to Russia, close to 2/3 of the total. Thus, the offensive behavior is heavily influenced by Russian actions.

Further, there is convergence in the data provided by the acquisition of cyber capabilities from the private sector, breaking down by region.

Southeast Asia and MENA regions stand out in total acquisitions, unique countries, multiple purchases, and intelligence / Armed Forces customers.

Table 16 – Purchases, type of customer, and state-sponsored target distribution by region (2008-2020)

Region	Total	Countries	Multiple Purchases	Intelligence / FFAA	State-Sponsored Target
Africa	23	12	5	7	2,7%
Americas	33	13	5	6	14,1%
Central Asia	16	7	4	9	5,6%
Europe	36	**23**	9	7	25,3%
MENA	**54**	16	**13**	**15**	22,9%
Southeast Asia	27	14	9	9	**29,4%**

Source: Izycki, Eduardo

The data gathered confirms the position from Valeriano and Maness that the overwhelming majority of cyber conflicts occur between long-standing rivals seeking to harm each other in the context of regional disputes (Valeriano and Maness 2014).

Although the dataset can provide no causal relationship, the regions that were targeted by a larger number of attacks were more inclined to acquire offensive cyber capabilities. Further study could determine if this is evidence of a cyber-arms race.

9.3.*Profiling Nation-State Behavior*

The data gathered confirms the position from Valeriano and Maness that the overwhelming majority of cyber conflicts occur between long-standing rivals seeking to harm each other in the context of regional disputes (Valeriano and Maness 2014).

Although the dataset can provide no causal relationship, the regions that were targeted by a larger number of attacks were more inclined to acquire offensive cyber capabilities. Further study could determine if this is evidence of a cyber-arms race.

9.3.1. GLOBAL PLAYERS

The first cluster of countries is composed of China, Iran, Israel, Russia, the United Kingdom, and the United States. All six countries have indigenous offensive cyber capabilities. They have a high number of total and unique targets. They engage with high geographical dispersion (across at least five regions). Their objectives with cyber actions are mainly espionage and sabotage, and the preferred sectors are government and military.

Table 17 – Global players main features

Country	Total Targets	Unique Targets	Espionage	Sabotage	Preferred Sectors
China	316	61	23	0	Military (89), Government (62), Dissidents (52)
Russia	204	74	12	6	Military (98), Government (62), Diplomatic (51), Elections (46)
Iran	179	47	13	1	Military (32), Government (30), Energy (23)
United States	121	68	6	1	Military (8), Government (4), Industry (5), Nuclear (7),
Israel	31	21	1	2	Industry (9), Nuclear (8), Military (7)
United Kingdom	86	61	5	0	Military (4), Government (3), Nuclear (3)

Source: Izycki, Eduardo

Despite their similarities, Chinese and Iranian state-sponsored threat-actors also consistently engage in offensive cyber actions with surveillance purposes (respectively 5 and 2).

Another difference relates to the cybercriminal actions performed by Chinese (10), Russian (9), and Iranian (3) state-sponsored threat-actors. This suggests that offensive capabilities are deployed by the same actors against a broad spectrum of targets and the state-sponsored actions are not a full-time commitment.

Moreover, these countries engage in multiple purpose campaigns simultaneously, suggesting they have a significant number of human resources.

The United States and Israel engaged in an offensive cyber action against the Iranian nuclear program (Stuxnet). They unleashed threat-actors for the purposes of espionage, respectively the Equation Group (Falliere, Murchu and Chien 2011) and Duqu 2.0 (Kaspersky 2015)

The United States had another joint venture with the United Kingdom (possibly with other Five Eyes countries). The Snowden leaks revealed that the GCHQ targeted attacks against the G20 Meeting as a state-conducted offensive cyber action (The Guardian 2013).

China used offensive cyber actions to conduct a long-term espionage campaign to speed up its technological development (FireEye 2013). Traditional espionage is also a frequent objective pursued by China through cyber means (Glyer, et al. 2020). Furthermore, there are a significant number of cases where the deployment of surveillance against its own citizens was observed (Amnesty International 2019).

Russia conducts multiple-layer pressure against its geopolitical goals, for instance, pressure on Estonia (Ashmore 2009), denial of service during the Georgian campaign (Georgia 2009), and destabilizing Ukraine (FireEye 2017). Its offensive cyber actions range from attacks

against critical infrastructures, sophisticated disinformation campaigns, and multi-targeted espionage. The actions against the power supply in Ukraine are strong evidence of the versatility of Russian threat-actors, since the knowledge to target industrial protocols was necessary, and it is an unusual skill (Lipovsky 2016).

Iran conducts multiple campaigns against opposition figures, including nationals living abroad and in countries with geopolitical interests (Qatar, Bahrain, Syria, and Lebanon) (Gundert, Chohan and Lesnewich 2018). Simultaneously it engages against its regional rivals (Saudi Arabia - 11, Israel - 11, Turkey - 8, UAE - 7, Iraq - 6) to assert itself within the MENA region (Insikt Group 2019).

This tier demonstrates the ability to engage against different targets with different purposes, denoting versatility and resources to adapt to multiple targets. It is reasonable to assume that innovative actions are not a problem for this group. Thus, cybersecurity initiatives by their targets can be overcome by these threat-actors.

9.3.2. REGIONAL CONTENDERS

The second group of countries is composed of France, India, Lebanon, North Korea, Pakistan, South Korea, Syria, Turkey, UAE, and Vietnam.

These ten countries display some level of self-made offensive cyber capabilities. They have multiple acquisitions of offensive cyber technologies from private vendors. Their actions are regionally oriented. Their objectives with cyber actions are mainly espionage, and the preferred sectors vary according to their own geopolitical imperatives.

Table 18 – Regional contenders main features

Country	Espionage	Purchases	Targets in own region	Most Targeted Countries
France	3	0	33,3%	Iran (4), Algeria (3), Turkey (2), Germany (2)
North Korea	6	0	44,0%	South Korea (30), US (11), India (8), China (7), Russia (7)
Pakistan	4	3	60,7%	India (8), Pakistan (6), Others (1)
Lebanon	2	2	37,5%	Lebanon (4), US (3), Israel (3), Saudi Arabia (2), Jordan (2)
Turkey	3	3	56,5%	Syria (4), Turkey (3), Iraq (2), Albania (2)
Vietnam	1	2	85,0%	Vietnam (9), Cambodia (7) Philippines (6), China (5)
India	1	2	66,7%	Pakistan (6), China (4), Bangladesh (3), Sri Lanka (2)
Syria	0	3	87,5%	Syria (2), Lebanon (2), Saudi Arabia (2)

South Korea	1	1	70,6%	Russia (3), Japan (3) China (2), North Korea (2)
UAE	2	8	70,6%	UAE (3), Qatar (3), Bahrain (2), US (2)

Source: Izycki, Eduardo

Regarding the origins of their cyber offensive capabilities, all countries displayed indigenous development. There were no acquisitions from France and North Korea, though the former has private companies selling technologies worldwide (Amesys/Bull and VUPEN).

France tends to act less regionally contained, targeting Algeria and Germany probably due to their location and historical ties. The actions against Iran and Turkey are aligned with the negotiations for the Iranian Nuclear Deal that involved the three countries in 2015 (ESET 2015).

North Korea has a huge number of unique targets (64), but its offensive cyber actions are strongly skewed towards South Korea (18%) (Sherstobitoff 2013). The actions against countries in other regions were mostly financially motivated against banks (SWIFT System) and cryptocurrency exchanges (Guerrero-Saade and Moriuchi 2017). North Korean threat-actors act as organized cybercriminals, likely to circumvent the several embargoes imposed by the United States (Group-IB 2017).

South Korea also fits the profile of regionally oriented offensive cyber actions. However, the South Korean threat-actor remains shrouded in secrecy since most of the reports described technical details without providing more details on its profile (Tencent 2019).

The case of India (Levene, Grunzweig and Barbehenn 2018) and Pakistan (Falcone, et al. 2018) is a further demonstration of cyber actions' geopolitical orientation. Both countries have a nuclear balance, historically engaged in several skirmishes, and constantly face each other in cyberspace (Inskit Group 2016).

The MENA region is also prolific in examples of regional engagement. Lebanon (Lookout and EFF 2018), Syria (Hasbini, Pontiroli and Saad 2014), and Turkey (Arsene, et al. 2020) display preferential targets within the same region. The Syrian Civil War's intricate consequences are one of the main reasons for these three countries' cyber offensive actions.

The UAE case is unique because its national digital authority hired former employees from the National Security Agency (NSA) to conduct offensive cyber actions. Called Project Raven (Bing and Schectman 2019), the entire technical staff was outsourced, but they were physically in the UAE and constantly supervised by the Emiratis during campaigns against Bahrain, Qatar, and American targets (Bing and Schectman 2019).

Finally, the Vietnam case reaffirms the group's characteristics. Besides a clear targeting of Southeast Asian countries (Wright 2020), the main sectors that Vietnamese threat-actors target was the maritime industry, perfectly aligning with the ongoing tensions in the South China Sea (Lassalle, Koessel and Adair 2017).

All countries in the group, except for Syria, performed offensive actions with the purpose of espionage. But financially motivated actions (North Korea, Pakistan, Turkey, and India) and surveillance operations (Lebanon, Vietnam, and Syria) have also occurred.

The group's similarities reside in the nascent self-made offensive cyber capabilities, the acquisition from third parties, and the focus on targets within the region (actions are not as widespread as in the case of Global Players).

9.3.3. LOCAL PLAYERS

The third cluster of countries is composed of Kazakhstan, Saudi Arabia, Ethiopia, Egypt, Uzbekistan, Morocco, Mexico, Bahrain, Yemen, Iraq, Thailand, Panama, and Togo.

These thirteen countries are dependent on private vendors to acquire or engage in offensive cyber actions. They have multiple providers. Their actions are focused on their own territory and citizens (occasionally targeting nationals abroad), and their objectives with cyber actions are mainly surveillance against dissidents and rival political organizations.

Table 19 – Local players main features

Country	Purchases	Intelligence	Espionage	Surveillance	Political Targeting
Kazakhstan	5	3	1	1	3
Saudi Arabia	6	2	1	1	5
Ethiopia	4	1	1	1	4
Egypt	7	4	0	1	5
Uzbekistan	4	3	1	1	2
Morocco	3	1	0	1	4
Mexico	13	1	1	1	11
Bahrain	5	0	1	1	2
Yemen	2	0	0	2	2 (Tied)
Iraq	0	0	0	1	0
Thailand	3	0	0	1	2 (Tied)
Panama	3	2	0	1	1 (Tied)
Togo	1	0	0	1	1 (Tied)

Source: Izycki, Eduardo

Uzbekistan is the only country that displayed some level of indigenous development of cyber capabilities. The self-made capabilities - threat-actor named SandCat - were uncovered due to the developer's operational security flaw. The State Security Service (SSS) tested the offensive cyber tool in an uncontrolled environment where Kaspersky's anti-virus solution was installed, thus identifying the new malware (Zetter 2019).

All countries from this group show a preference for surveillance operations against citizens from their own countries. That is reinforced by the political targeting performed by all countries, except for Iraq (Senft, et al. 2014). Political targets are considered dissidents, expatriate communities, and rival political organizations or parties.

In Kazakhstan (Galperin, et al. 2016), Ethiopia (Marczak, et al. 2014), Saudi Arabia (Amnesty International 2018), Mexico (Scott-Railton, Marczak, et al. 2017), Morocco (Amnesty International 2019), and Panama (Marczak, Guarnieri, et al. 2014), the extraterritorial actions are targeted against the migrants or expatriate nationals living abroad. This means that offensive cyber actions are motivated by domestic reasons but the effects reach different parts of the world. That is empirical evidence of the strategic advantages introduced by operating in cyberspace.

Finally, despite local interest, this group exhibits intent to engage in cyberspace with multiple means. Twelve countries - excluding Iraq - acquired offensive cyber solutions. Except for Togo (Scott-Railton, Anstis, et al. 2020), all eleven countries acquired multiple solutions, and most of them (8) placed them in intelligence agencies.

9.4. *Building Cyber Offensive Capabilities*

Three interesting cases arise from the profiling of nation-state behavior in cyberspace: Lebanon (Marczak, Scott-Railton, et al. 2015), Turkey (Marczak, Dalek, et al. 2018), and Vietnam (Marquis-Boire, et al. 2013). These countries have acquired offensive cyber solutions from private vendors and later developed their own capabilities.

Offensive cyber capabilities are increasingly becoming efficient tools for countries to compensate their lesser power in other domains (Barrinha and Renard 2020).

The acquisition of third-party solutions precedes the deployment of self-made tools, which suggests that a maturation process is in place. There is no evidence of reverse engineering or technology transfer. Nevertheless, in all three cases, countries displayed progression with similar targeting and objectives patterns.

Table 20 – Lebanon, Turkey, and Vietnam comparison

	Lebanon	**Turkey**	**Vietnam**
Acquired Solutions	**Gamma International, FinFisher** - 2015 By the General Directorate of General Security (Intelligence Agency) and	**Hacking Team**, 2011 By the Turkish National Police	**Hacking Team**, 2011 By the Vietnam GD1 (Military Intelligence) **Gamma International**,

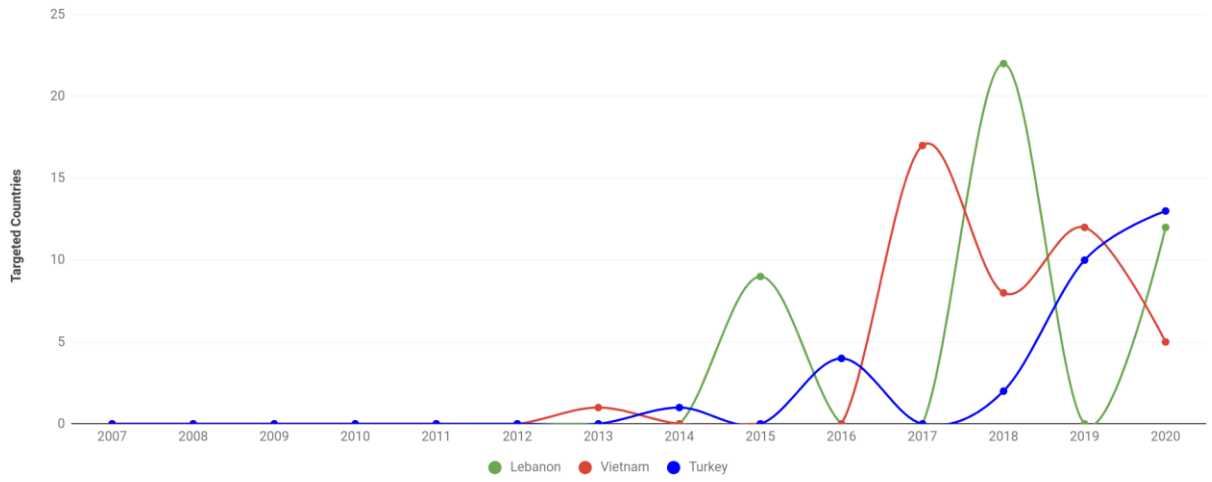
	Internal Security Forces (National Police)	**Sandvine - PacketLogic**, 2018 (Türk Telekom)	FinFisher – 2013 (Unknown user)
State-Sponsored Threat-Actors	**Dark Caracal** (2018) and **Volatile Cedar** (2015)	**StrongPity** (2012) and **Sea Turtle** (2017)	**APT32/OceanLotus** (2013)
Targeted Region	MENA	MENA	Southeast Asia

Source: Izycki, Eduardo

The three countries acquired offensive capabilities from the private sector in early 2010, and there is evidence that they were deployed against several targets.

Following that first experience with third-party technology, the three countries increased their offensive cyber actions through state-sponsored threat-actors, according to the chart below.

Figure 13 – Number of countries target by year (2008-2020)



Source: Izycki, Eduardo

This suggests that there is a maturing process for deploying and developing indigenous offensive cyber capabilities. The threat-actors did not explicitly reverse-engineer the acquired technologies, nor did they appear to demand a knowledge transfer as part of the purchase. However, the training received, and the experience gathered during the actual use against real targets probably helped during the development process.

This suggests that the pool of potential nation-state cyber actors can increase significantly, considering that 85 countries have acquired technology from the private sector.

9.5. *Correlating Cyber Offensive Capabilities and Authoritarianism*

There are differences in the framing of defensive cyber actions. While most western countries use "cybersecurity," a significant number of nations prefer to use "information security,"

where information content is within the scope of protection. This division reflects the views on an "open and free internet" versus those who defend the principle of "cyber sovereignty" and government action to maintain order in cyberspace (Barrinha and Renard 2020).

This difference is also emphasized when using cyber capabilities against political targets (opposition and activists) and the acquiring of offensive cyber tools by intelligence agencies.

By applying the Chi-Square Distribution test for Independence, this research correlates the data gathered on purchasing offensive cyber capabilities with the World index's Freedom of the World – FOTW (Freedom House 2020).

The index is produced by Freedom House and assesses political rights and civil liberties. It establishes three levels: Free, Partly Free, and Not Free.

The Freedom in the World annual global report describes the status of political rights and civil liberties. It is composed of numerical ratings and descriptive texts for each country and territory. The report's methodology is derived largely from the Universal Declaration of Human Rights, adopted by the UN General Assembly in 1948.

From the 198 countries that are considered for the FOTW, 82 countries (41.41%) are classified as Free, 60 labeled as Partly Free (30.30%), and 56 as Not Free (28.28%). Thus, if the acquisition of offensive cyber capabilities is not related to the FOTW, it would be expected to observe a proportional distribution of purchases among the three categories.

Therefore, the question set out is the following: is the number of intelligence agency purchases of offensive cyber capabilities independent of the FOTW classification?

- The null hypothesis (H0) is that intelligence agencies' acquisition of cyber offensive capabilities is not related to the FOTW index on political freedom.
- The alternative hypothesis (H1) is that the intelligence agencies' purchasing is related to the FOTW index on political freedom.

There are two degrees of freedom (three categories of FOTW), and this research sets the level of significance at 5%. Also, as displayed below, all expected frequencies are above 5.

The following table displays the data gathered concerning the acquisition of offensive cyber capabilities by intelligence agencies according to the FOTW index

Table 21 – Cyber offensive capabilities purchase by intelligence agencies and FOTW index (observed values)

Observed Data	Total Purchases	Intelligence Agencies	TOTAL
Free	26	6	38
Partly Free	11	14	39
Not Free	16	12	40
TOTAL	85	32	117

Source: Izycki, Eduardo

Considering the proportion of countries in each FOTW category, the expected results would be the following:

Table 22 – Cyber offensive capabilities purchase by intelligence agencies and FOTW index (expected frequencies)

Expected Frequencies	Total Purchases	Intelligence Agencies	TOTAL
Free	19,95	12,05	48,45
Partly Free	15,59	9,41	35,45
Not Free	17,46	10,54	33,09
TOTAL	85	32	117

Source: Izycki, Eduardo

The calculated Chi-Square result for the observed and expected data is 8.78, and the P-Value is 99,37%.

The critical value for two degrees of freedom and 5% significance is 5.99. This was obtained by applying an MS Excel formula: CHISQ.INV(0,95; 2).

This means that the Chi-Square result is larger than the critical value, thus rejecting the null hypothesis that intelligence agencies purchasing offensive cyber capabilities are independent of the FOTW classification.

A second question is set out to determine if performing surveillance actions through cyberspace is independent of the FOTW classification?

- The null hypothesis (H0) is that performing surveillance actions through cyberspace is not related to the FOTW index on political freedom.
- The alternative hypothesis (H1) is that performing surveillance actions through cyberspace is related to the FOTW index on political freedom.

There are two degrees of freedom (three categories of FOTW), and this research sets the level of significance at 5%. Also, as displayed below, all expected frequencies are above 5.

The following table displays the data gathered concerning the acquisition of offensive cyber capabilities by intelligence agencies according to the FOTW index.

Table 23 – Surveillance actions by cyber means and FOTW index (observed values)

Observed Data	Surveillance Actions	Remaining Actions	TOTAL
Free	1	19	20
Partly Free	4	8	12
Not Free	20	94	114
TOTAL	25	121	146

Source: Izycki, Eduardo

Considering the proportion of countries in each FOTW category, the expected results would be the following:

Table 24 – Surveillance actions by cyber means and FOTW index (expected frequencies)

Expected Frequencies	Surveillance Actions	Remaining Actions	TOTAL
Free	12,47	7,53	20
Partly Free	7,48	4,52	12
Not Free	71,08	42,92	114
TOTAL	91,04	54,96	146

Source: Izycki, Eduardo

The calculated Chi-Square result for the observed and expected data is 129.84.

The critical value for two degrees of freedom and 5% significance is 5.99. This was obtained by applying an MS Excel formula: CHISQ.INV(0.95; 2).

This means that the Chi-Square result is larger than the critical value, thus rejecting the null hypothesis that performing surveillance actions through cyberspace is independent of the FOTW classification.

Therefore, there is a correlation between authoritarian countries, surveillance actions through cyberspace, and the acquisition of offensive capabilities allocated to intelligence agencies.

Based on this simple statistical test, there is room to consider that the use of offensive cyber capabilities may be influenced by its relation to political freedom and civil rights. It is possible to infer the future use of offensive cyber capabilities in the countries according to FOTW classification would likely be deployed against their own population for political purposes. Further research would be necessary to assert this categorically, but this sample serves at least to raise this hypothesis.

Furthermore, considering that 53 countries (62.3%) that acquired offensive cyber capabilities are classified as Not Free or Partly Free, the number of surveillance actions is expected to be even higher than is currently known

9.6. *Is the best defense a good offense?*

The football adage is often applied to cyberspace due to an alleged offensive natural inclination. Although it is a contested argument (Valeriano, Jensen and Maness 2018), the overwhelming evidence suggests that offensive cyber capabilities do not deter other states from engaging in cyber actions (Martin 2020).

From the twenty most frequent targets of offensive cyber-attacks, only five are not also actors with actual offensive cyber actions (Germany, Japan, Canada, Taiwan, and Indonesia).

Four of the five countries remaining have potential offensive capabilities. Germany has (at least) two private vendors of offensive cyber capabilities (Trovicor and Gamma Group), Canada is a member of the Five Eyes (network of intelligence agencies whose offensive capabilities were revealed by Edward Snowden), Taiwan has an unconfirmed state-sponsored threat actor (attribution by a single Chinese cybersecurity company), and Indonesia acquired offensive capabilities for its National Encryption Agency (Lembaga Sandi Negara).

Table 25 – Top 20 most targeted countries, state sponsored APTs and cyber offensive capabilities

Country	Total	Cyber offensive capabilities
United States	88	13
China	72	75
India	56	3
Russia	54	48
Germany	48	Private Sector Provider (2)
Japan	**46**	**LEA Purchase**
Iran	44	38
Saudi Arabia	43	3
Turkey	37	5
South Korea	35	2
Pakistan	32	8
United Kingdom	32	6
France	31	3
Canada	31	Five Eyes Member
Taiwan	29	Threat Actor (not confirmed)
Vietnam	27	5
Israel	26	6
Mexico	25	8
Indonesia	25	Intelligence Agency Purchase
UAE	23	4

Source: Izycki, Eduardo

Except for Japan, every country within the top 25 target list has demonstrated some offensive cyber capabilities. How to reconcile the evidence with the idea of cyber deterrence? To put it bluntly, it is impossible.

The evidence presented is undermining the idea that offensive cyber capabilities will deter other countries' actions in an analogy with nuclear weapons during the Cold War. Ciaran Martin asserts that offensive cyber capabilities appear to be incapable of affecting opponent psychology when deciding to engage (Martin 2020).

One reason for the enduring belief in deterrence frameworks for offensive cyber capabilities comes from the constant comparison with nuclear weapons (J. Nye 2011). One must be skeptical with analogies about it because nuclear actions are an escalation of conventional weapons, while offensive cyber actions are mostly below the threshold of the use of force (UN Charter, Article (2)4).

A study regarding cyber deterrence merits research on its own, but the empirical evidence opposes the concept's effectiveness. As this research presents through its results, offensive cyber actions are a potentialized form of power projection. Thus, “cyber deterrence” seems only plausible by combining with different statecraft tools (criminal indictments, economic sanctions, and threat or use of force).

Cyberspace does not appear as an enclosed boxing ring where states can only engage and respond with offensive cyber actions (Martin 2020). As an additional resource available for nation-states, offensive cyber capabilities must be considered another tool to be used in the international arena.

9.7.*Multipolarity in Cyberspace*

In a simplified concept, a system is considered multipolar when three or more countries share comparable influence over the others considering their economic, cultural, political, and military capabilities.

As stated above, cyber capabilities are instruments for a countries' cultural, military, and economic power projection. In this sense, cyberspace can be viewed as a microcosm of the international order and provide useful analogies for what the future might hold.

Regarding the complexity of attacks, the fact that countries displayed similar CVE severity levels suggests the absence of dominance by any particular country. Moreover, 16 countries displayed evidence of self-made cyber capabilities.

Conventional forces are also measured in quantities of equipment and troops. In terms of threat actors and targets engaged, the numbers displayed by China, Russia, and Iran (Table nº 2) are equal or superior to the United States.

These variables indicate that the United States does not exercise dominance in cyberspace. Thus, one should not consider this dimension under a unipolar order.

Although the United States and China are clearly rivals engaging in cyberspace, the goals are not the same as those from the Cold War (Lewis 2021).

Considering the global and regional players' behavior, there is no clear alignment of countries that suggests a bi-polar order in cyberspace between China and the United States. Russia and Iran engage with China frequently. The same applies to the United States and France, countries that were supposed to be in the same “pole”.

- Russia -> China (5)

- China -> Russia (9)
- Iran -> China (6)
- China -> Iran (4)
- The United States -> France (4)
- France -> The United States (1)

Another example is the North Koreans who frequently perform actions against Chinese targets, its main ally. Furthermore, the United States and India's mutual actions against each other.

- North Korea -> China (7)
- The United States -> India (4)
- India -> The United States (2)

The fact that several countries possess similar offensive capabilities and no clear alignment in a bipolar structure (i.e., China and Russia engage each other) suggests that cyberspace offers a glimpse of multipolarity in action.

Cyberspace provides opportunities for allies and rivals to mutually engage each other, while there is no clear balance of power in place. The multiple agendas collide or occasionally coalesce, offering a grim perspective on a multipolar international order.

10. CONCLUSIONS

Many actors play significant roles in cyberspace, whether they are individuals, non-state actors, private companies, or the nation-state. As service users, maintaining internet infrastructure, providing content, providing security, and (occasionally) as threat actors.

Despite the importance of all those actors, nation-states remain the most aggressive and incisive actors in that ecosystem (J. Nye 2010).

This research set out to provide an in-depth view of nation-state offensive cyber capabilities. As a result, it gathered evidence of 29 different countries engaging in offensive cyber actions (Section 7.1) and (at least) 85 nations acquired offensive cyber technologies from private vendors (Sections 8.1 and 8.2). The numbers are impressive, especially considering the average perception of concentration of cyber capabilities in a few "traditional" actors.

A theoretical implication for this result is that the evolutionary faction appears to be correct in its predictions (so far), but there is some merit to the revolutionary perspective.

The majority of offensive cyber actions are a variation of traditional instruments of statecraft (sabotage, surveillance, espionage, and disinformation) potentialized by cyberspace's unique characteristics (Sections 7.4 and 9.2). This means that the environment is new but its purposes are well known.

There is a revolutionary component, though; offensive cyber actions allow countries to promote attacks against critical infrastructures, or, at least, to access and be surreptitiously in

place to strike those targets in the future. That is indeed new, although rare in cyberspace (Section 7.6).

The fact that only the United States, Israel (Stuxnet), Russia (NotPetya, and Triton & Trisis), and Iran (Shamoon) manage to conduct sabotage with kinetic effects through offensive cyber actions suggests that despite feasible, actions that reach the threshold of attack are still quite uncommon (Izycki and Vianna 2021).

Additional evidence to support the evolutionary claim is the geographical orientation behind most offensive cyber actions (Section 7.3). This highlights that despite cyberspace being a human-made environment, it is highly influenced by geopolitical imperatives from the "real world."

Therefore, the evidence presented frame offensive cyber capabilities as an additional tool of statecraft, not a revolution in the making. It has benefits, such as the difficulties in attribution (plausible deniability) and the almost unprecedented low escalation risk, which encourage nations to deploy these tactics to achieve strategic objectives.

The number of actors and their similarities regarding exploited CVE's suggest diffusion of power, but there is hardly equality of cyber capabilities. Most countries depend on third-party technologies from the foreign private sector (Sections 7.2 and 9.1). The roster of countries that have displayed self-made capabilities is small (16) compared to the number of countries offensively capable.

This creates an opportunity that many states are resorting to. The low-cost ability to erode the advantages of geopolitical rivals and challenge the status-quo is present. In this sense, the international dynamics is influenced by cyber capabilities, resulting in countries punching above their weight on the international system (Barrinha and Renard 2020).

Regarding political alignments in cyberspace, several countries possess a similar level of offensive capabilities (Section 7.5), which means that no nation acts in a dominant position. Moreover, there is not a bipolar structure similar to the Cold War. This suggests that cyberspace offers a glimpse of multipolarity dimension. There is no clear balance of power, and multiple agendas collide or occasionally coalesce (Section 9.7).

Cyber conflict is ambiguous and less oriented towards conventional military strategies, and international conflict studies lack the analytic tools to reframe strategies for it (Lewis 2021). The fact that cyber actions do not create an existential threat gives states plenty of room to maneuver in cyberspace and to engage with competitors. This is seen by the cumulative effect that offensive cyber actions can achieve, i.e., a single action might not be relevant but repeated engagement can influence the relative balance of power.

In this sense, offensive cyber capabilities are not transforming the nature of war itself. Rather, it provides alternatives for the bargaining and interactions of nation-states below the threshold of the use of force. Actors are able to achieve strategic outcomes and influence the balance of power without having to resort to an armed attack and minimize the risk of a military or nuclear response from their targets (Harknett and Smeets 2020).

For example, this research identified: North Korean actions to circumvent economic sanctions through cyber theft, China's acquisition of state-of-the-art technology by cyber espionage, and Russia's ability to behave aggressively in its vicinity and challenge the United States.

More broadly, this research also points to the fact that offensive cyber actions are tolerated by western and non-western standards, provided they do not aim to destroy or provoke loss of functionality in critical infrastructure services. This threshold is extracted from the dataset given the few occurrences in the last decade and the reports from the Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) on Advancing responsible State behavior in cyberspace in the context of international security, both at the United Nations.

The data indicates that there is an increasingly clear distinction between offensive cyber capabilities and cybersecurity (Martin 2020). While both can be a measure of cyber power and a useful indicator for policy making, the evidence suggests that offensive cyber capabilities do not deter other countries from engaging in cyberspace (Section 9.6).

The issues with attribution, the lack of clear red lines, and the challenges of clearly responding to an attack (imposing costs) explain the lack of effectiveness of deterrence strategies by the countries with the most notable offensive cyber capabilities.

Looking forward, a continuous increase in offensive cyber actions is expected, given that more countries are acquiring and developing offensive capabilities (Section 9.4). The argument that security is a traditional government function has often been used to justify the acquisition of offensive capabilities, which reinforces the nation-state's role in cyberspace (Nye 2018).

However, the evidence so far suggests that escalation is not a salient issue since no conflict has started with offensive cyber actions and then become a conventional conflict. One could argue the opposite, that the Stuxnet is an example of de-escalatory action because the alternative would be a conventional strike against the Iranian nuclear program (Valeriano, Jensen and Maness 2018).

The episode of the Israeli Armed Forces bombing of the Palestinian cyber force headquarters (Groll 2019) is the single clear case of escalation from cyber to a physical response. Interestingly, Israel argues that it did not happen against a nation-state but a non-state actor (Hamas cyber division).

Conversely, the use of offensive cyber actions against political opposition (domestic targets) and expatriates is expected to rise given a countries' profile of acquiring offensive cyber capabilities, assuming the evaluation as authoritarian by the FOTW Index (Section 9.5). This echoes the findings of Valeriano and Maness (2015, 2018).

Regions such as MENA and Southeast Asia are likely to continue with the highest number of offensive cyber actions. For the former, the tensions among regional competitors (Iran and Saudi Arabia), Turkey's rise, and the civil wars in Syria and Yemen remain. The latter, with tensions in the South China Sea and the increasing geopolitical competition in the Indian Ocean and Himalayas (Section 9.2).

The use of offensive cyber actions is foreseeable in other regions due to border and resource disputes, albeit the likely use in a broader spectrum in support of conventional weapons. For examples:

- The River Nile dispute involving Egypt and Ethiopia (backed by Sudan) could spark the use of cyber-enabled means from both sides, given all sides' proven capabilities.
- Border disputes in Central Asia and Caucasus – such as the conflict between Armenia and Azerbaijan for the Nagorno-Karabakh region – are another potential theatre of operations for offensive cyber capabilities.

Nevertheless, a pure cyber conflict is unlikely to reach the threshold of force – physical destruction, injuries and death or the long-term loss of critical infrastructure functionality. This kind of cyber action appears to be dependent on a broader conventional conflict involving nation-states. Instead, cyberspace is a domain where relative power can be influential and strategic balance can evolve without resorting to the level of armed conflict.

A few closing remarks on the future of offensive cyber capabilities and some encouragement for future researcher is appropriate at this point.

Offensive cyber capabilities will be directly impacted by the increase of interconnectivity prompted by 5G and the adoption of AI, quantum computing and other disruptives technologies. The first conclusion is that offensive cyber actions will dramatically increase with the widespread adoption of additional disruptive technologies.

The 5G technology is going to enable the increase of connected devices to the internet of all things, it is predicted that smart devices will be so common that they will be placed on disposable items such as fruits and vegetables. This, in turn, will increase the attack surface available for threat actors who will be granted a new universe of big data to perform espionage and surveillance against its targets.

With AI the speed and operational width for offensive actions (no longer exclusive to humans) will increase, for instance, providing endless reconnaissance capabilities and mind-blowing intrusion persistence (limited by human knowledge nowadays). This may increase escalatory consequences, as AI enabled cyber actions might inadvertedly cross accepted thresholds.

As for quantum computing the prospects are even more staggering. The computational power of these new machines will render the current cryptography standards useless, which means that the whole defense apparatus in place is going to overwhelmed by it. It is most likely that security measures will also improve with quantum technology, but the difference from the “haves” and “have nots” tends to be huge during this transition period.

To my fellow researchers in the fields of international relations and cyber security I believe this research opens several topics for further research that I welcome you to follow by using the data provided by this research.

First, the issue of deterrence applied to cyberspace can be explored under the light of empirical evidence. The conceptual framework of this concept – frequently mentioned in cyber security national strategies – can be tested against cases of offensive cyber actions and the countries response to it. The subject welcomes a fresh approach from the adoption of nuclear deterrence concepts from the Cold War.

A second subject that can be further studied is the nation-state profiling suggested in Section 9.3. The proposed taxonomy is intended to set the grounds for a policy debate regarding behavior in cyberspace and how countries should consider their rivals actions. The acquisition or development of offensive cyber capabilities ought not to be viewed as simple threatening behavior according to the proposed framework.

Another issue that derives from the development of cyber capabilities is the existence of a security dilemma and an arms race in cyberspace. Albeit the increase of offensive cyber capabilities worldwide, this research was unable to determine if there is any causal relationship. Are countries responding to their peers by acquiring and developing new capabilities? This is an issue that should be taken into consideration in further studies.

Finally, the offensive cyber actions that aim to produce disinformation against their targets is another subject that can be further explored. In this research the number of cases (5 documents) was very small because these actions are not usually described as APTs. An important addition to this line of research would benefit from the inclusion of the current dataset from data provided by the social networks (Twitter and Facebook) that started to proactively disclose these kinds of operations from 2020 onwards.

REFERENCES

Amnesty International. 2018. *Amnesty International Among Targets of NSO-powered Campaign.* 08. Accessed 2019. https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

—. 2019. *Morocco: Human Rights Defenders Targeted with NSO Group's Spyware.* 10. Accessed 2020. https://www.amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware/.

—. 2019. *State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack.* 04. Accessed 2020. https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/.

Arquilla, John , and David Ronfeldt. 1993. *Cyberwar is Coming!* Santa Monica, CA: RAND Corporation.

Arsene, Liviu, Radu Tudorica, Cristina Vatamanu, and Alexandru Maximciuc. 2020. *StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure.* 06. Accessed 2020. https://labs.bitdefender.com/2020/06/strongpity-apt-revealing-trojanized-tools-working-hours-and-infrastructure/.

Ashmore, William C. 2009. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defence Review.*

Australian Strategic Policy Institute. 2019. "Mapping China's Tech Giants." *Australian Strategic Policy Institute.* Accessed 2020. https://chinatechmap.aspi.org.au/#/map/f3-Surveillance.

Bandla, Kiran . 2020. *APTnotes data.* Accessed 12 2020. https://github.com/aptnotes/data.

Barrinha, André, and Thomas Renard. 2020. "Power and diplomacy in the post-liberal cyberspace." *International Affairs 96(3).*

Bartholomew, Brian, and Juan Andrés Guerrero-Saade. 2016. "Wave your false flags! Deception tactics muddying attribution in targeted attacks." *Virus Bulletin.* Virus Bulletin.

BBC. 2012. *Leon Panetta warns of 'cyber Pearl Harbour'.* https://www.bbc.com/news/av/technology-19923046.

Bencsáth, Boldizsár , Gábor Pék, Levente Buttyan, and Mark Felegyhazi. 2012. "The Cousins of Stuxnet: Duqu, Flame, and Gauss." *Future Internet.*

Bing, Christopher, and Joel Schectman. 2019. *American Hackers Helped UAESpy on Al Jazeera Chairman, BBC Host.* 04. Accessed 2020. https://www.reuters.com/investigates/special-report/usa-raven-media/.

—. 2019. *Special Report: Inside the UAE's secret hacking team of U.S. mercenaries.* 01. Accessed 2020. https://www.reuters.com/article/us-usa-spying-raven-specialreport/special-report-inside-the-uaes-secret-hacking-team-of-u-s-mercenaries-idUSKCN1PO19O.

Bing, Cristopher , and Joel Schectman. 2019. *Project Raven.* 01 30. Accessed 2019. https://www.reuters.com/investigates/special-report/usa-spying-raven/.

Cardenal, Juan Pablo, Jacek Kucharczyk, Grigorij Mesežnikov, and Gabriela Pleschová. 2017. *Sharp Power: Rising Authoritarian Influence.* Report, International Forum for Democratic Studies.

Cherepanov, Anton. 2017. "WIN32/INDUSTROYER A new threat for industrial control systems." *ESET WeLiveSecurity.* 06 12. Accessed July 2017. https://app.box.com/s/ec8zyav7snvm6vsfhy8ocvvngphe8lqp.

Cimpanu, Catalin. 2019. *Source code of Iranian cyber-espionage tools leaked on Telegram.* 04 17. Accessed 2 2020. https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/.

CitizenLab. 2014. "Information controls during Thailand's 2014 Coup." *CitizenLab.* Accessed 2019. https://citizenlab.ca/wp-content/uploads/2015/03/Information-controls-during-Thailand%E2%80%99s-2014-Coup.pdf.

Clarke, Richard A. , and Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins.

Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous.* Verso.

Council on Foreign Relations. 2020. "Cyber Operations Tracker." *Digital and Cyberspace Policy.* Accessed 12 2020. https://www.cfr.org/cyber-operations/.

Egloff, Florian J., and Andreas Wenger. 2019. *Public Attribution of Cyber Incidents.* CSS Analysis, Zurich: Center for Security Studies (CSS), ETH Zurich.

Eichensehr, Kristen. 2020. "The Law & Politics of Cyberattack Attribution." *UCLA Law Review 67.*

ESET. 2015. *Dino – the latest spying malware from an allegedly French espionage group analyzed.* 06. Accessed 2018. https://www.welivesecurity.com/2015/06/30/dino-spying-malware-analyzed/.

Falcone, Robert, David Fuertes, Josh Grunzweig, and Kyle Wilhoit. 2018. *The Gorgon Group: Slithering Between Nation State and Cybercrime.* 08. Accessed 2019. https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/.

Falliere, Nicolas, Liam Murchu, and Eric Chien. 2011. *W32.Stuxnet Dossier.* Technical Report, Symantec.

Farwel, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival, 53:1* 23-40.

FireEye. 2017. *At the Center of the Storm: Russia's APT28 Strategically Evolves its Cyber Operations.* 11. Accessed 2018. https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf.

—. 2013. *FireEye Uncovers Chinese Cyber Espionage Campaign Targeting European Ministries of Foreign Affairs.* Accessed 2018. https://www.fireeye.com/company/press-releases/2013/fireeye-uncovers-chinese-cyber-espionage-campaign-targeting-european-ministries-of-foreign-affairs.html.

Freedom House. 2020. *Freedom in the World 2020 A Leaderless Struggle for Democracy.* Freedom House.

Galperin, Eva, Cooper Quintin, Morgan Marquis-Boire, and Claudio Guarnieri. 2016. *Operation Manul: I Got a Letter From the Government the Other Day...Unveiling a Campaign of Intimidation, Kidnapping, and Malware in Kazakhstan.* Technical Report, EFF.

Gartzke, Erik. 2013. "The myth of cyberwar: Bringing war on the internet back down to earth." *International Security 38(2)* 41–73.

2015. "Cyber war in perspective: Russian aggression against Ukraine." In *Cyber War in Perspective: Russian Aggressionagainst Ukraine*, by Kenneth Geers and James A. Lewis, 39-49. Tallin: NATO Cooperative Cyber Defence Centre of Excellence.

Georgia. 2009. *Russian Cyberwar on Georgia.* Accessed 2018. https://lawlordtobe.files.wordpress.com/2018/03/cyberwar-georgia.pdf.

Glyer, Christopher, Dan Perez, Sarah Jones, and Steve Miller. 2020. *This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits.* 03. Accessed 2020. https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html.

Groll, Ellias. 2019. "The Future Is Here, and It Features Hackers Getting Bombed." *Foreign Policy.* 06 02. Accessed 2020. https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Group-IB. 2017. *Lazarus Arisen: Architecture, Techniques and Attribution.* 05. Accessed 2018. https://www.group-ib.com/resources/threat-research/lazarus.html.

Guerrero-Saade, Juan Andres, and Priscilla Moriuchi. 2017. *North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign.* Accessed 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-0116.pdf.

Gundert, Levi, Sanil Chohan, and Greg Lesnewich. 2018. *Iran's Hacker Hierarchy Exposed.* Accessed 2019. https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf.

Harknett, Richard J., and Max Smeets. 2020. "Cyber campaigns and strategic outcomes." *Journal of Strategic Studies.*

Harknett, Richard J., and Smeets Max. 2020. "Cyber campaigns and strategic outcomes." *Journal of Strategic Studies.*

Hasbini, Mohamad Amin, Santiago Pontiroli, and Ghareeb Saad. 2014. *The Syrian Malware House of Cards.* 08. Accessed 2018. https://securelist.com/the-syrian-malware-house-of-cards/66051/.

Healey, Jason , and Karl Grindal. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Cyber Conflict Studies Association.

Hunter, Max. 2016. *Operation Manul.* Report, Electronic Frontier Foundation.

Insikt Group. 2019. *Iranian Threat Actor Amasses Large Cyber Operations Infrastructure Network to Target Saudi Organizations.* 06. Accessed 2020. https://www.recordedfuture.com/iranian-cyber-operations-infrastructure/.

Inskit Group. 2016. *Hacktivism: India vs. Pakistan.* 02. Accessed 2018. https://www.recordedfuture.com/india-pakistan-cyber-rivalry/.

Izycki, Eduardo, and Eduardo Wallier Vianna. 2021. "Critical Infrastructure: A Battlefield for Cyber Warfare?" *16th International Conference on Cyber Warfare and Security (ICCWS).* Tennessee Tech, USA: Academic Conferences International.

Izycki, Eduardo, and José Eduardo Malta de Sá Brandão. 2019. "CAPÍTULO 10 - PODER OFENSIVO NO ESPAÇO CIBERNÉTICO." In *Desafios contemporâneos para o exército brasileiro*, by Israel de Oliveira Andrade, Valério Luiz Lange, Oscar Medeiros Filho and Raphael Camargo Lima. IPEA.

Izycki, Eduardo, and Rodrigo Colli. 2019. "Protection of critical infrastructures in national cyber security strategies." *ECCWS 2019 - Proceedings of the 18th European Conference on Cyber Warfare and Security.* Coimbra, Portugal: ACPI, Ltd (ISBN: 9781912764280).

Jervis, Robert. 1976. *Perception and Misperception in International Politics.* Princeton University Press.

Jorge, Bernardo Wahl Gonçalves de Araújo. 2017. "Estados Unidos, Poder cibernético E a 'guerra cibernética: Do Worm Stuxnet Ao Malware Flame/Skywiper '" E além." *Meridiano 47 - Journal of Global Studies 13* 43-48.

Kaspersky. 2016. "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents." *Kaspersky.* 01 28. Accessed February 2016. https://app.box.com/s/igygz8ihex1hok5r1dp215ui0gz1ghwr.

—. 2015. *The Duqu 2.0 Technical Details.* 06. Accessed 2018. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

Kello, Lucas. 2017. *The Virtual Weapon and International Order.* Yale University Press.

Kramer, Franklin D. 2009. *Cyberpower and National Security.* University of Nebraska Press.

Lassalle, Dave, Sean Koessel, and Steven Adair. 2017. *OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society.* 11. Accessed 2019. https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/.

Levene, Brandon, Josh Grunzweig, and Brittany Barbehenn. 2018. *Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent.* 03. Accessed 2019. https://unit42.paloaltonetworks.com/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/.

Lewis, Jim. 2021. "Toward a More Coercive Cyber Strategy." *U.S. Cyber Command Legal Conference.*

Lindsay, Jon R. 2013. "Stuxnet and the limits of cyber warfare." *Security Studies 22(3)* 365–404.

Lindsay, Jon R. 2014. "The impact of China on cybersecurity: Fiction and friction." *International Security* 7-47.

Lipovsky, Robert. 2016. *New wave of cyberattacks against Ukrainian power industry.* 01. Accessed 2019. https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/.

Lookout and EFF. 2018. *Dark Caracal: Cyber-espionage at a Global Scale.* 01. Accessed 2019. https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf.

Lopes, Gills Vilar. 2016. *Relações internacionais cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos de segurança internacional.* PhD Thesis, Recife: Gills Vilar Lopes.

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. 2014. *Hacking Team and the Targeting of Ethiopian Journalists.* 02. Accessed 2019. https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/.

—. 2014. *Mapping Hacking Team's "Untraceable" Spyware.* 02. Accessed 2019. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

Marczak, Bill, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. 2018. *BAD TRAFFIC - Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?* 03. Accessed 2019. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.

Marczak, Bill, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune. 2015. *Pay No Attention to the Server Behind the Proxy.* 10. Accessed 2019. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, and John Scott-Railton. 2013. *You Only Click Twice.* 03. Accessed 2019. https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

Martin , Ciaran. 2020. *Cyber weapons are called viruses for a reason: statecraft, security and safety in the digital age.* Accessed 2020. https://thestrandgroup.kcl.ac.uk/event/ciaran-martin-cyber-weapons-are-called-viruses-for-a-reason-statecraft-security-and-safety-in-the-digital-age.

Maurer, Tim. 2018. *Cyber Mercenaries: The State, Hackers, and Power.* Cambridge: Cambridge University Press.

McGrath, MC, Brennan Novak, and Kevin Gallagher. 2016. "Surveillance Industry Index." *Transparency Toolkit.* Accessed Nov. 20, 2018. https://sii.transparencytoolkit.org/.

MISP. 2019. *Malware Information Sharing Platform.* Accessed 05 10, 2019. https://www.misp-project.org/.

MITRE Corporation. 2017. *Finding Cyber Threats with ATT&CK-Based Analytics.* June. Accessed 2020. https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics.

MITRE. 2019. "Groups - MITRE ATT&CK." Accessed 2019. https://attack.mitre.org/groups/.

Nye, Joseph. 2010. *Cyber Power.* Belfer Center for Science and International Affairs. Harvard Kennedy School,.

Nye, Joseph. 2018. *Normative Restraints on Cyber Conflict.* Belfer Center for Science and International Affairs.

Nye, Joseph. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly 5(4)* 18-38.

Nye, Joseph S. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly 5(4)* 18-38.

Richardson, John. 2011. "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield." *J. Marshall J. Computer & Info.*

Rid, Thomas. 2011. "Cyberwar will not take place." *Journal of Strategic Studies* 1-28.

Rid, Thomas, and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies, Vol. 38* 4-37.

Rid, Thomas, and Peter McBurney. 2012. "Cyber-Weapons." *The RUSI Journal* 6-13.

Risk Based Security. 2016. *The Shadow Brokers: Lifting the Shadows of the NSA's Equation Group?* 08 15. Accessed 2019. https://www.riskbasedsecurity.com/2016/08/15/the-shadow-brokers-lifting-the-shadows-of-the-nsas-equation-group/.

Roth, Florian. 2019. "APT Groups and Operations." *APT Groups and Operations.* https://docs.google.com/spreadsheets/u/0/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml.

—. 2018. *The Newcomer's Guide to Cyber Threat Actor Naming.* 03 25. Accessed 2019. https://cyb3rops.medium.com/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263.

SCOTT-RAILTON, J. et al. 2017. "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware." *The Citizen Lab.* Accessed nov. 20, 2018. https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. 2017. *Reckless III - Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware.* 07. Accessed 2019. https://citizenlab.ca/2017/07/mexico-disappearances-nso/.

—. 2017. *Reckless III - Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware.* 07. Accessed 2019. https://citizenlab.ca/2017/07/mexico-disappearances-nso/.

SCOTT-RAILTON, John, Bill MARCZAK, Claudio GUARNIERI, and Masashi CRETE-NISHIHATA. 2017. "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links." *Citizen Lab.* 11 02. Accessed 2018. https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/.

Scott-Railton, John, Siena Anstis, Sharly Chan, Bill Marczak, and Ron Deibert. 2020. *Nothing Sacred - Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware.* 08. Accessed 2020. https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/.

Senft, Adam, Jakub Dalek, Helmi Noman, and Masashi Crete-Nishihata. 2014. *Monitoring Information Controls in Iraq in Reaction to ISIS Insurgency.* 07. Accessed 2019. https://citizenlab.ca/2014/06/monitoring-information-controls-in-iraq/.

—. 2014. "Monitoring Information Controls in Iraq in Reaction to ISIS Insurgency." *CitizenLab.* Accessed 2019. https://citizenlab.ca/2014/06/monitoring-information-controls-in-iraq/.

Sherstobitoff, R. 2013. *Dissecting Operation Troy: Cyberespionage in South Korea.* Accessed 2018. https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf.

Teach, Edward. 2020. *The Big Black Book of Electronic Surveillance .* Kindle Edition.

Tencent. 2019. *Be wary of blessings from the holidays - APT attack organization "Higaisa".* 11. Accessed 2020. https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/tree/master/2019/2019.11.04.Higaisa_APT.

The Guardian. 2013. *GCHQ intercepted foreign politicians' communications at G20 summits.* 06. Accessed 2018. https://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

2018. "Underlying Dimensions of Yemen's Civil War: Control of the Internet." *Recorded Future.* Accessed 2020. https://www.recordedfuture.com/yemen-internet-activity/.

United Nations. 2020. *E-Government Survey.* New York: United Nations.

United Nations Institute for Disarmament Research (UNIDIR). 2013. *The Cyber Index: International Security Trends and Realities.* New York and Geneva: United Nations.

United Nations. 2019. *Surveillance and Human Rights, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* A/HRC/41/35, United Nations.

n.d. *V.*

Valentino-DeVries, Jennifer , Lam Thuy Vo, and Danny Yadron. 2015. "Cataloging the World's Cyberforces." *Wall Street Journal.* 12 28. Accessed 12 10, 2020. https://graphics.wsj.com/world-catalogue-cyberwar-tools/.

Valeriano, Brandom, and Ryan C. Maness. 2018. "How We Stopped Worrying about Cyber Doom and Started Collecting Data." *Global Cybersecurity: New Directions in Theory and Methods* 49-60.

Valeriano, Brandon , and Ryan C. Maness. 2016. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System.* New York, NY: Oxford University Press.

Valeriano, Brandon , Benjamin Jensen, and Ryan Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion.* Oxford: Oxford Scholarship Online.

Valeriano, Brandon, and Ryan C. Maness. 2014. "The dynamics of cyber conflict between rival antagonists, 2001–11." *Journal of Peace Research.*

Voo, Julia, Hemani Irfan , Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach. 2020. *National Cyber Power Index 2020.* Harvard Kennedy School.

Wardle, Claire, and Hossein Derakhshan. 2017. *Information disorder: Toward an interdisciplinary framework for research and policy making.* DGI(2017)09, Council of Europe.

WikiLeaks. 2015. *Hacking Team.* 07 08. Accessed 11 20, 2018. https://wikileaks.org/hackingteam/emails/.

—. 2014. *SpyFiles 4.* Accessed 11 20, 2018. https://wikileaks.org/spyfiles4/customers.html.

—. 2017. *Vault 7: CIA Hacking Tools Revealed.* 03 07. Accessed 12 2020. https://wikileaks.org/ciav7p1/.

Wright, Charity. 2020. *New APT32 Malware Campaign Targets Cambodian Government.* 11. Accessed 2020. https://www.recordedfuture.com/apt32-malware-campaign/.

Zetter, Kim. 2019. *Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC.* 10 03. Accessed 2020. https://www.vice.com/en/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec.

APPENDIX A - CYBER CAPABILITIES PROVIDERS

Amesys

The Advanced Middle East Systems (AMESys) was a subsidiary from the French technology company Bull SA (acquired in 2010). It provided the EAGLE system which provides Monitoring Centres, Internet Monitoring, Audio Surveillance and Location Monitoring technology. In 2013, this product was divested to Nexa Technologies with the help of former Amesys employees (Stéphane Salies, a former Bull SA director).

The EAGLE System allows the creation of investigations focused on individuals. It also performs analysis of different data including web traffic, VoIP, chat protocols and search engine queries.

This research identified two cases for government acquisition, Libya and Syria, including former Lybian secret police during the Gaddafi regime.

- Libya
- Syria

The human-rights NGO called *Fédération internationale pour les droits humains* prosecuted Amesys in 2011 for being complicit for tortures during Gaddafi's regime in Libya.

Cyberbit and Elbit Systems

Elbit Systems is an Israeli traditional military and defense equipment provider. In 2015, it acquired Cyberbit to bolster its cybersecurity and intelligence collection portfolio.

Their approach to the offensive capabilities market is that boundaries between national security, defense and law enforcement agencies (even local ones) are increasingly blurred. That creates opportunities for an all-encompassing intelligence solution.

Cyberbit's capabilities include bulk metadata collection and analytics, malware, open-source intelligence, satellite communications, and a platform that can unify all of that. It can all be acquired in a single purchase or as separate modules.

Additional features include the PC Surveillance System (PSS), a solution that provides zero-days exploits to plant malware for "monitoring and extracting information". The user can bypass encryption and security mechanisms to control and collect data from the target device.

This includes VoIP conversations, e-mails exchange, web browsing history, keystrokes, screen shots, extract credentials, obtain geo-location in real time, and activation of microphone and cameras. The advertised solution is flexible to act in conformity to local legislation worldwide.

This research identified six sales to state users, including intelligence agencies and a law enforcement agency.

- Ethiopia
- Kazakhstan
- Philippines
- Thailand
- Uzbekistan
- Zambia

The most noticeable cases include the actions against opposition political organizations in Ethiopia (Ginbot 7), Bahraini human rights activists and Malay language speakers during the 2013 General Elections.

Dreamlab

Dreamlab Technologies is Swiss company operating in Bern since 2004. Its main product is called iProxy and provides communications monitoring coming across the internet. In one of its commercial enterprises Dreamlab was associated with Gamma Group. The bundle allowed for the customer to deploy Gamma's FinFisher intrusion software.

This research found evidence of Dreamlab's equipment in two countries:

- Oman
- Turkmenistan

Gamma Group

Gamma Group is a British-German enterprise that provides “ethical hacking” programs. Its product, called FinSpy suite, possesses a host of functionalities that derives from the privileged access granted with the remote control of the target`s device.

The tool allowed the customer to access web browsing, keystrokes, audio collected by the phone, instant messaging, and voice conversations. Moreover, credentials to private services (user/password) would also be collected by the FinSpy suite, allowing the customer to go further than the compromised device into other systems. The tool also worked cross-platforms (mobile and desktop) and operating systems (Windows, iOS, Android).

The company gained unwanted notoriety in 2014 as a result of a data breach - by a hacktivist identified as “PhineasFisher,” - that made public 30 GB of information regarding technical capabilities and their customers (WIKILEAKS).

The offensive actions are a product of multiple vectors such as zero-day vulnerabilities, spear-phishing attacks, drive-by downloads, and social engineering deployed against the targets.

Its architecture includes a main server (Master FinFisher) that acts as a command and control, and FinProxy that host and deploy malware solutions. The FinSpy module communicates with the FinProxy, to communicate with the Master Server.

The company also provides solutions for hacking into devices with physical access (FinFisher USB Suite) and a Remote Hacking Kit to remotely gain access to the target computer.

Other features include dynamically changing files as the download occurs (FinFly), high-performance password cracking (FinCrack), sniffing strokes from remote keyboards (Fin Wi-Fi KeySpy), attacks against Bluetooth protocol (FinBluez),

This research identified 55 sales to state users, including intelligence agencies and a law enforcement agency.

- South Africa
- Germany
- Angola
- Saudi Arabia
- Australia
- Austria
- Bahrain
- Bangladesh
- Belgium
- Bosnia & Herzegovina
- Brunei Darussalam
- Bulgaria
- Canada
- Kazakhstan
- Egypt
- United Arab Emirates
- Slovenia
- Spain
- United States
- Estonia
- Ethiopia
- Gabon
- Netherlands
- Hungary
- India
- Indonesia
- Italy
- Japan
- Jordan
- Latvia
- Lebanon
- Lithuania
- Macedonia
- Malaysia
- Morocco
- Mexico
- Mongolia
- Nigeria
- Oman
- Panama
- Pakistan
- Paraguay
- Qatar
- Kenya
- United Kingdom
- Czechia
- Romania
- Serbia
- Singapore
- Taiwan
- Turkmenistan
- Turkey
- Uganda
- Venezuela
- Vietnam

The most noticeable cases include the actions against opposition political organizations in Ethiopia (Ginbot 7), Bahraini human rights activists and Malay language speakers during the 2013 General Elections.

Hacking Team

Hacking Team is an Italian company provider of “ethical hacking” programs. The company was later acquired by a Swiss group called Memento Labs. Its main product was called Remote Control System (RCS), a later version was branded Galileo. Its functionalities allowed the customer to have full control over the target device.

The tool allowed the customer to access web browsing, keystrokes, audio collected by the phone, instant messaging, and voice conversations. Moreover, credentials to private services (user/password) would also be collected by the RCS, allowing the customer to go further than the compromised device into other systems. The tool also worked cross-platforms (mobile and desktop) and operating systems (Windows, iOS, Android).

The company gained unwanted notoriety in 2014 as a result of a data breach - by a hacktivist identified as Phineas Phisher - that made public 30 GB of information regarding technical capabilities and their customers (WIKILEAKS).

This research identified 61 sales to state users, including Armed Forces, intelligence agencies and law enforcement agencies.

- Saudi Arabia
- Azerbaijan
- Bahrain
- Brazil
- Kazakhstan
- Chile
- Cyprus
- Colombia
- South Korea
- Egypt
- United Arab Emirates
- Ecuador
- Spain
- United States
- Ethiopia
- Guatemala
- Honduras
- Hungary
- Italy
- Lebanon
- Lithuania
- Luxemburg
- Malaysia
- Morocco
- Mexico
- Mongolia
- Nigeria
- Oman
- Panama
- Poland
- Czechia
- Russia
- Singapore
- Sudan
- Switzerland
- Thailand
- Turkey
- Uzbekistan
- Vietnam

Among the famous cases, the targeting of Moroccan media outlet Mamfakinch, the Emirati human rights activist Ahmed Mansoor, Ethiopian Satellite Television Service (ESAT) employees, and the use against Korean speaking targets by the South Korean National Intelligence Service (NIS).

Sandvine

Sandvine is a rebranding of Procera Networks after Francisco Partners (an American private equity firm) acquired the Ontario-based networking equipment company. The group is known to have multiple investments in companies with dual-use technology (among them NSO Group).

Its main product is called PacketLogic. It is a Deep Packet Inspection (DPI) device. It can interact in different manners (degrade, block, inject, and log) a great number of types of Internet traffic. This was used by governments to inject malicious programs into the target devices (Turkey) and to suppress legitimate traffic (acting as a censorship mechanism in Egypt to block access to Report Without Borders, Human Rights Watch and other ONGs).

This research identified three countries that acquired the Sandvine PacketLogic:

- Egypt
- Turkey
- Pakistan

One of the most prominent cases is the use of Sandvine by the Türk Telekom to bundle legitimate internet traffic with malware used by StrongPity APT. The targets were physically located in Syria and Turkey.

NICE Systems

The company was founded by former Israeli military personnel, NICE (Neptune Intelligence Computer Engineering) began as a provider of intelligence and defense related products.

The group has multiple solutions that include real-time predictive analysis and surveillance packages that can provide data for the predictive actions of the first product.

The company's products are used in over 150 countries, including customers in the Fortune 100. The main product NiceTrack Mass Detection Center (MDC) can be utilized in a bulk collection system for a big data set-up.

This research identified five cases where NICE Systems equipment was sold individually or bundled together with Hacking Team RCS.

- Colombia
- Kazakhstan
- Nigeria
- Uganda
- Uzbekistan

NSO Group

NSO Group was founded in 2010 by Unit 8200 three former agents, Israel's military intelligence service. The company's chairman was also a retired general from the Israeli Armed Forces. Its core product is called Pegasus and its targets are mobile devices by a combination of malware and social engineering skills.

One of the striking features of Pegasus is its zero-click installation vector, by which the target is compromised without any action of the human target. It also has one-click vectors, that require some level of social engineering or other instances to trick the victim.

After the initial access to the target device, Pegasus can collect and exfiltrate all the data available in the device. Emails, instant messages, keystrokes logging, web browsing, search history, record audio/video, screen shots from the camaras, follow its GPS location, and so forth.

The NSO Group came to public awareness due to Citizen's Lab work. As part of the Munk School of Global Affairs and Public Policy at the University of Toronto, the Lab researched several cases of targeting of human rights defenders across the Middle-East (they previously exposed FinFisher and Hacking Team campaigns).

This research identified 19 sales to state users.

Probable User/Buyer

- Bahrain
- Croatia
- Honduras
- Hungary
- Kazakhstan
- Latvia
- Morocco
- Mozambique
- Nigeria
- Poland
- Saudi Arabia
- Switzerland
- Uzbekistan
- Zambia

Confirmed User/Buyer

- Mexico
- Panama
- United Arab Emirates
- Togo

The high-profile cases of the Pegasus include the targeting of Emirati human rights activist Ahmed Mansoor, several targets in Mexico public and private sector, Amnesty International and

Saudi dissidents (Omar Abdulaziz, Ghanem al-Masarir, and Yahya Assiri), and Togolese civil society (including a Catholic Bishop).

Another interesting fact is the lawsuit that Facebook and WhatsApp against NSO Group claiming it has engaged in unlawful conduct for exploiting an audio-calling vulnerability in WhatsApp. The action affected over 1400 app's customers. Several companies - such as Microsoft, Google, and Cisco - joined the action as amicus curiae in support of WhatsApp.

No definitive decision has been made, but the court acknowledged that NSO Group might be held responsible for the actions undertaken by its "sovereign" customers.

SS8

SS8 provides lawful interception and cyber offensive capabilities. Their line of products includes communications interception, social media monitoring, and analytics.

The hacking of Blackberry's phones offered by the United Arab Emirates mobile operator, Etisalat. The company also provided cyber offensive solutions for the GCHQ.

This research identified three sales to nation-states.

- Pakistan (Ufone)
- Suriname
- United Arab Emirates

Trovicor

Trovicor is a German company that has roots in the Siemens conglomerate and later initiatives with Nokia Siemens Networks (NSN), the latter known as Nokia Networks. It provides lawful interception, mobile locations, analytics, open-source intelligence, and cyber offensive capabilities.

The company's cyber offensive technologies deploy zero-day exploits provided by Gamma Group/FinFisher. Thus, features such as social engineering, phishing, gaining access to targets device, collecting information, and ultimately taking control of the device.

This research identified nine sales to state users, including Armed Forces, intelligence agencies and law enforcement agencies.

- Bahrain
- Bangladesh
- Egypt
- Ethiopia
- Oman
- Syria
- Tajikistan
- Tunisia
- Yemen

APPENDIX B - CYBER CAPABILITIES PURCHASES

Amesys Sales to Libya. Amesys. Retrieved from: Transparency Toolkit. Link: www.wsj.com/articles/SB10001424053111904199404576538721260166388

Amesys Sales to Syria (2007). Amesys. Retrieved from: Vice. Link: https://www.vice.com/en/article/nz75wd/european-surveillance-companies-agt-rcs-sell-syria-tools-of-oppression

Area SpA Sales to Egypt (2016). Area SpA. Retrieved from: Transparency Toolkit. Link: http://www.lastampa.it/2016/06/28/italia/litalia-esporter-software-di-sorveglianza-in-egitto-11iR9uYFcPpkP9PebyHdwM/pagina.htmlCustomer: Trd

Area SpA Sales to Syria (2009). Area SpA. Retrieved from: Transparency Toolkit. Link: http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.htmlCustomer: 225, Syrian intelligence

Cyberbit Sales to Ethiopia (2017). Cyberbit. Retrieved from: CitizenLab. Link: Citizen Lab, 'Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware', September 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Cyberbit Sales to Kazakhstan (2017). Cyberbit. Retrieved from: CitizenLab. Link: Citizen Lab, 'Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware', September 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/Customer: National Security Committee of the Republic of Kazakhstan

Cyberbit Sales to Philippines (2017). Cyberbit. Retrieved from: CitizenLab. Link: Citizen Lab, 'Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware', September 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/Customer: Philippine President’s Malacañang Palace

Cyberbit Sales to Thailand (2017). Cyberbit. Retrieved from: CitizenLab. Link: Citizen Lab, 'Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware', September 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/Customer: Royal Thai Army

Cyberbit Sales to Uzbekistan (2017). Cyberbit. Retrieved from: CitizenLab. Link: Citizen Lab, 'Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware', September 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/Customer: Uzbekistan’s National Security Service

Cyberbit Sales to Zambia (2017). Cyberbit. Retrieved from: CitizenLab. Link: Citizen Lab, 'Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware', September 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/Customer: Zambia’s Financial Intelligence Centre

Dreamlab Sales to Oman (2010). Dreamlab. Retrieved from: Transparency Toolkit. Link: www.corpwatch.org/article.php?id=15867Customer: Government of Oman

Dreamlab Sales to Turkmenistan (2010). Dreamlab. Retrieved from: Transparency Toolkit. Link: www.corpwatch.org/article.php?id=15867Customer: Government of Turkmenistan

Egypt Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Elbit Systems Sales to Nigeria. Elbit Systems. Retrieved from: Transparency Toolkit. Link: http://www.premiumtimesng.com/investigationspecial-reports/196964-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websitesinvestigation-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websites-2.htmlCustomer: National Security Adviser

Gamma International, FinFisher Sales to Angola. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Australia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Austria. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Bahrain (2010). Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://bahrainwatch.org/blog/2014/08/07/United Kingdom-spyware-used-to-hack-bahrain-lawyers-activists/

Gamma International, FinFisher Sales to Bangladesh. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Directorate General of Forces Intelligence (DGFI)

Gamma International, FinFisher Sales to Belgium. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Federal Police

Gamma International, FinFisher Sales to Bosnia and Herzegovina. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Brunei. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Bulgaria. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Canada. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Czech Republic. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Egypt. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Technology Research Department (TRD)

Gamma International, FinFisher Sales to Estonia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Ethiopia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Gabon. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Germany. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Hungary. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to India. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

"Gamma International, FinFisher Sales to Indonesia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: National Encryption Body (Lembaga Sandi Negara)

Unknown other entities"

Gamma International, FinFisher Sales to Italy. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Unknown multiple entities

Gamma International, FinFisher Sales to Japan. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Jordan. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Kazakhstan. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Kenya. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: National Intelligence Service (NIS)

Gamma International, FinFisher Sales to Latvia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

"Gamma International, FinFisher Sales to Lebanon (2015). Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: General Directorate of General Security

Internal Security Forces (ISF)"

Gamma International, FinFisher Sales to Lithuania. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Macedonia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Malaysia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Mexico. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Mongolia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Special State Security Department (SSSD)

"Gamma International, FinFisher Sales to Morocco. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Conseil Superieur De La Defense Nationale (CSDN)

Unknown other entities"

Gamma International, FinFisher Sales to Netherlands. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Nigeria. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Unknown multiple entities

Gamma International, FinFisher Sales to Oman. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Pakistan. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Panama (2009). Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/Customer: President Security

Gamma International, FinFisher Sales to Paraguay. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Qatar. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Romania. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Saudi Arabia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Serbia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Security Information Agency (BIA)

Gamma International, FinFisher Sales to Singapore. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Slovenia. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to South Africa. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Spain. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Taiwan. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Turkey. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Turkmenistan. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/Customer: Ministry of Communications

Gamma International, FinFisher Sales to Uganda (2012). Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://privacyinternational.org/sites/default/files/Uganda_Report.pdf

Gamma International, FinFisher Sales to United Arab Emirates. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to United Kingdom. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to United States of America. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Gamma International, FinFisher Sales to Venezuela. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Gamma International, FinFisher Sales to Vietnam. Gamma International, FinFisher. Retrieved from: Transparency Toolkit. Link: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Hacking Team Sales to Azerbaijan (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Azerbajan NS

Hacking Team Sales to Bahrain (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Midworld Barhein

Hacking Team Sales to Brazil (2015). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Brasil PF

Hacking Team Sales to Chile (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: PDI/DIE Chile

Hacking Team Sales to Colombia (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: DIPOL

Hacking Team Sales to Cyprus (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Intelligence

Hacking Team Sales to Czech Republic (2010). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: UZC

Hacking Team Sales to Ecuador (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: SENAIN

Hacking Team Sales to Egypt (2015). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Egypt TRD GNSE

Hacking Team Sales to Ethiopia (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Information Network Security Agency

Hacking Team Sales to Honduras (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Honduras

Hacking Team Sales to Hungary (2009). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: SSNS - Ungheria

Hacking Team Sales to Italy (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: AREA

Hacking Team Sales to Italy (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Guardia di Finanza

Hacking Team Sales to Kazakhstan (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: SIS of NSC

Hacking Team Sales to Lebanon (2015). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Lebanon Army Forces

Hacking Team Sales to Luxembourg (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: State security (Falcon)

Hacking Team Sales to Malaysia (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Malysia K

Hacking Team Sales to Mexico (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Jalisco Mexico

Hacking Team Sales to Mongolia (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: AC Mongolia

Hacking Team Sales to Morocco (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Morocco - DST

Hacking Team Sales to Nigeria (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Bayelsa State Government

Hacking Team Sales to Oman (2011). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Oman - Intelligence

Hacking Team Sales to Panama (2011). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: President Security

Hacking Team Sales to Poland (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: CBA Poland

Hacking Team Sales to Russia (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Russia - KVANT

Hacking Team Sales to Saudi Arabia (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: MOD Saudi

Hacking Team Sales to Singapore (2008). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: IDA SGP

Hacking Team Sales to South Korea (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: The 5163 Army Division

Hacking Team Sales to Spain (2006). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: CNI

Hacking Team Sales to Sudan (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: NISS - National Intelligence and Security Services

Hacking Team Sales to Switzerland (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Kantonspolizei Zurich

Hacking Team Sales to Thailand (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Royal Thai Army

Hacking Team Sales to Turkey (2011). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Turkish National Police

Hacking Team Sales to United Arab Emirates (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: UAE - Intelligence

Hacking Team Sales to United States of America (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Drug Enforcement Administration

Hacking Team Sales to Uzbekistan (2011). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: NSS

Hacking Team Sales to Vietnam (2015). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Vietnam GD1

Hacking Team, NICE Systems Sales to Nigeria (2012). Hacking Team, NICE Systems. Retrieved from: Transparency Toolkit. Link: http://saharareporters.com/2015/07/11/nigerian-governor-bayelsa-state-distributes-hacked-blackberry-phones-so-he-could-monitorCustomer: Bayelsa State Government

Indonesia Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Jordan Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Kuwait Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Malaysia Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Netsweeper systems Use in Afghanistan. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in Bahrain. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in India. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in Kuwait. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in Pakistan. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in Qatar. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in Somalia. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in Sudan. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in UAE. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

Netsweeper systems Use in Yemen. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/04/planet-netsweeper/

NICE Systems Sales to Colombia (2013). NICE Systems. Retrieved from: Transparency Toolkit. Link: Demand/Supply: Exposing the Surveillance Industry in Colombia', Privacy International, September 2015, https://www.privacyinternational.org/sites/default/files/DemandSupply_English.pdfCustomer: Police

NICE Systems Sales to Kazakhstan. NICE Systems. Retrieved from: Transparency Toolkit. Link: Private Interests: Monitoring Central Asia', Privacy International, Nov. 2014Customer: Committee of National Security (KNB)

NICE Systems Sales to Uganda (2015). NICE Systems. Retrieved from: Transparency Toolkit. Link: http://www.africaintelligence.com/ION/politics-power/2015/11/06/museveni-commits-dollars85.5%C2%A0million-to-monitor-the-web,108110202-ARTCustomer: Chieftaincy of Military Intelligence, Special Forces Command Counter Intelligence

NICE Systems Sales to Uzbekistan. NICE Systems. Retrieved from: Transparency Toolkit. Link: Private Interests: Monitoring Central Asia', Privacy International, Nov. 2014Customer: National Security Service (SNB)

NSO Group Sales to Bahrain. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Croatia. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Honduras. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Hungary. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Kazakhstan. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Latvia. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Mexico (2013). NSO Group. Retrieved from: Transparency Toolkit. Link: Barbara Opall-Rome, 'Israeli Smartphone Targeting System Cleared for Export', Defense News, Aug. 2013

NSO Group Sales to Morocco. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Mozambique. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Panama. NSO Group. Retrieved from: Transparency Toolkit. Link: Bamford, James, “The Espionage Economy”, Foreign Policy, 22 January 2016, http://foreignpolicy.com/2016/01/22/the-espionage-econom

NSO Group Sales to Poland. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Saudi Arabia. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Switzerland. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to UAE. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to United Arab Emirates. NSO Group. Retrieved from: Transparency Toolkit. Link: Citizen Lab, 'The Million Dollar Dissident: NSO Group’s iPhone Zero-Days used against a UAE Human Rights Defender', August 2016, https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

NSO Group Sales to Uzbekistan. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

NSO Group Sales to Zambia. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Oman Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Philippines Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Qatar Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

"Sandvine Use in Egypt. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/ Customer: Telecom Egypt"

Sandvine Use in Turkey. Sandvine. Retrieved from: CitizenLab. Link: https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/Customer: Türk Telekom's network

Saudi Arabia Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

Singapore Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

SS8 Sales to Pakistan. SS8. Retrieved from: Transparency Toolkit. Link: https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdfCustomer: Ufone

SS8 Sales to Suriname (2010). SS8. Retrieved from: Transparency Toolkit. Link: "List Of Contract Actions Matching Your Criteria: SS8", Federal Procurement Data System, 3 February 2016 https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=ss8Customer: Drug Enforcement Administration

SS8 Sales to United Arab Emirates (2009). SS8. Retrieved from: Transparency Toolkit. Link: http://news.bbc.co.uk/1/hi/8161190.stm

SS8 Sales to United States of America (2010). SS8. Retrieved from: Transparency Toolkit. Link: "List Of Contract Actions Matching Your Criteria: SS8", Federal Procurement Data System, 3 February 2016
https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=ss8Customer: Drug Enforcement Administration

Trovicor Sales to Bahrain (2009). Trovicor. Retrieved from: Transparency Toolkit. Link: http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networkingCustomer: Government of Bahrain

Trovicor Sales to Bangladesh. Trovicor. Retrieved from: Transparency Toolkit. Link: https://global.handelsblatt.com/edition/145/ressort/politics/article/big-brother-made-in-germanyCustomer: Directorate General of Forces Intelligence (DGFI)

Trovicor Sales to Egypt (2009). Trovicor. Retrieved from: Transparency Toolkit. Link: http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking

Trovicor Sales to Ethiopia (2010). Trovicor. Retrieved from: Transparency Toolkit. Link: https://www.privacyinternational.org/node/546

Trovicor Sales to Oman. Trovicor. Retrieved from: Transparency Toolkit. Link: Spy-tech firms Gamma and Trovicor target Shell Oil in Oman, https://www.theregister.com/2015/05/20/omani_intel_docs/

Trovicor Sales to Syria (2009). Trovicor. Retrieved from: Transparency Toolkit. Link: http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.htmlCustomer: Syriatel

Trovicor Sales to Tajikistan (2010). Trovicor. Retrieved from: Transparency Toolkit. Link: https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdfCustomer: Government of Tajikistan

Trovicor Sales to Tunisia. Trovicor. Retrieved from: Transparency Toolkit. Link: http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.htmlCustomer: Government of Tunisia

Trovicor Sales to Yemen (2009). Trovicor. Retrieved from: Transparency Toolkit. Link: http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking

United Arab Emirates Purchase of Intrusion software Technology (2015). . Retrieved from: Transparency Toolkit. Link: https://www.exportcontroldb.bis.gov.uk

NSO Group Sales to Togo. NSO Group. Retrieved from: CitizenLab. Link: Citizen Lab, 'Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware', August 2020, https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/

Hacking Team Sales to Mexico (2010). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: La Dependencia y/o Cisen

Hacking Team Sales to Mexico (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Estado del Mexico

Hacking Team Sales to Mexico (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Estado de Qeretaro

Hacking Team Sales to Mexico (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Governo de Puebla

Hacking Team Sales to Mexico (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Governo de Campeche

Hacking Team Sales to Mexico (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Mexico - PEMX

Hacking Team Sales to Mexico (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Mex Taumalipas

Hacking Team Sales to Mexico (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Sec. De Planeacion y Finanzas

Hacking Team Sales to Mexico (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Mexico Yucatan

Hacking Team Sales to Mexico (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Mexico Durango

Hacking Team Sales to Guatemala (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: MOI Guatemala

Hacking Team Sales to United States of America (2011). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: DOD

Hacking Team Sales to United States of America (2011). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: FBI

Hacking Team Sales to Egypt (2011). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Egypt - MOD

Hacking Team Sales to Sudan (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: NISS - National Intelligence and Security Services

Hacking Team Sales to Luxembourg (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: IR Authorities (Condor)

Hacking Team Sales to Spain (2006). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: CNI

Hacking Team Sales to United Arab Emirates (2012). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: UAE - MOI

Hacking Team Sales to Thailand (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Dept. of Correction Thai Police

Hacking Team Sales to Saudi Arabia (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: GIP Saudi

Hacking Team Sales to Saudi Arabia (2013). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Saudi - GID

Hacking Team Sales to Hungary (2008). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Information Office

Hacking Team Sales to Lithuania (2014). Hacking Team. Retrieved from: Transparency Toolkit. Link: https://wikileaks.org/hackingteam/emails/emailid/3168Customer: Lituania Criminal Police

NSO Group Sales to Nigeria (2012). NSO Group. Retrieved from: Premium Times Services. Link: Ogala Emmanuel, ‘How Governors Dickson, Okowa spend billions on high tech spying on opponents, others’, Premium Times Services, 2016Customer: Rivers State, Delta State e Bayelsa State

APPENDIX C - COUNTRIES PROFILES

In this appendix the information gathered about mentioned countries is compiled into an infographic profile. The purpose is to offer the reader an easy access to a summary of the findings regarding every nation-state.

The countries are ordered alphabetically, because it is not a ranking to list the most powerful countries in cyberspace. Rather, it is a synthesis of the data collected and analyzed during this research.

To graphically represent the results four variables are display into a radar chart:

- Offensive Capabilities - the value considers the launching of state-sponsored actions, the homegrown private companies selling cyber offensive technologies, APT originated from the country (not classified as state-sponsored action) or the acquisition of at least one cyber offensive capability from private vendors.
- Offensive Intent – the value ponders the launching of state-sponsored actions, the number of purchases of offensive capabilities, and the acquisition by intelligence agencies or armed forces.
- Target Frequency - index built with the number of cyber offensive actions that targeted each country. The data was normalized from 1 to 0, the former being the country most frequent targeted and the latter the least targeted.
- Freedom House Index - the overall value provided by the FOTW assessment for the 2020 report. The index was normalized from 0 to 1, the original values are from 0 to 100.

The information regarding the identified threat-groups (list), the objectives pursued with state-sponsored cyber offensive actions, homegrown private vendors (list), and the purchased cyber offensive capabilities (list) are also displayed in the profile.

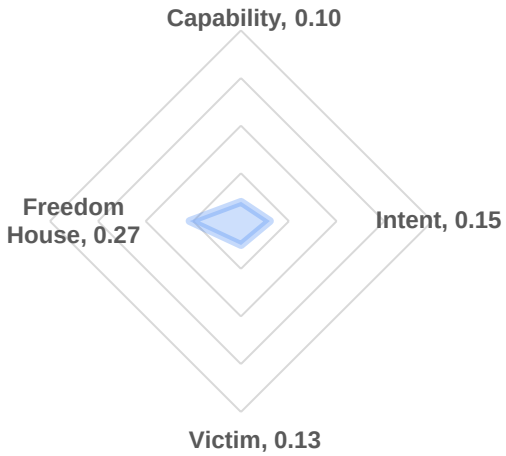
The total number of purchases and sales from a country is not restricted to cyber offensive technologies. The sources collected for this purpose provided evidence of a broader range of acquisitions that included monitoring centers, off-the-air telephone interception, satellite interception, and many other categories.

The data concerning the acquisition of cyber offensive technologies is also listed. The cases where the customers are identified (name and taxonomy) are highlighted because this correlation was alluded during the dissertation. In some cases, neither seller, nor the customer was identified (data extracted from exports reports).

Finally, a map also illustrates the origins of attacks against the country (Victim Profile). In the case of state-sponsored APTs the maps display the targets of those actions (Targeting Profile).

AFGHANISTAN

COUNTRY PROFILE



OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

FREEDOM HOUSE
Not Free (0.27)

VICTIM
Targeted in 11 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

THREAT ACTORS

No threat-actors found

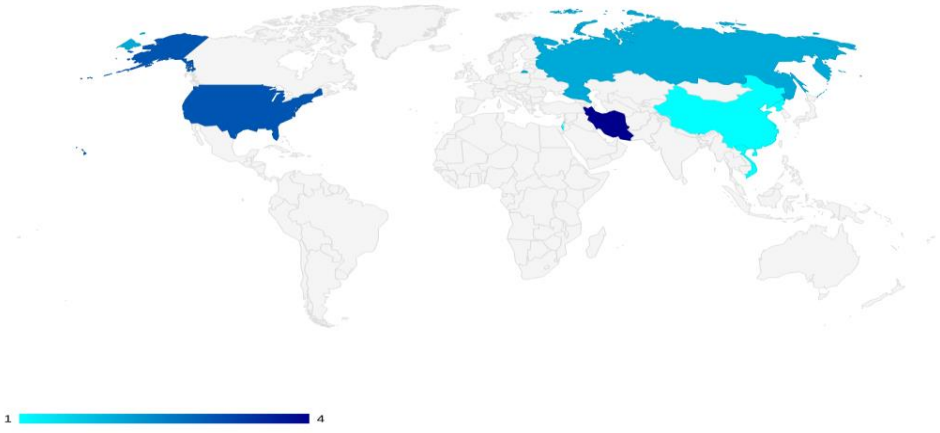
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Netsweeper systems Use in Afghanistan

VICTIM PROFILE



ALGERIA

OFFENSIVE ACTIONS
Homegrown APTs (1)

CYBER TECH EXCHANGE
No sales or purchases found

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

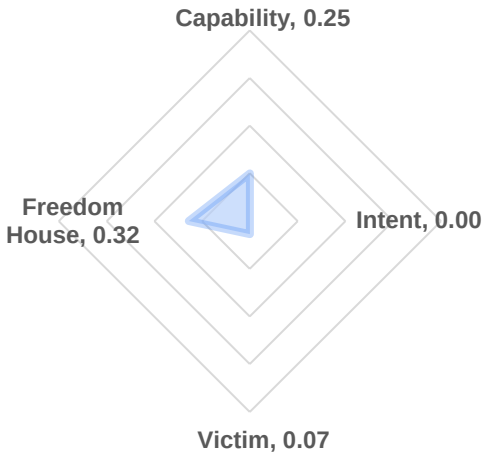
FREEDOM HOUSE
Not Free (0.32)

VICTIM
Targeted in 6 documents

THREAT ACTORS
APT Threat Actors (1)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

APT-C-44 (2020)

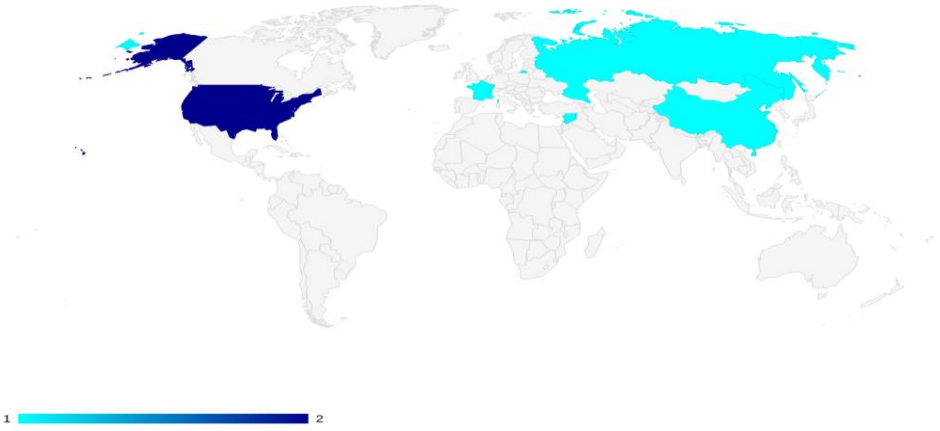
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

VICTIM PROFILE



AUSTRALIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

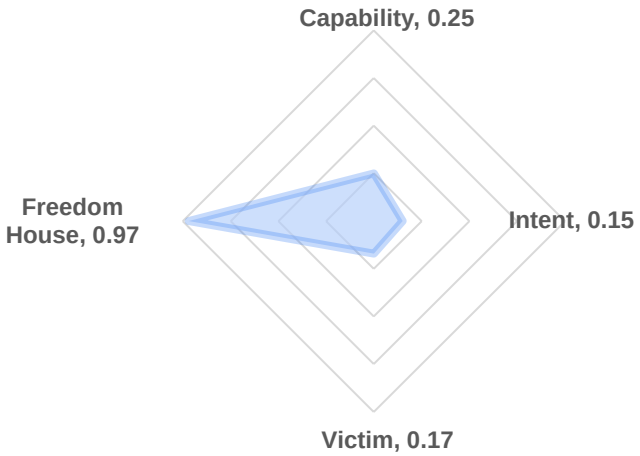
FREEDOM HOUSE
Free (0.97)

VICTIM
Targeted in 15 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 5 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

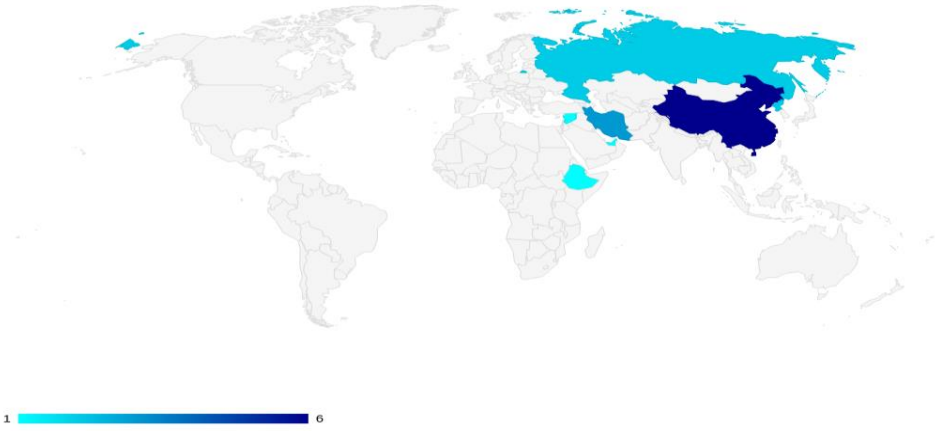
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Australia

VICTIM PROFILE



AUSTRIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

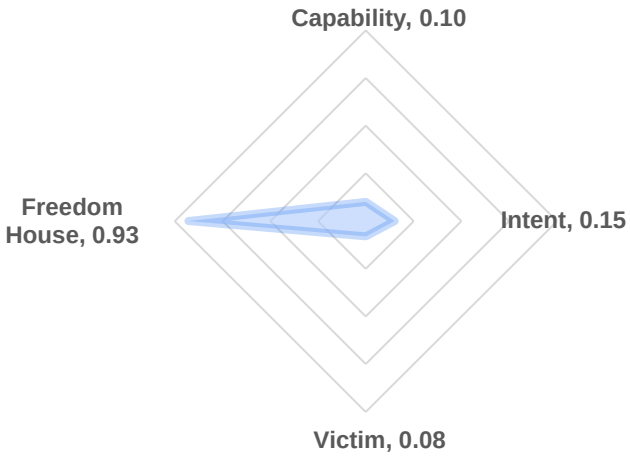
FREEDOM HOUSE
Free (0.93)

VICTIM
Targeted in 7 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 3 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

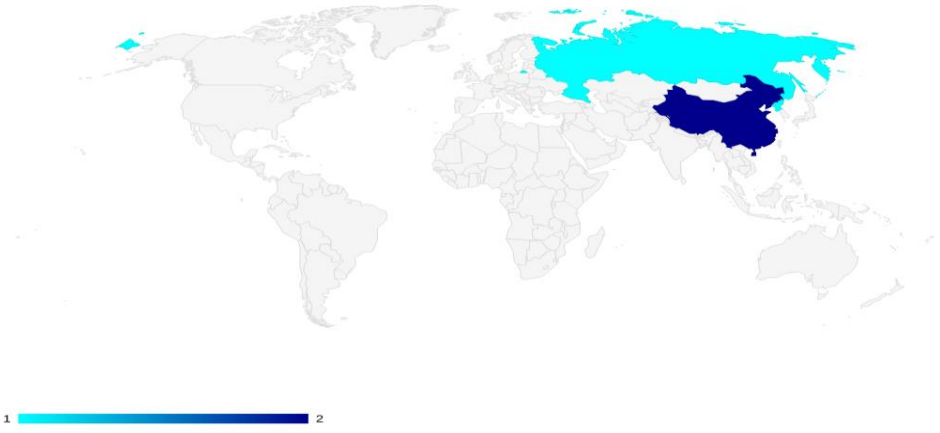
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Austria

VICTIM PROFILE



AZERBAIJAN

OFFENSIVE ACTIONS
Homegrown APTs (3)

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

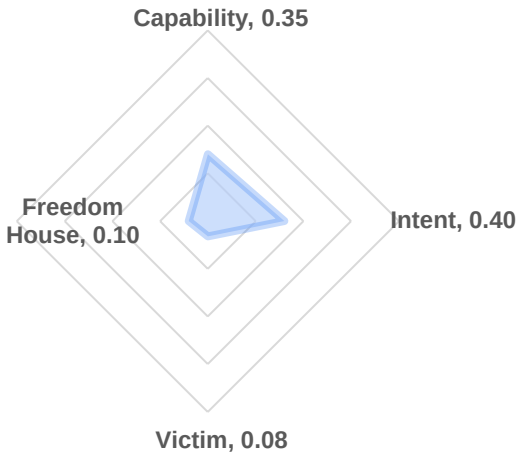
FREEDOM HOUSE
Not Free (0.1)

VICTIM
Targeted in 7 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

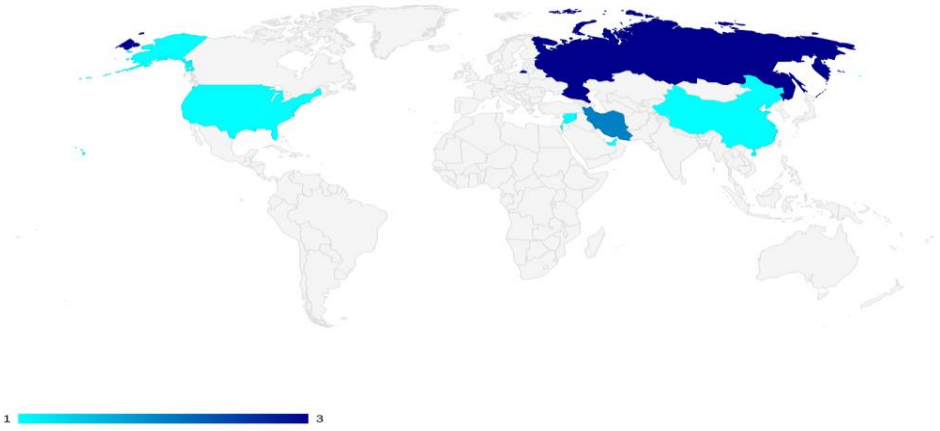
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Azerbaijan (Azerbajan NS / Intelligence) - 2013

VICTIM PROFILE



BAHRAIN

OFFENSIVE ACTIONS
State-Sponsored APTs (2)
Homegrown APTs (2)

CYBER TECH EXCHANGE
Purchases (5)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Espionage (1), Surveillance (1)

FREEDOM HOUSE
Not Free (0.12)

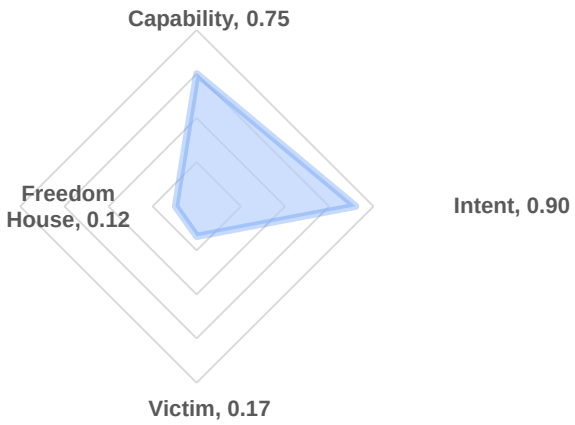
VICTIM
Targeted in 15 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

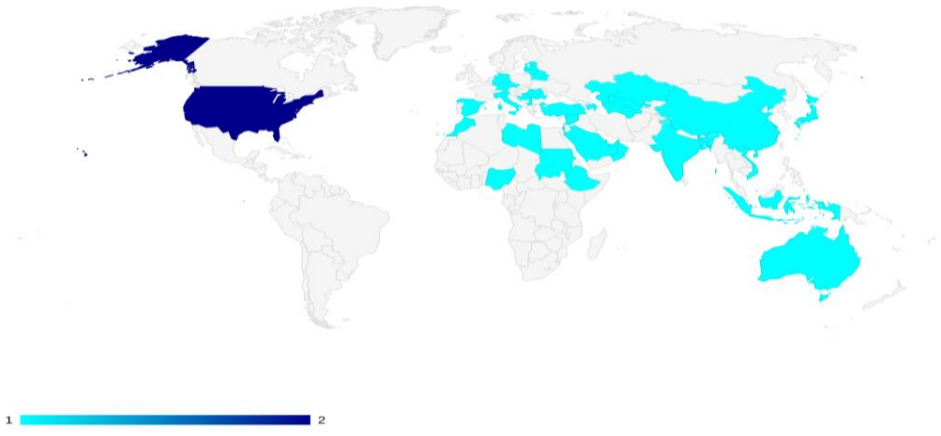
OFFENSIVE PRIVATE VENDORS

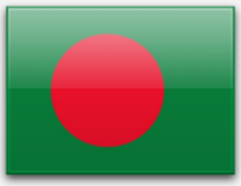
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Netsweeper systems Use in Bahrain
NSO Group Sales to Bahrain
FinFisher Sales to Bahrain - 2010
Trovicor Sales to Bahrain (Government of Bahrain / Civil) - 2009
Hacking Team Sales to Bahrain (Midworld Barhein / Civil) – 2013

TARGETING PROFILE





BANGLADESH

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

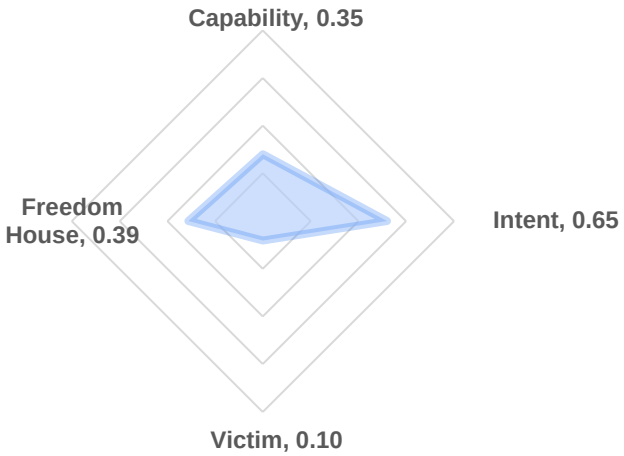
FREEDOM HOUSE
Partly Free (0.39)

VICTIM
Targeted in 9 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

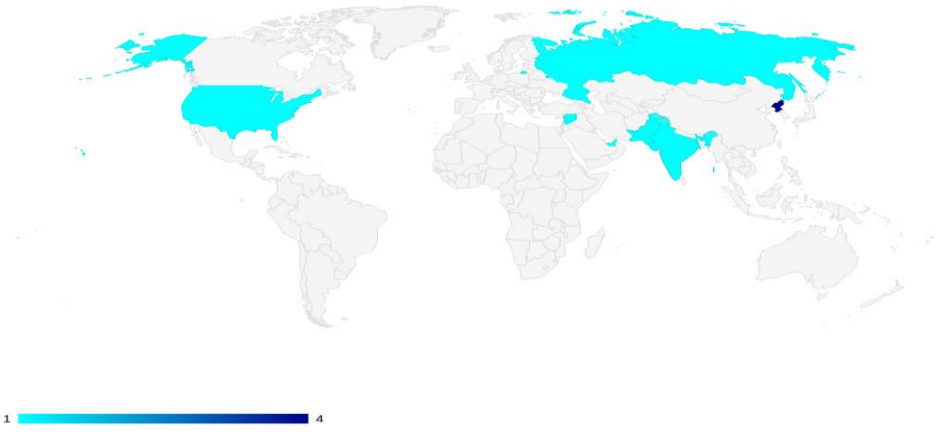
Ezzy Enterprise (Internet Monitoring, Intrusion, Phone Monitoring)

PURCHASED CAPABILITIES

FinFisher Sales to Bangladesh (Directorate General of Forces Intelligence (DGFI) / Intelligence)

Trovicor Sales to Bangladesh (Directorate General of Forces Intelligence (DGFI) / Intelligence)

VICTIM PROFILE



BELGIUM

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

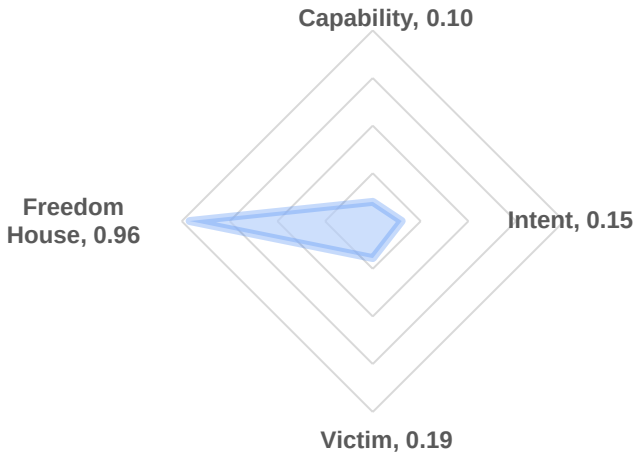
FREEDOM HOUSE
Free (0.96)

VICTIM
Targeted in 17 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 2 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

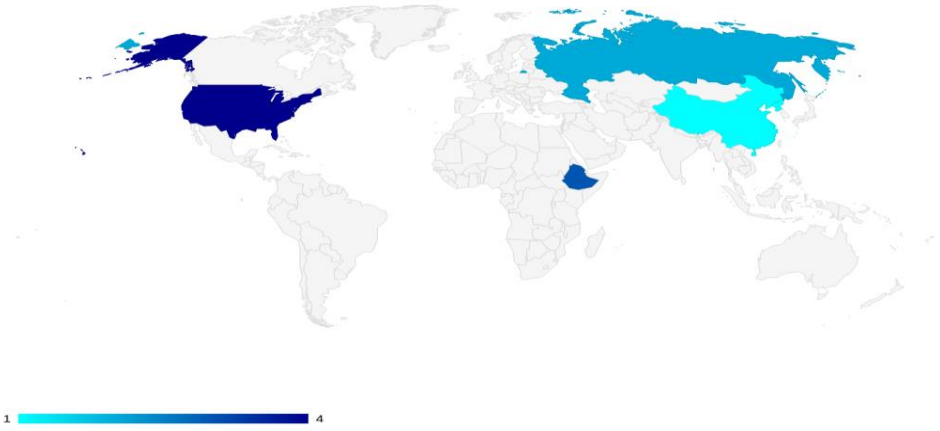
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Belgium (Federal Police / LEA)

VICTIM PROFILE



BOSNIA AND HERZEGOVINA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

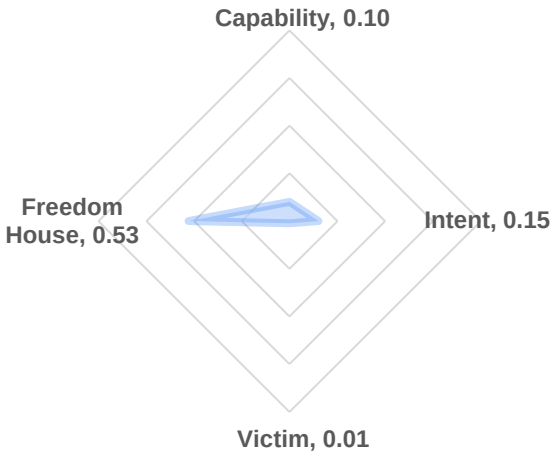
FREEDOM HOUSE
Partly Free (0.53)

VICTIM
Targeted in 1 document

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Bosnia and Herzegovina

VICTIM PROFILE

BRAZIL

OFFENSIVE ACTIONS
Homegrown APTs (5)

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

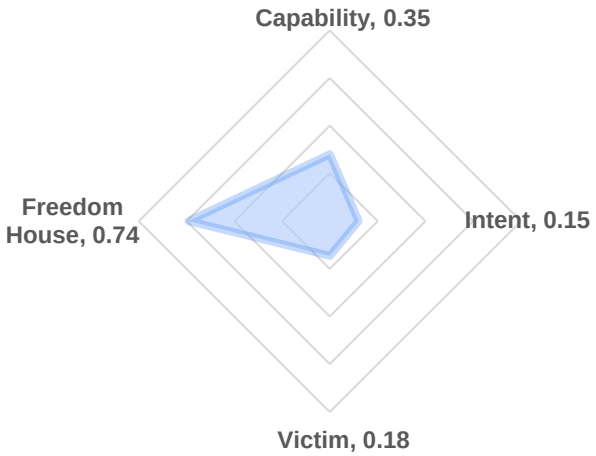
FREEDOM HOUSE
Free (0.74)

VICTIM
Targeted in 16 documents

THREAT ACTORS
APT Threat Actors (2)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

Operation Comando (2018)

Poseidon Group (2005)

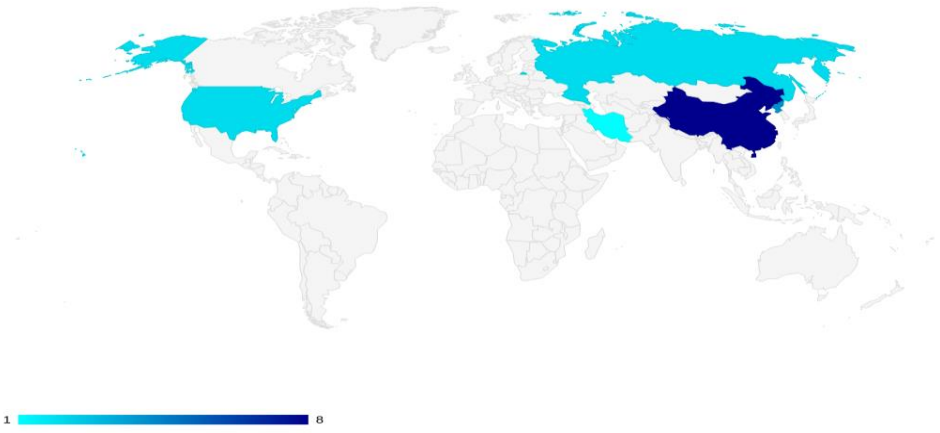
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Brazil (DPF / LEA) - 2015

VICTIM PROFILE



BRUNEI DARUSSALAM

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

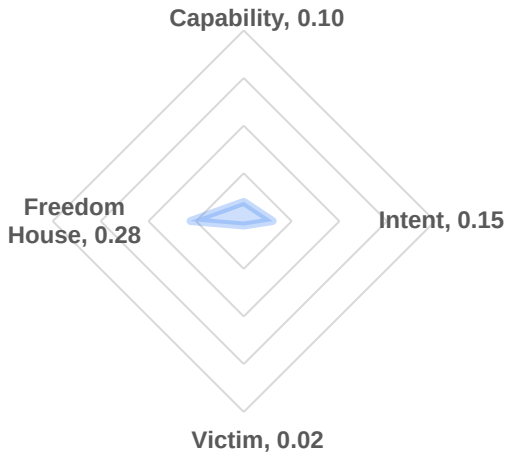
FREEDOM HOUSE
Not Free (0.28)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

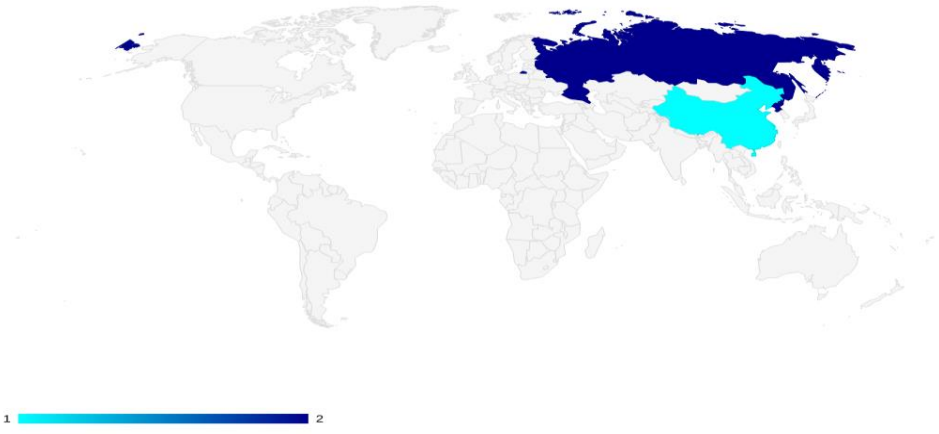
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Brunei

VICTIM PROFILE



BULGARIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

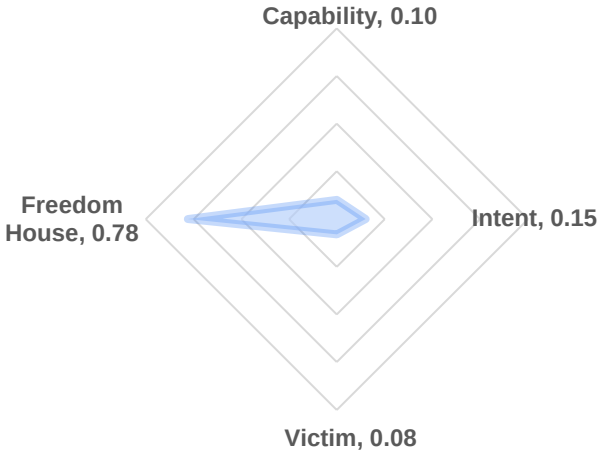
FREEDOM HOUSE
Free (0.78)

VICTIM
Targeted in 7 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

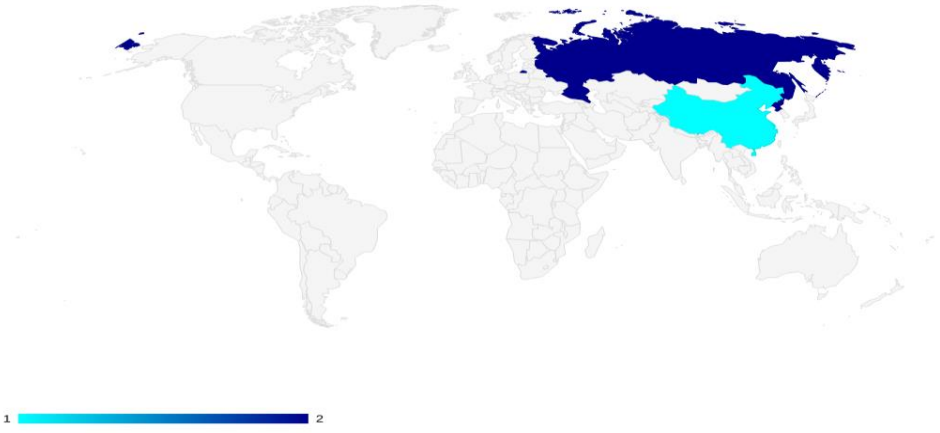
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Bulgaria

VICTIM PROFILE



CANADA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (12)
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

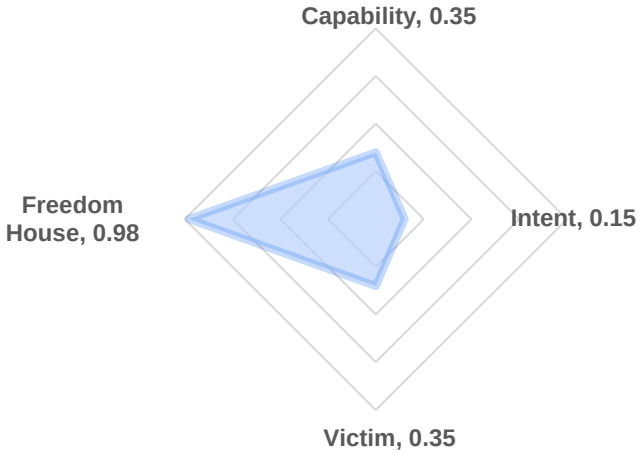
FREEDOM HOUSE
Free (0.98)

VICTIM
Targeted in 31 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 15 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

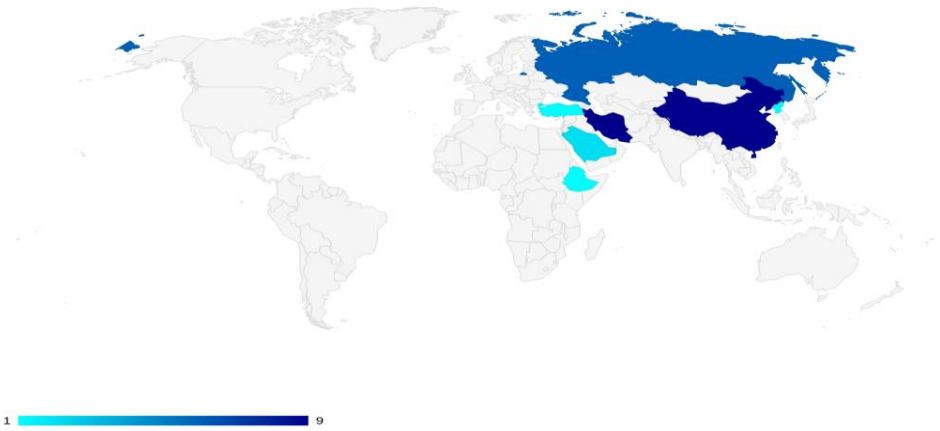
CRU (Intrusion)

Netsweeper (Internet Monitoring)

PURCHASED CAPABILITIES

FinFisher Sales to Canada

VICTIM PROFILE



CHILE

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

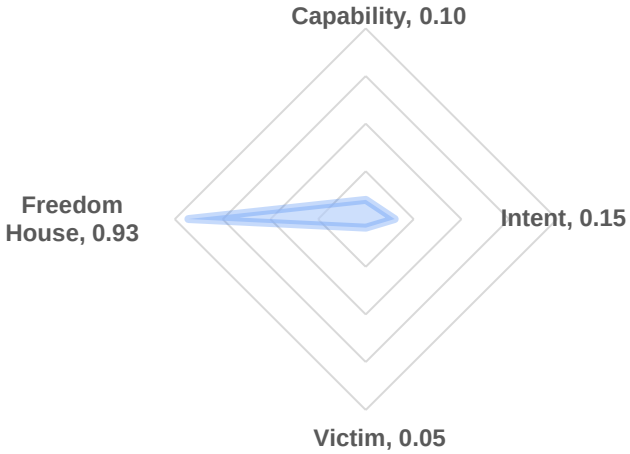
FREEDOM HOUSE
Free (0.93)

VICTIM
Targeted in 4 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

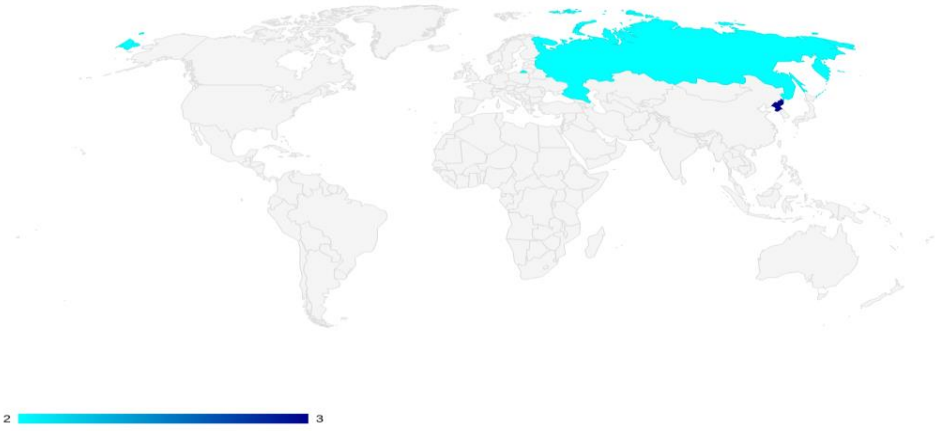
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Chile (PDI/DIE Chile / LEA) - 2014

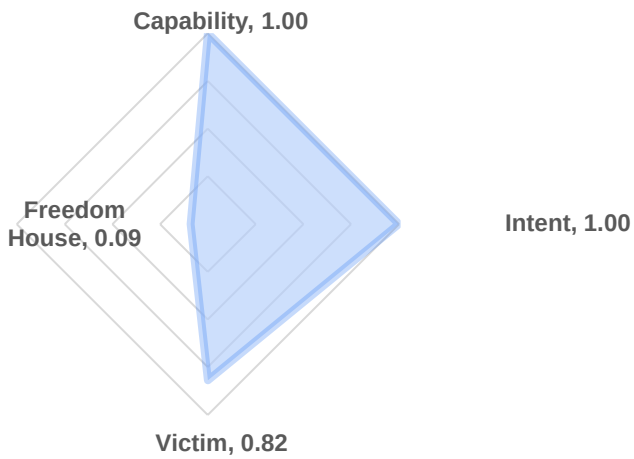
VICTIM PROFILE



COUNTRY PROFILE

Global Power

CHINA



OFFENSIVE ACTIONS

State-Sponsored APTs (75)
Homegrown APTs (229)

CYBER TECH EXCHANGE

Sales (7)

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (23), Surveillance (5), Disinformation (1), Crime (10)

FREEDOM HOUSE

Not Free (0.09)

VICTIM

Targeted in 72 documents

THREAT ACTORS

THREAT ACTORS

Anchor Panda (State-sponsored, PLA Navy) - 2012

APT 3 (State-sponsored, Ministry of State Security and Internet security firm Guangzhou Bo Yu Information Technology Company Limited ("Boyusec")) - 2007

APT 4 (State-sponsored, PLA Navy) - 2007

APT 12 - 2009

APT 17 (State-sponsored, Jinan bureau of the Chinese Ministry of State Security) - 2009

APT 18 (State-sponsored, PLA Navy) - 2009

APT 19 (A group likely composed of freelancers, with some degree of sponsorship by the Chinese government. (FireEye)) - 2013

APT 30 - 2005

APT 31 - 2016

APT 41 - 2012

Axiom - 2008

Barium - 2016

BlackTech - 2010

Bronze Butler (State-sponsored, National University of Defense and Technology) - 2010

Comment Crew (State-sponsored, 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398) - 2006

Icefog - 2011

Ke3chang - 2010

Lead APT - 2016

Leviathan (State-sponsored, Hainan province) - 2013

Lotus Blossom - 2012

Naikon (State-sponsored, PLA Unit 78020) - 2012

Operation Shady RAT - 2006

State-Sponsored (34)
APT Threat Actors (118)

PRIVATE VENDORS

There are 8 private vendors

Operation Titan Rain (State-sponsored, PLA Unit 61398) - 2003

PassCV - 2016

Putter Panda (State-sponsored, Unit 61486 of the 12th Bureau of the PLA's 3rd General Staff Department (GSD)) - 2007

RedAlpha (State-sponsored, possibly PLA and/or Nanjing Qinglan Information Technology Co. Ltd) - 2015

RedDelta - 2020

Samurai Panda (State-sponsored, PLA Navy) - 2009

Stone Panda (State-sponsored, Tianjin bureau of the Chinese Ministry of State Security, Huaying Haitai) - 2006

Tonto Team (State-sponsored, Shenyang Military Region Technical Reconnaissance Bureau, possibly Unit 65017) - 2009

Tropic Trooper - 2011

Turbine Panda (State-sponsored, the Jiangsu Bureau of the MSS (JSSD/????????)) - 2010

Winnti Group - 2010

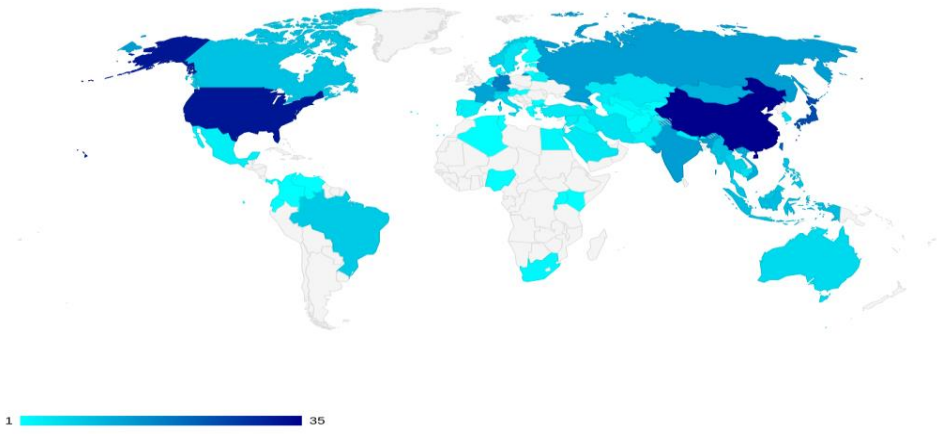
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

TARGETING PROFILE



COLOMBIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

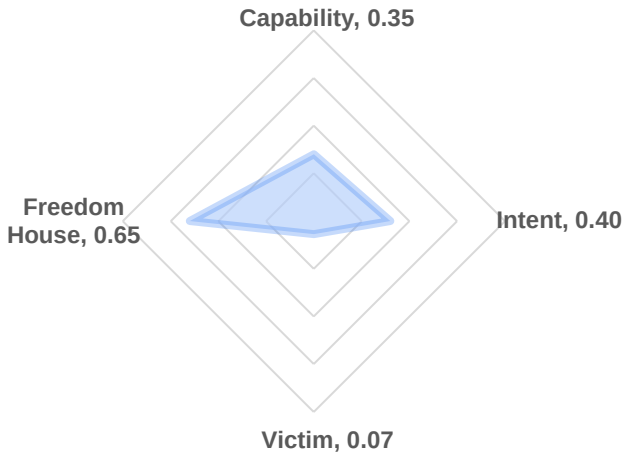
FREEDOM HOUSE
Partly Free (0.65)

VICTIM
Targeted in 6 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 2 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

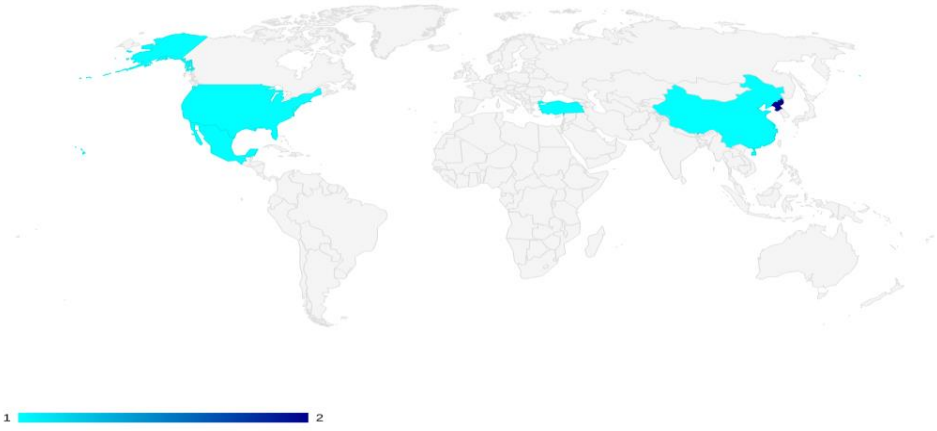
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

NICE Systems Sales to Colombia (Police / LEA) - 2013

Hacking Team Sales to Colombia (DIPOL / LEA) - 2013

VICTIM PROFILE



CROATIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

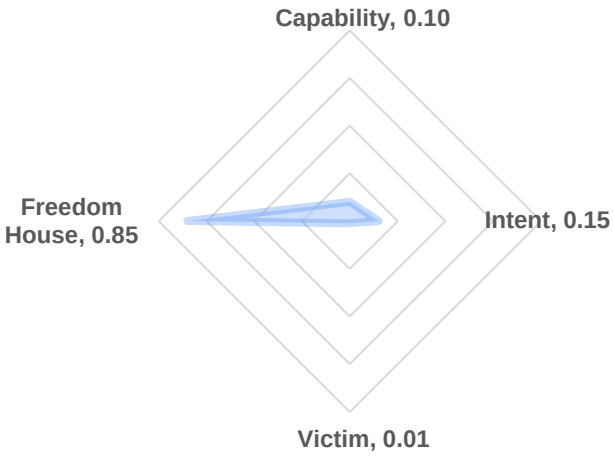
FREEDOM HOUSE
Free (0.85)

VICTIM
Targeted in 1 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

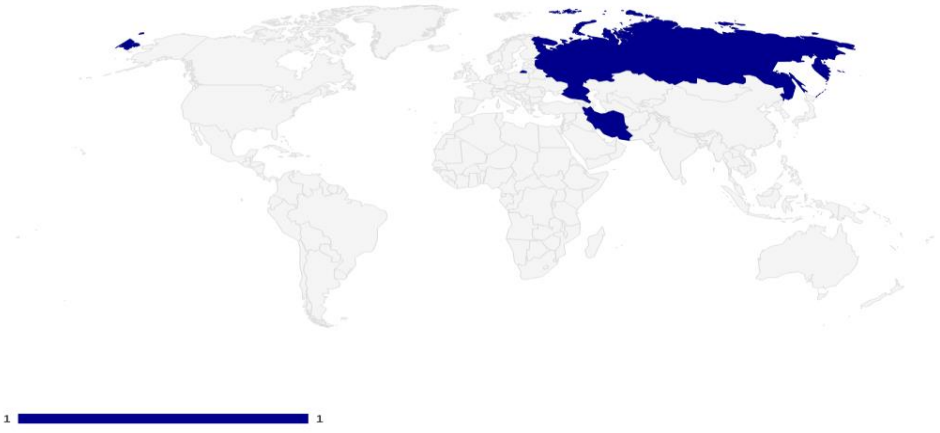
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

NSO Group Sales to Croatia

VICTIM PROFILE



CYPRUS

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

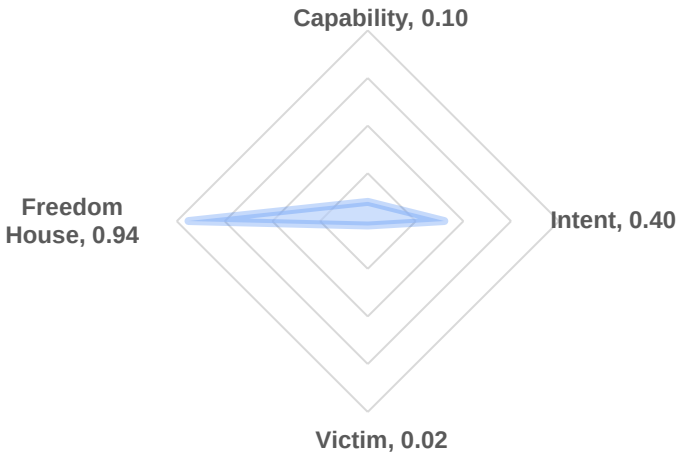
FREEDOM HOUSE
Free (0.94)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

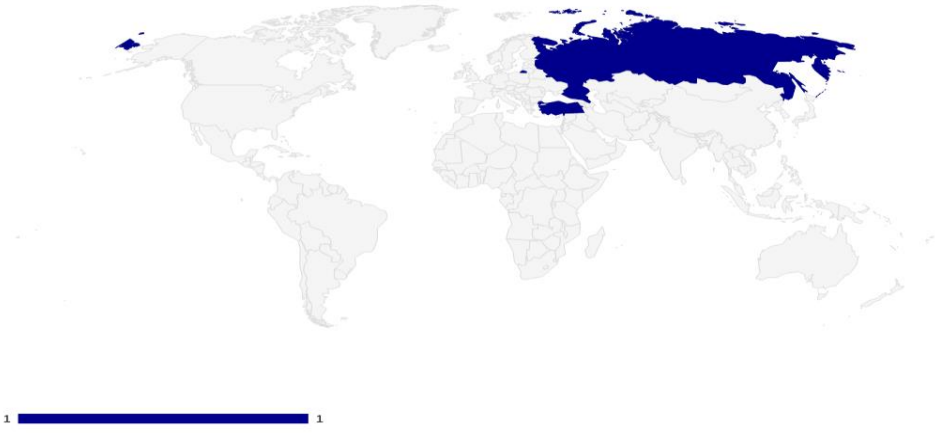
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Cyprus (Intelligence / Intelligence) - 2013

VICTIM PROFILE



CZECHIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

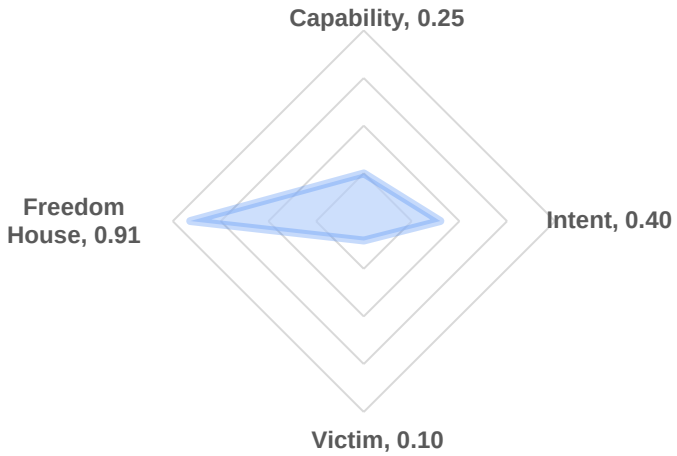
FREEDOM HOUSE
Free (0.91)

VICTIM
Targeted in 9 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 8 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

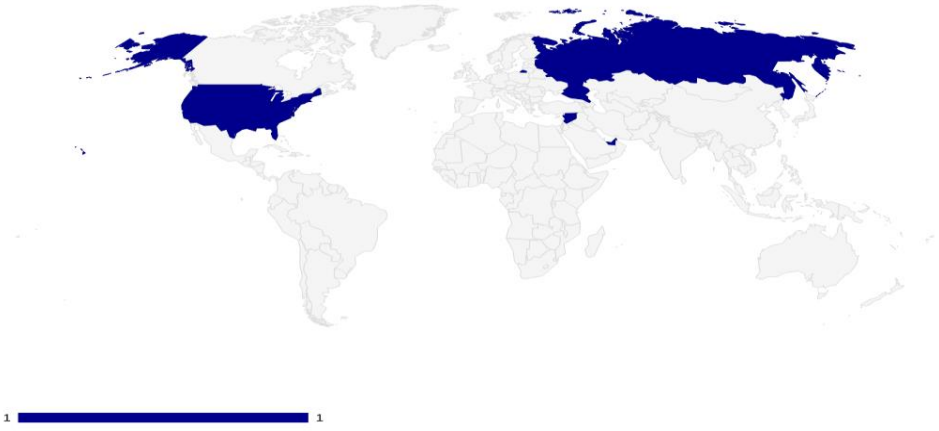
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Czech Republic

Hacking Team Sales to Czech Republic (UZC / LEA) - 2010

VICTIM PROFILE



DENMARK

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (6)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

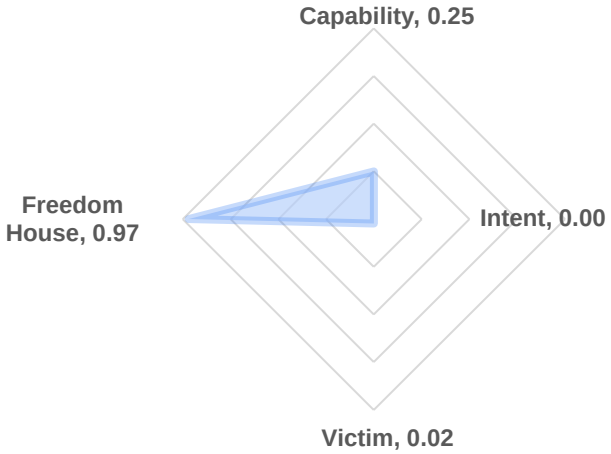
FREEDOM HOUSE
Free (0.97)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 7 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

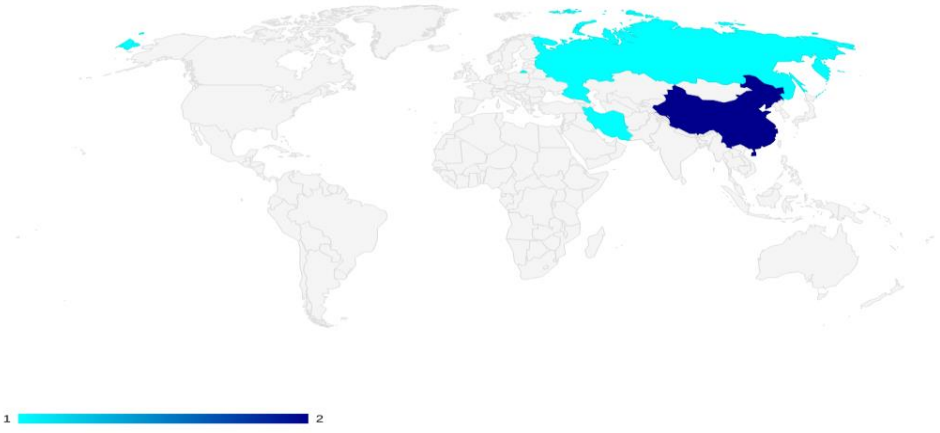
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

VICTIM PROFILE



ECUADOR

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

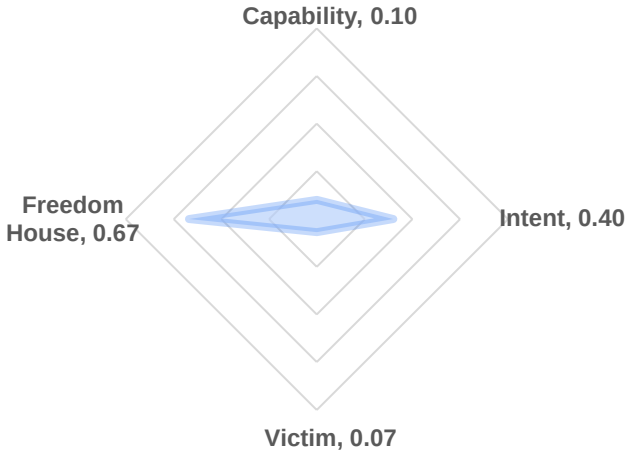
FREEDOM HOUSE
Partly Free (0.67)

VICTIM
Targeted in 6 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

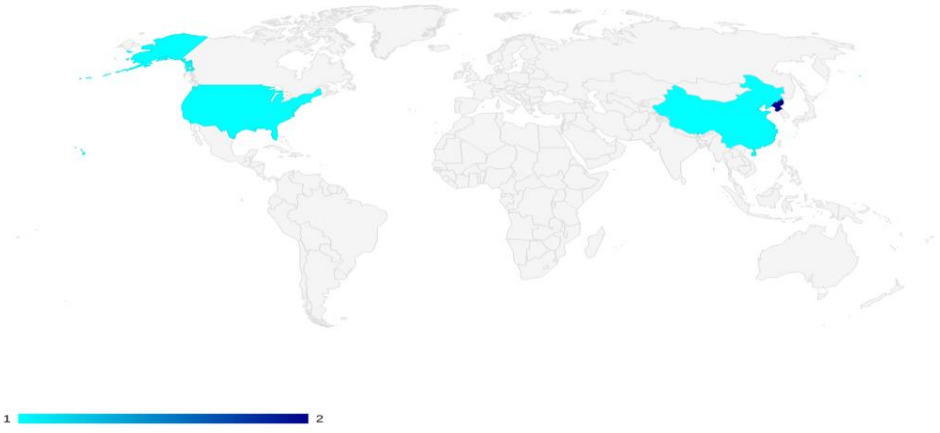
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Ecuador (SENAIN / Intelligence) - 2013

VICTIM PROFILE



EGYPT

OFFENSIVE ACTIONS
State-Sponsored APTs (4)
Homegrown APTs (3)

CYBER TECH EXCHANGE
Purchases (7)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
Surveillance (1)

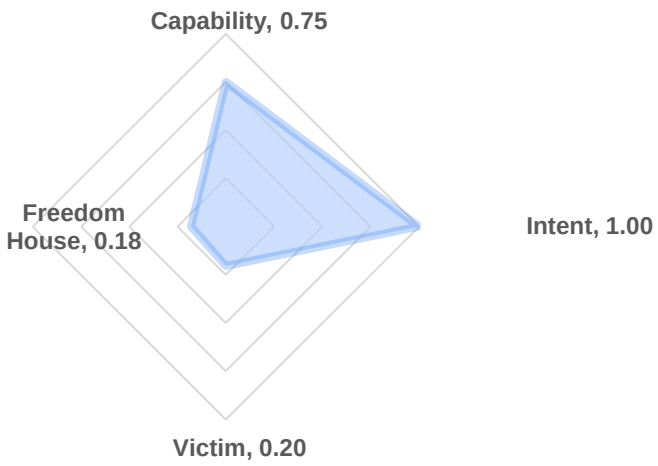
FREEDOM HOUSE
Not Free (0.18)

VICTIM
Targeted in 18 documents

THREAT ACTORS
No threat-actors found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

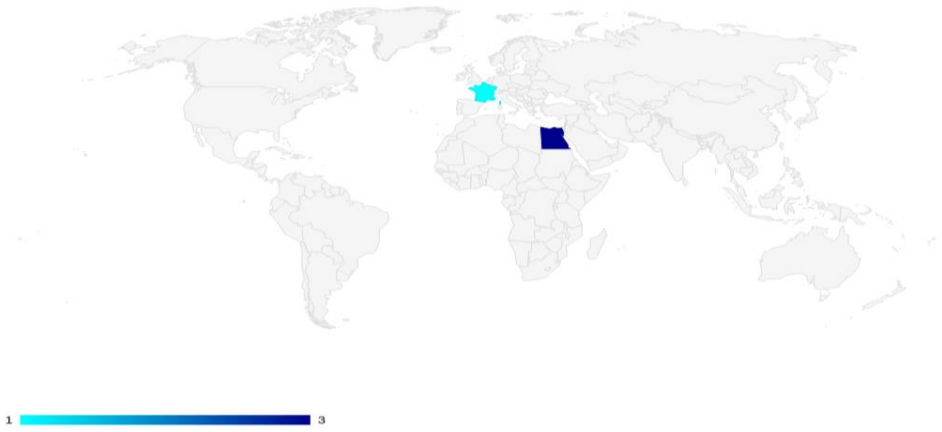
PURCHASED CAPABILITIES

Area SpA Sales to Egypt (Trd / Intelligence) - 2016
Egypt Purchase of Intrusion software Techology - 2015
Trovicor Sales to Egypt - 2009
FinFisher Sales to Egypt (Technology Research Department (TRD) / Intelligence)
Hacking Team Sales to Egypt (Egypt - MOD / Intelligence) - 2011
Hacking Team Sales to Egypt (Egypt TRD GNSE / Intelligence) – 2015

PRIVATE VENDORS

There are 1 private vendors

TARGETING PROFILE



ESTONIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

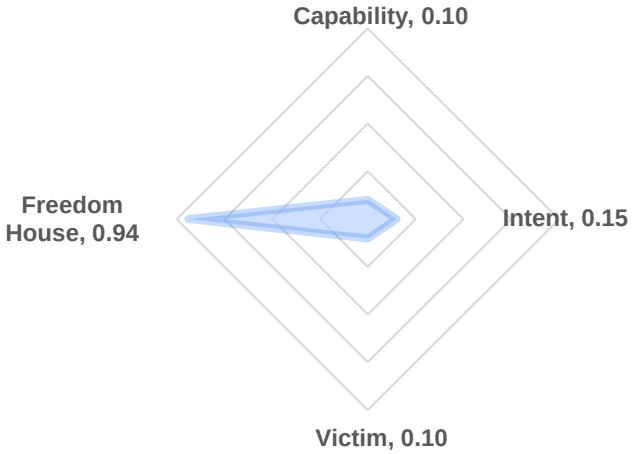
FREEDOM HOUSE
Free (0.94)

VICTIM
Targeted in 9 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

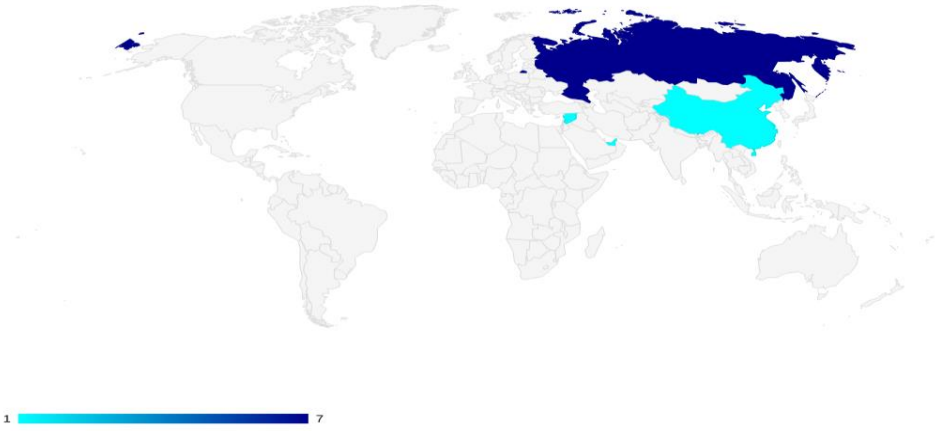
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Estonia

VICTIM PROFILE



ETHIOPIA

OFFENSIVE ACTIONS
State-Sponsored APTs (5)
Homegrown APTs (2)

CYBER TECH EXCHANGE
Purchases (4)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Espionage (1), Surveillance (1)

FREEDOM HOUSE
Not Free (0.22)

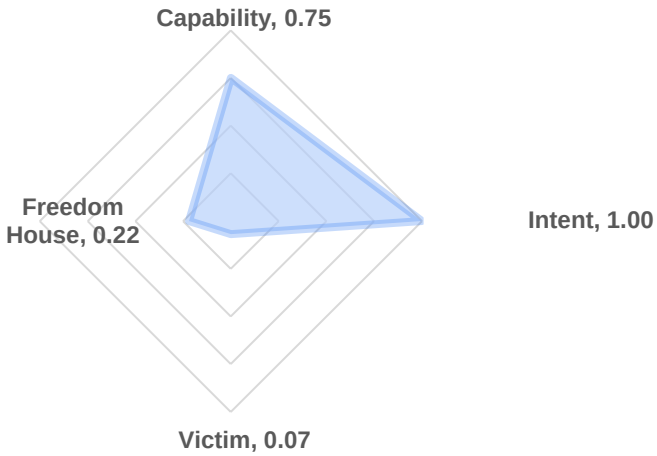
VICTIM
Targeted in 6 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

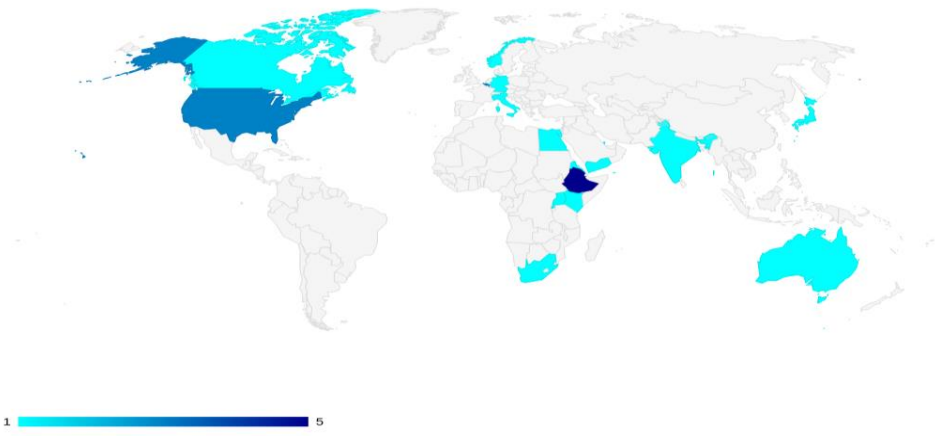
Cyberbit Sales to Ethiopia - 2017

Trovicor Sales to Ethiopia - 2010

FinFisher Sales to Ethiopia

Hacking Team Sales to Ethiopia (Information Network Security Agency / Intelligence) - 2012

TARGETING PROFILE



FINLAND

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (16)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

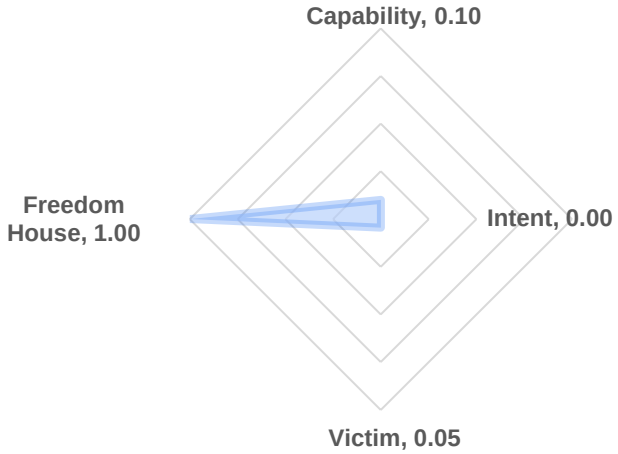
FREEDOM HOUSE
Free (1)

VICTIM
Targeted in 4 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 2 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

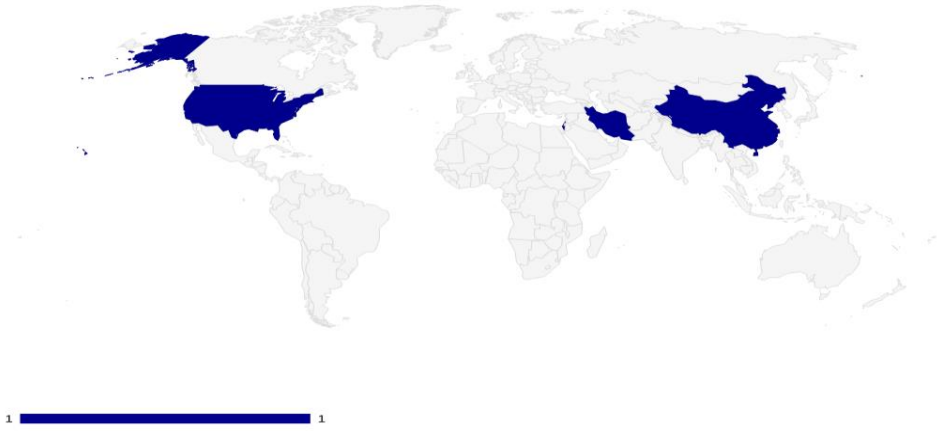
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

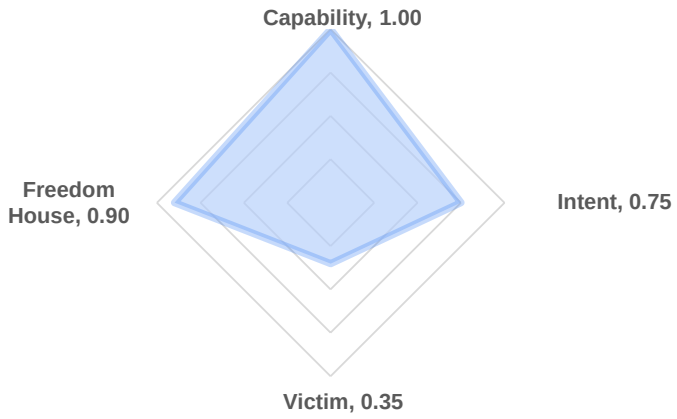
No purchases found

VICTIM PROFILE



COUNTRY PROFILE

Regional Contender



FRANCE

OFFENSIVE ACTIONS

State-Sponsored APTs (3)
Homegrown APTs (4)

CYBER TECH EXCHANGE

Sales (4)

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (3)

FREEDOM HOUSE

Free (0.9)

VICTIM

Targeted in 31 documents

THREAT ACTORS

State-Sponsored (1)
APT Threat Actors (3)

THREAT ACTORS

Snowglobe (2011)

OFFENSIVE PRIVATE VENDORS

Amesys (Internet Monitoring, Monitoring Centre, Audio Surveillance, Counter-Surveillance, Location Monitoring, Equipment, Monitoring Centres)

Bull Group (Analysis, Internet Monitoring, Phone Monitoring, Biometrics, Communications Monitoring)

Nexa Technologies (Internet Monitoring)

Qosmos (Internet Monitoring, Monitoring Centre, Analysis, Monitoring Centres)

VUPEN (Intrusion, Counter-Surveillance)

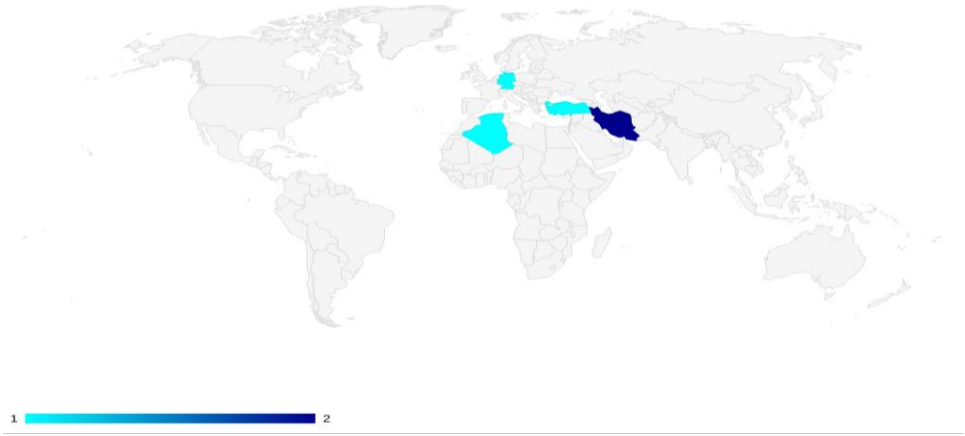
PURCHASED CAPABILITIES

No purchases found

PRIVATE VENDORS

There are 45 private vendors

TARGETING PROFILE



GERMANY

OFFENSIVE ACTIONS

No offensive actions found

CYBER TECH EXCHANGE

Sales (115)
Purchases (1)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

No objectives found

FREEDOM HOUSE

Free (0.94)

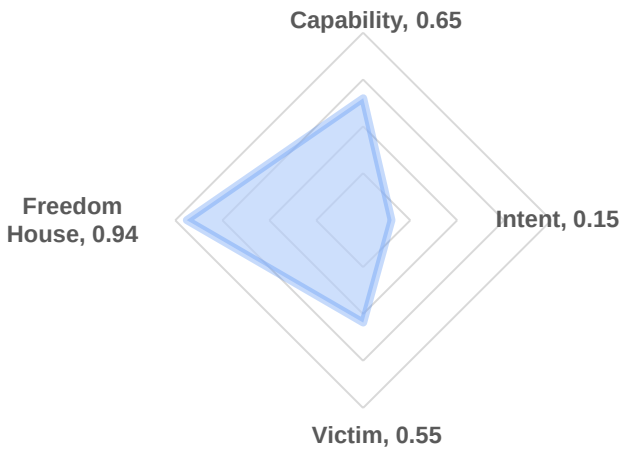
VICTIM

Targeted in 48 documents

THREAT ACTORS

APT Threat Actors (1)

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

DigiTask (Internet Monitoring, Intrusion, Location Monitoring)

Elaman (Internet Monitoring, Intrusion, Phone Monitoring, Monitoring Centre, Location Monitoring, Audio Surveillance, Video Surveillance, Analysis, Equipment, Monitoring Centres, Communications Monitoring, Technical Surveillance)

Gamma Group (Trojans , Tactical Interception)

MIB Electronic (Intrusion, Phone Monitoring, Audio Surveillance)

Trovicor (Monitoring Centre, Monitoring Centres)

Wolf Intelligence (Intrusion)

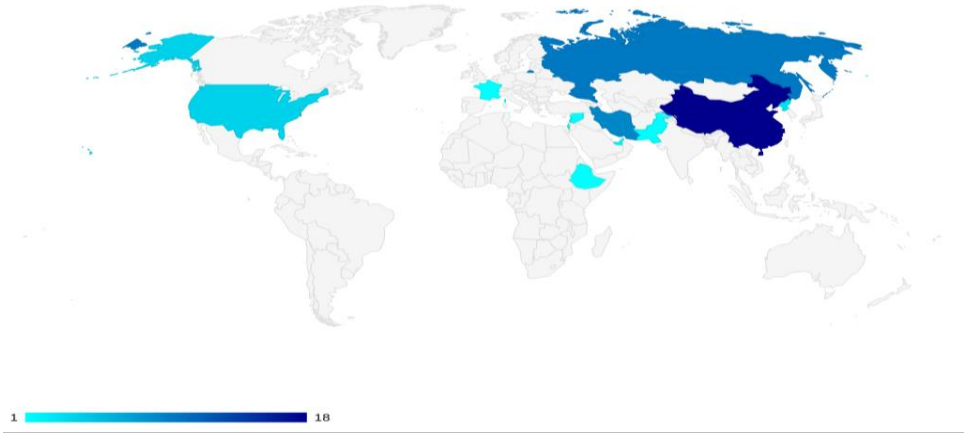
PURCHASED CAPABILITIES

FinFisher Sales to Germany

VICTIM PROFILE

PRIVATE VENDORS

There are 45 private vendors



GUATEMALA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

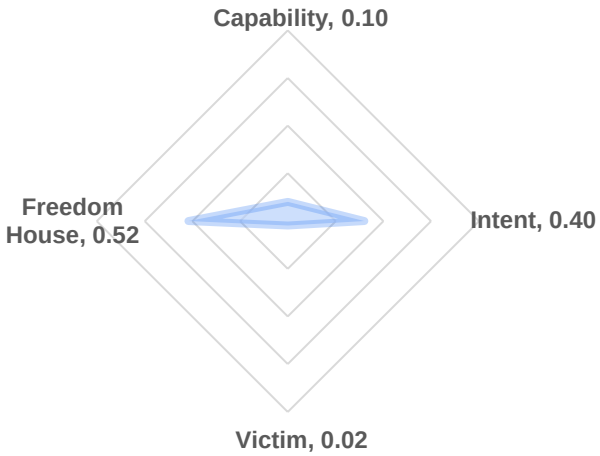
FREEDOM HOUSE
Partly Free (0.52)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

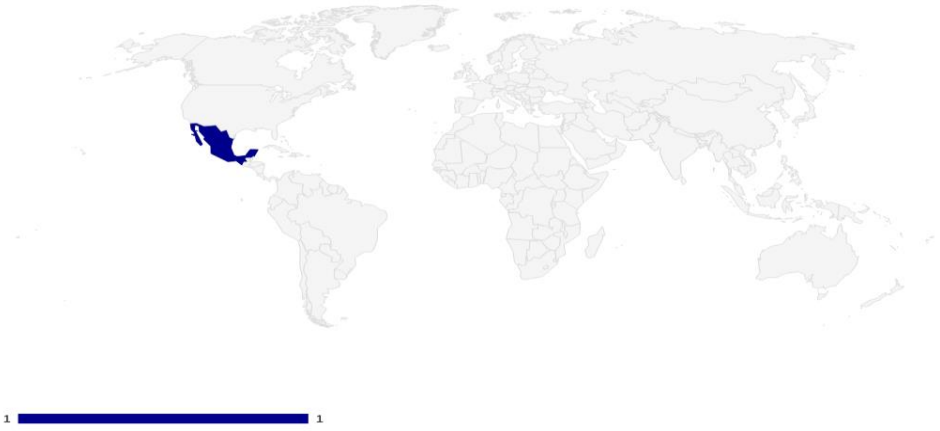
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Guatemala (MOI Guatemala / Intelligence) - 2014

VICTIM PROFILE



HUNGARY

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (4)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

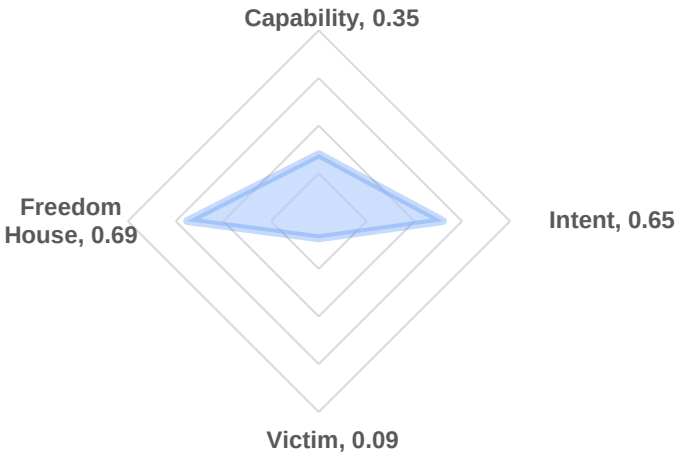
FREEDOM HOUSE
Partly Free (0.69)

VICTIM
Targeted in 8 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 3 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

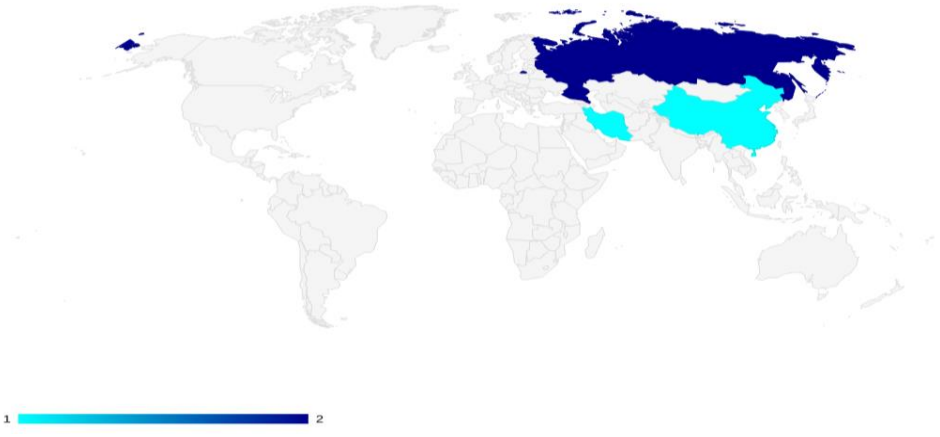
NSO Group Sales to Hungary

FinFisher Sales to Hungary

Hacking Team Sales to Hungary (SSNS - Ungheria / Intelligence) - 2009

Hacking Team Sales to Hungary (Information Office / Intelligence) - 2008

VICTIM PROFILE



INDIA

OFFENSIVE ACTIONS

State-Sponsored APTs (3)
Homegrown APTs (22)

CYBER TECH EXCHANGE

Purchases (2)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

Espionage (1), Crime (1)

FREEDOM HOUSE

Partly Free (0.67)

VICTIM

Targeted in 56 documents

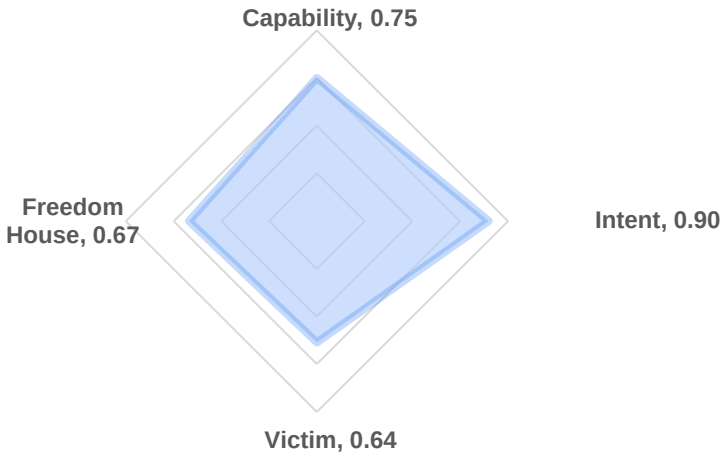
THREAT ACTORS

State-Sponsored (1)
APT Threat Actors (6)

PRIVATE VENDORS

COUNTRY PROFILE

Regional Contender



THREAT ACTORS

Confucius (2013)

Operation HangOver (2010)

Patchwork (2013)

SideWinder (2012)

Dark Basin (2013)

OFFENSIVE PRIVATE VENDORS

Aglaya (Intrusion)

ClearTrail (Intrusion, Monitoring Centre, Phone Monitoring, Internet Monitoring, Monitoring Centres, Communications Monitoring)

Paladion Networks (Internet Monitoring, Phone Monitoring, Intrusion, Monitoring Centre, Analysis, Monitoring Centres, Communications Monitoring)

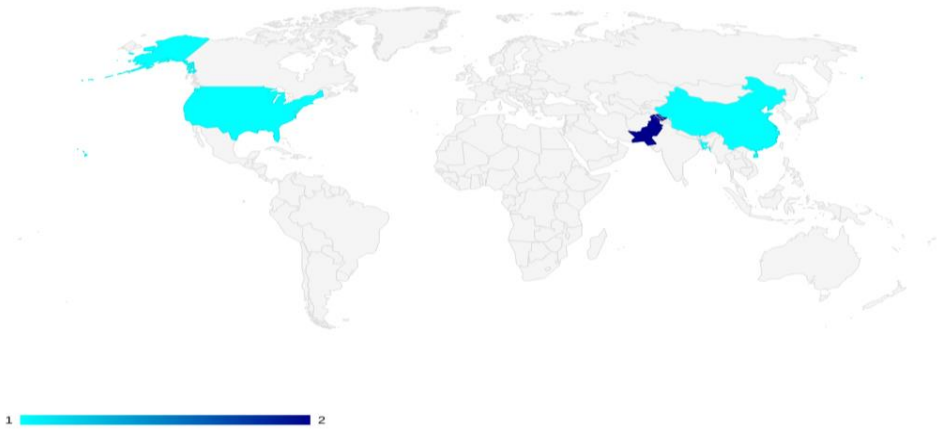
PURCHASED CAPABILITIES

Netsweeper systems Use in India

FinFisher Sales to India

There are 8 private vendors

TARGETING PROFILE



INDONESIA

OFFENSIVE ACTIONS
Homegrown APTs (3)

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

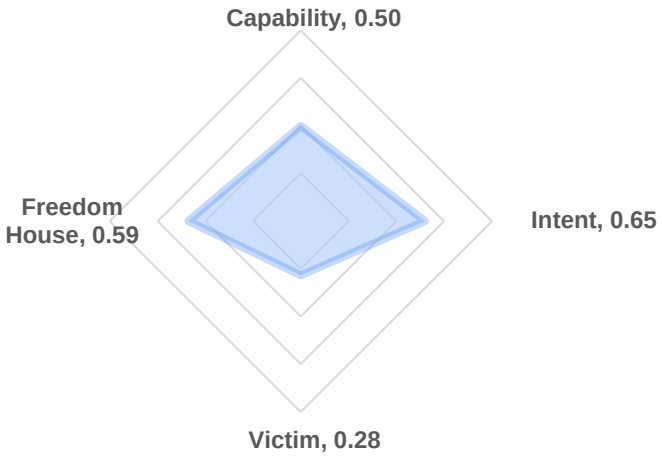
FREEDOM HOUSE
Partly Free (0.59)

VICTIM
Targeted in 25 documents

THREAT ACTORS
APT Threat Actors (1)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

Planetary Reef (2020)

OFFENSIVE PRIVATE VENDORS

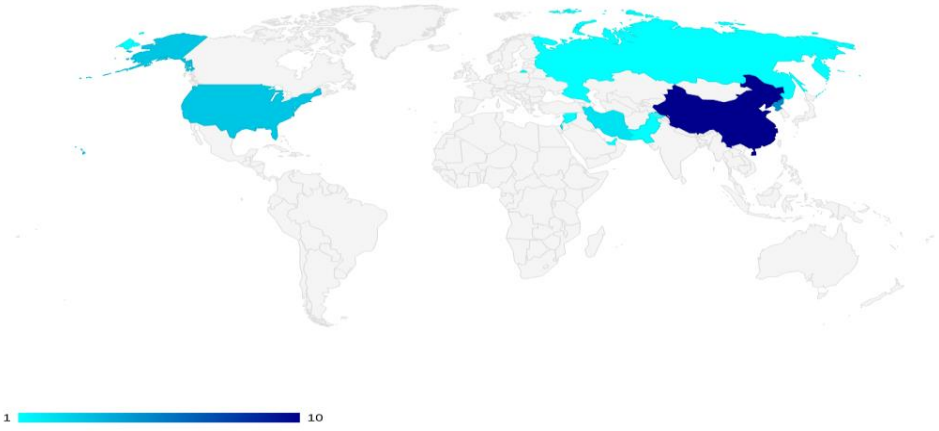
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Indonesia Purchase of Intrusion software Technology - 2015

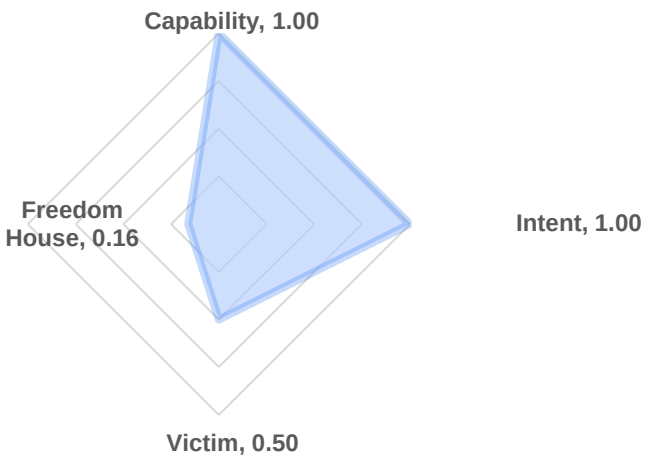
FinFisher Sales to Indonesia (National Encryption Body (Lembaga Sandi Negara))

VICTIM PROFILE



COUNTRY PROFILE

Global Power



IRAN

OFFENSIVE ACTIONS

State-Sponsored APTs (38)
Homegrown APTs (75)

CYBER TECH EXCHANGE

No sales or purchases found

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (13), Surveillance (2), Kinetic (1), Disinformation (2), Crime (3)

FREEDOM HOUSE

Not Free (0.16)

VICTIM

Targeted in 44 documents

THREAT ACTORS

APT 33 - 2013
Cadelle - 2011
Chafer (State-sponsored, Rana Intelligence Computing Company) - 2014
Cutting Kitten (State-sponsored, security company ITSecTeam) - 2012
DarkHydrus - 2016
DNSpionage - 2019
Flying Kitten - 2010
Group5 - 2015
Infy - 2013
Mabna Institute (State-sponsored, Islamic Revolutionary Guard Corps) - 2013
Magic Hound - 2013
MuddyWater (State-sponsored, Islamic Revolutionary Guard Corps) - 2017
OilRig - 2014
Rocket Kitten - 2011
Tortoiseshell - 2018
Cyber fighters of Izz Ad-Din Al Qassam - 2012

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

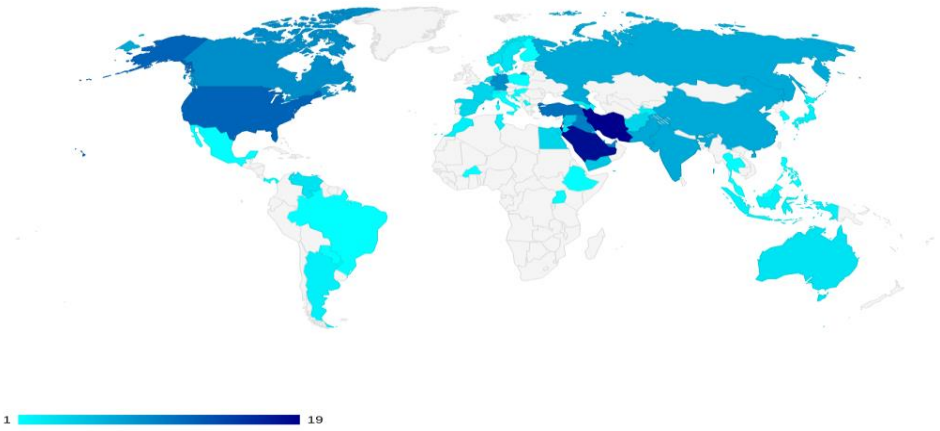
TARGETING PROFILE

THREAT ACTORS

State-Sponsored (17)
APT Threat Actors (33)

PRIVATE VENDORS

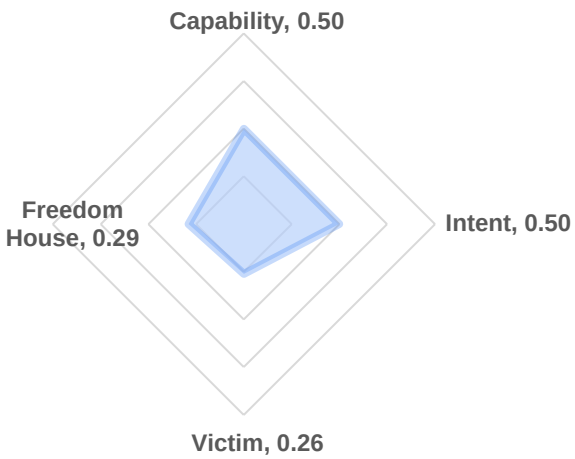
No private providers found



IRAQ

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

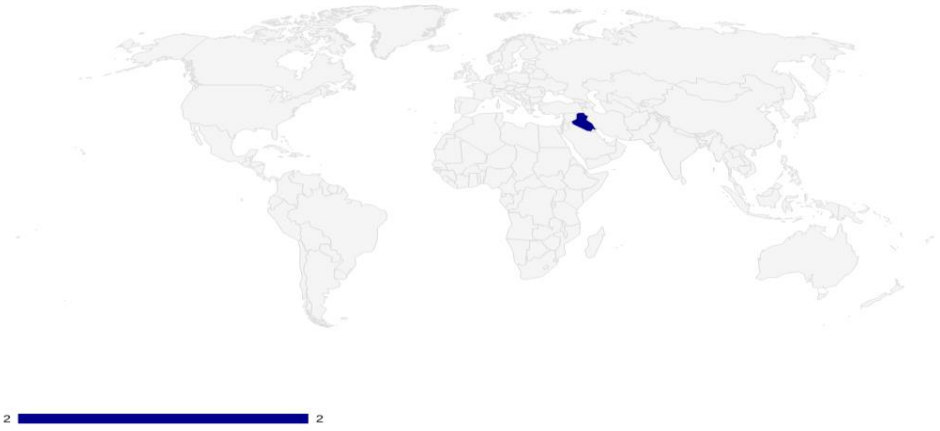
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

TARGETING PROFILE



OFFENSIVE ACTIONS

State-Sponsored APTs (2)

CYBER TECH EXCHANGE

No sales or purchases found

AUTONOMY

Third-Party Capabilities

OBJECTIVES

Surveillance (1)

FREEDOM HOUSE

Not Free (0.29)

VICTIM

Targeted in 23 documents

THREAT ACTORS

No threat-actors found

PRIVATE VENDORS

No private providers found

IRELAND

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (3)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

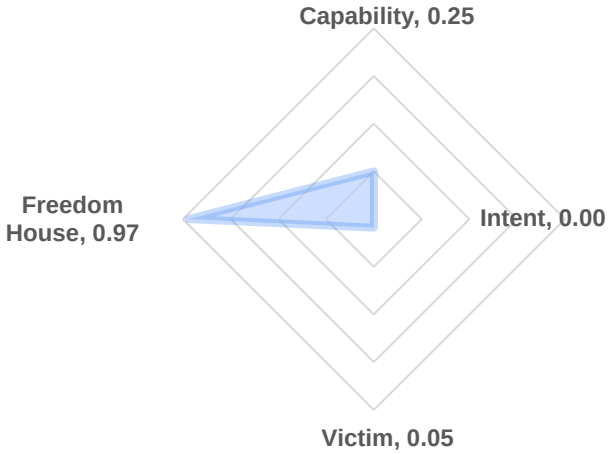
FREEDOM HOUSE
Free (0.97)

VICTIM
Targeted in 4 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 8 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

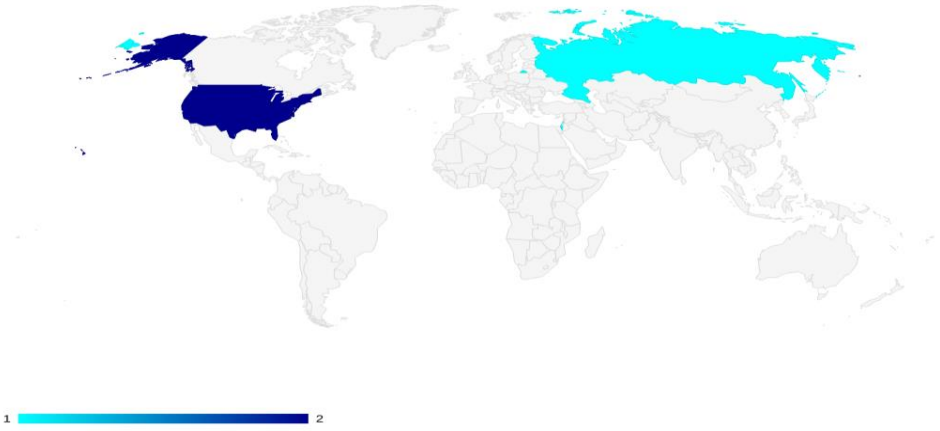
OFFENSIVE PRIVATE VENDORS

VigiTrust (LEA & Intelligence Services)

PURCHASED CAPABILITIES

No purchases found

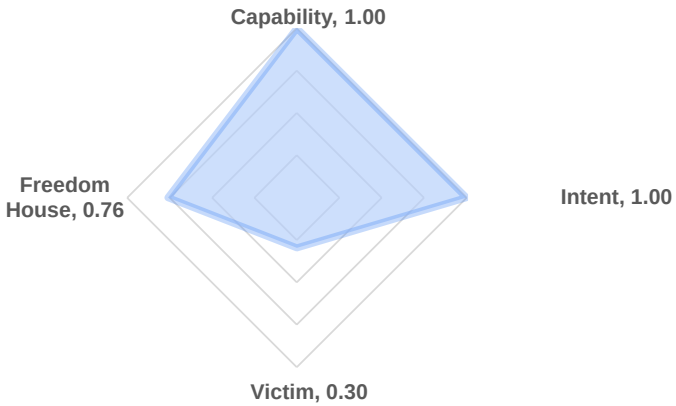
VICTIM PROFILE



ISRAEL

COUNTRY PROFILE

Global Power



OFFENSIVE ACTIONS

State-Sponsored APTs (6)
Homegrown APTs (14)

CYBER TECH EXCHANGE

Sales (51)

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (1), Kinetic (3)

FREEDOM HOUSE

Free (0.76)

VICTIM

Targeted in 26 documents

THREAT ACTORS

Circles (2015)
Unit 8200

OFFENSIVE PRIVATE VENDORS

Cellebrite (Phone Monitoring, Analysis)
Cyberbit (Counter-Surveillance, Internet Monitoring)
Elbit Systems (Intelligence Support, C4I. Collection, PC Surveillance, Intelligence)
NSO Group (Intrusion, Phone Monitoring)
Silicom (Internet Monitoring, Intrusion)
Wintego (Internet Monitoring, Intrusion)

PURCHASED CAPABILITIES

No purchases found

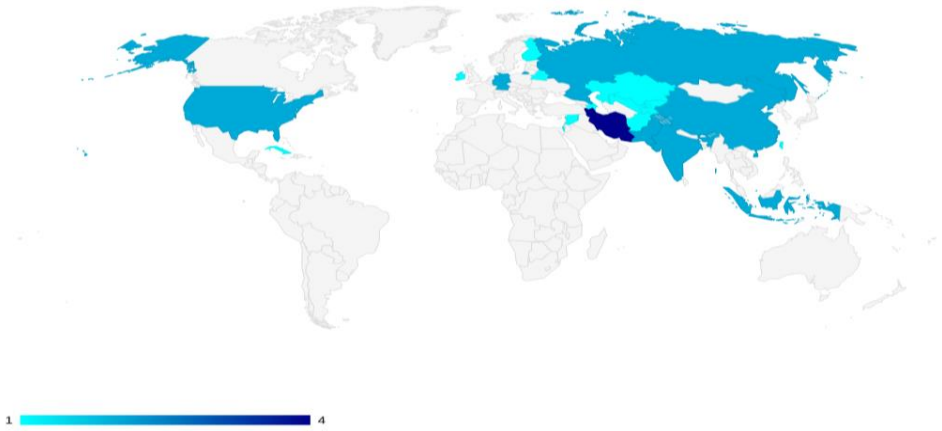
TARGETING PROFILE

THREAT ACTORS

State-Sponsored (1)
APT Threat Actors (4)

PRIVATE VENDORS

There are 29 private vendors



ITALY

OFFENSIVE ACTIONS

Homegrown APTs (6)

CYBER TECH EXCHANGE

Sales (64)
Purchases (3)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

No objectives found

FREEDOM HOUSE

Free (0.9)

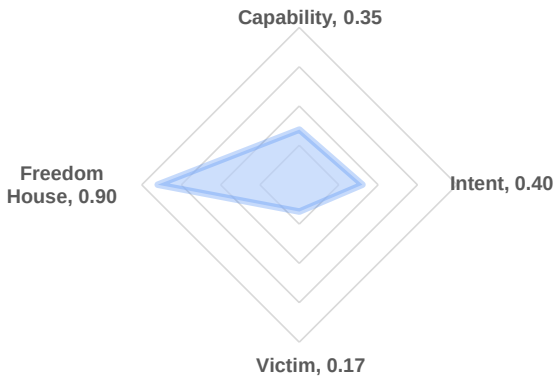
VICTIM

Targeted in 15 documents

THREAT ACTORS

APT Threat Actors (1)

COUNTRY PROFILE



THREAT ACTORS

Hacking Team (2003)

OFFENSIVE PRIVATE VENDORS

Area (Internet Monitoring, Monitoring Centre, Location Monitoring, Surveillance)

GR Sistemi (Internet Monitoring, Phone Monitoring, Intrusion, Biometrics, Communications Monitoring)

Hacking Team (Intrusion)

IPS (Internet Monitoring, Monitoring Centre, Analysis, Audio Surveillance, Video Surveillance, Intrusion, Monitoring Centres, Technical Surveillance)

PURCHASED CAPABILITIES

FinFisher Sales to Italy (Unknown multiple entities / Civil)

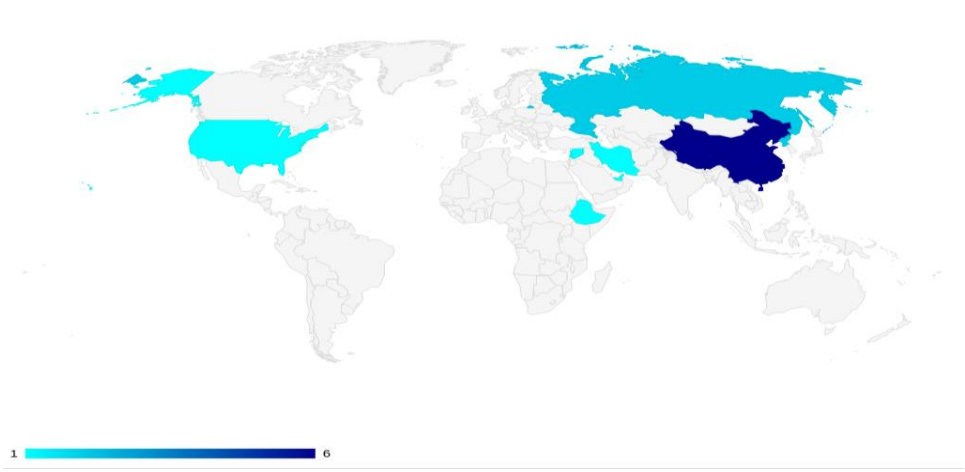
Hacking Team Sales to Italy (AREA / Civil) - 2014

Hacking Team Sales to Italy (Guardia di Finanza / Civil) – 2013

VICTIM PROFILE

PRIVATE VENDORS

There are 18 private vendors



JAPAN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

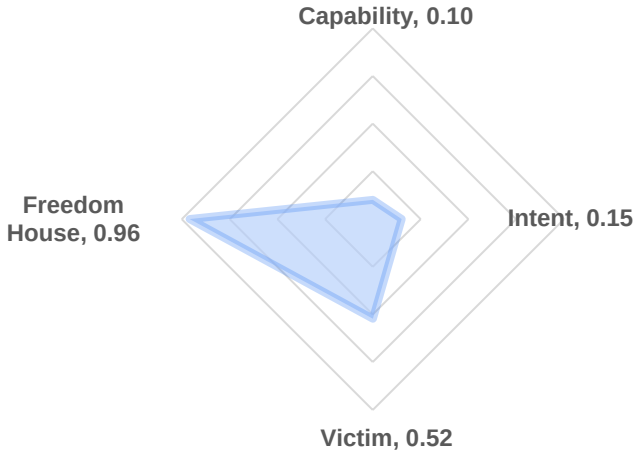
FREEDOM HOUSE
Free (0.96)

VICTIM
Targeted in 46 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 4 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

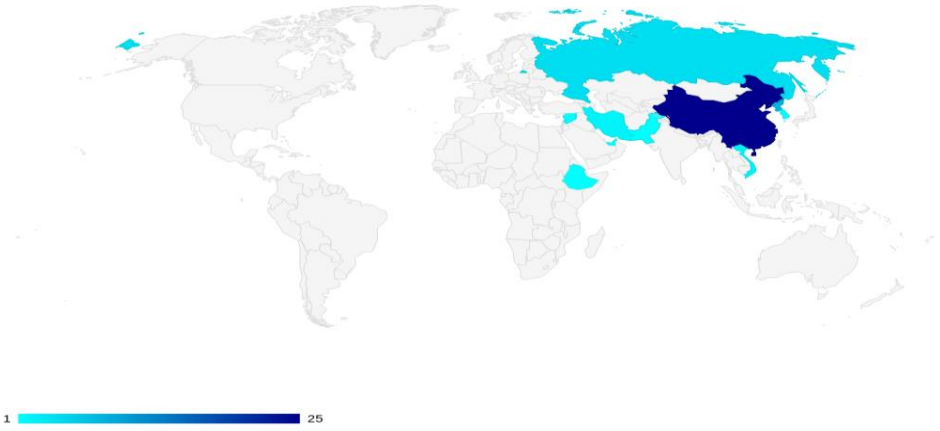
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Japan

VICTIM PROFILE



JORDAN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

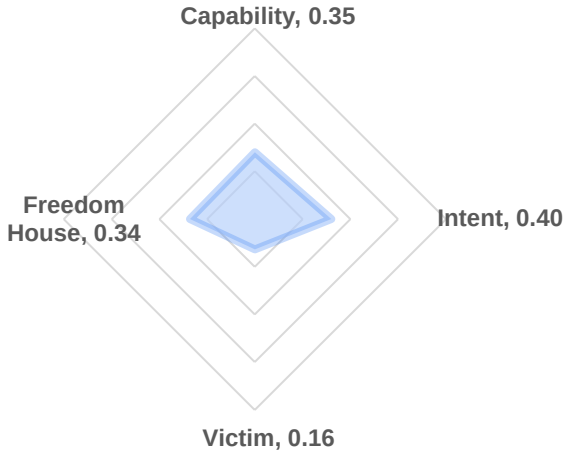
FREEDOM HOUSE
Not Free (0.34)

VICTIM
Targeted in 14 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

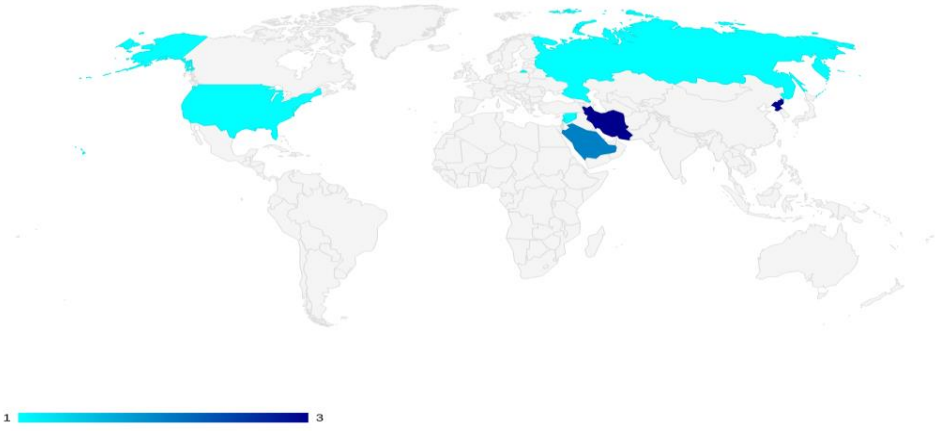
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Jordan Purchase of Intrusion software Techology - 2015

FinFisher Sales to Jordan

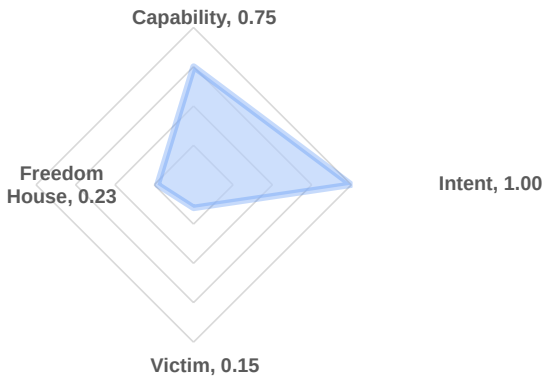
VICTIM PROFILE



KAZAKHSTAN

COUNTRY PROFILE

Local Player



OFFENSIVE ACTIONS

State-Sponsored APTs (3)
Homegrown APTs (2)

CYBER TECH EXCHANGE

Sales (2)
Purchases (5)

AUTONOMY

Third-Party Capabilities

OBJECTIVES

Espionage (1), Surveillance (1)

FREEDOM HOUSE

Not Free (0.23)

VICTIM

Targeted in 13 documents

THREAT ACTORS

State-Sponsored (2)
APT Threat Actors (3)

THREAT ACTORS

Operation Manul (2015)
Fxmsp (2016)
APT-C-34 (2019)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

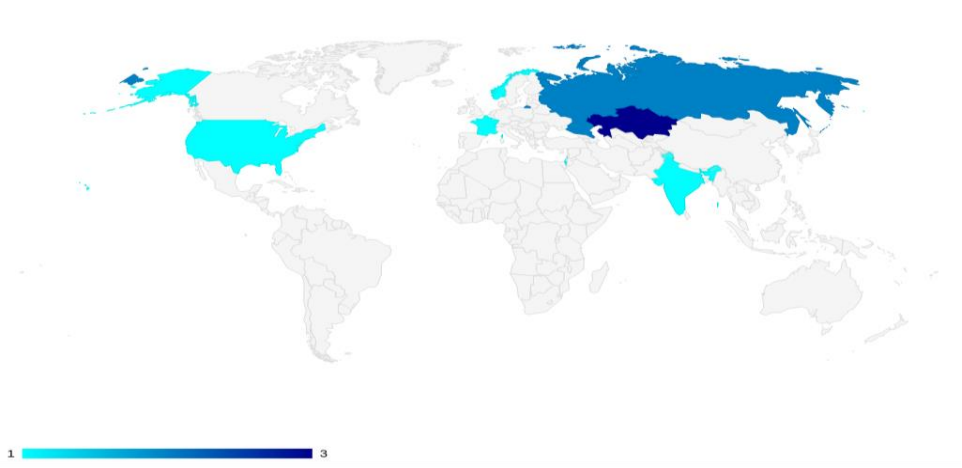
PURCHASED CAPABILITIES

NICE Sales to Kazakhstan (Committee of National Security (KNB) / Intelligence)
NSO Group Sales to Kazakhstan
Cyberbit Sales to Kazakhstan (National Security Committee / Intelligence) - 2017
FinFisher Sales to Kazakhstan
Hacking Team Sales to Kazakhstan (SIS of NSC / Intelligence) – 2012

PRIVATE VENDORS

No private providers found

TARGETING PROFILE



KENYA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

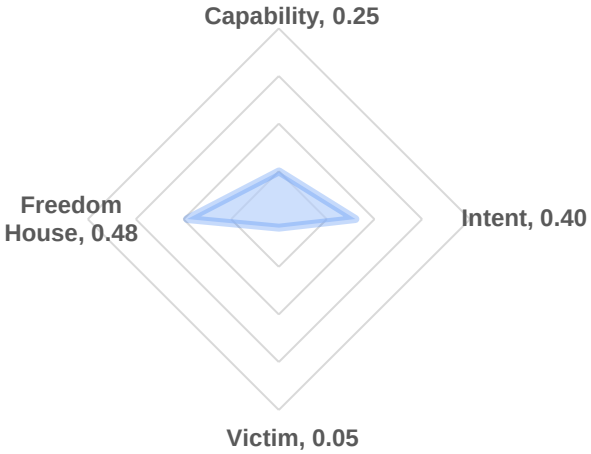
FREEDOM HOUSE
Partly Free (0.48)

VICTIM
Targeted in 4 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

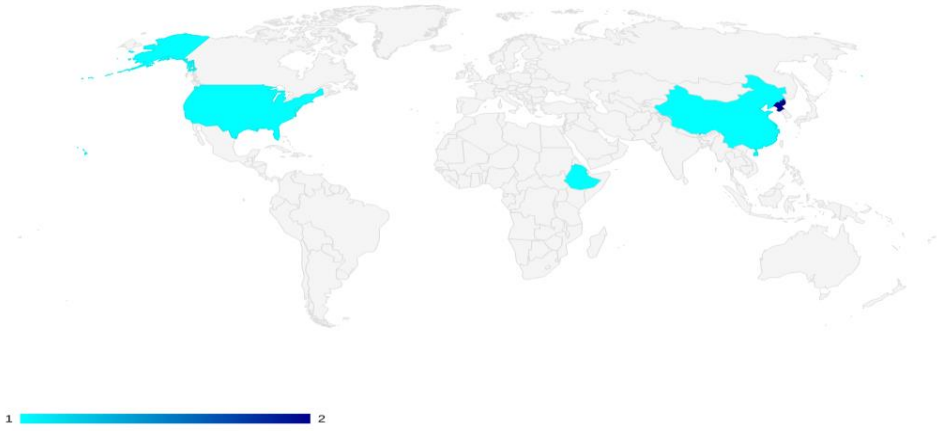
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Kenya (National Intelligence Service (NIS) / Intelligence)

VICTIM PROFILE



KUWAIT

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

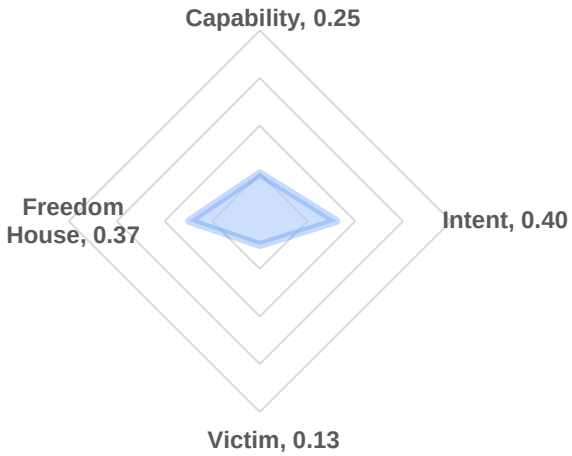
FREEDOM HOUSE
Partly Free (0.37)

VICTIM
Targeted in 11 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

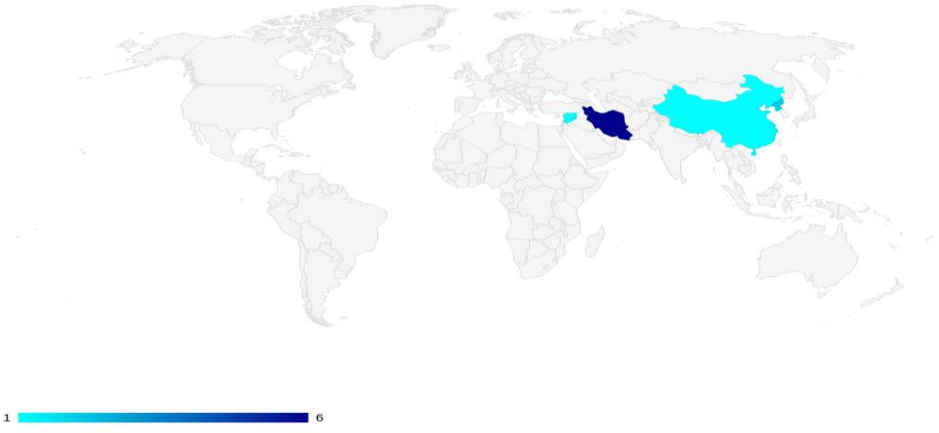
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Kuwait Purchase of Intrusion software Techology - 2015

Netsweeper systems Use in Kuwait

VICTIM PROFILE



LATVIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

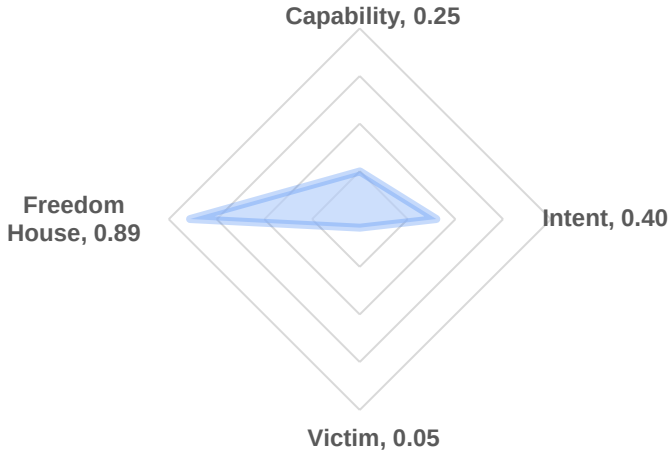
FREEDOM HOUSE
Free (0.89)

VICTIM
Targeted in 4 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

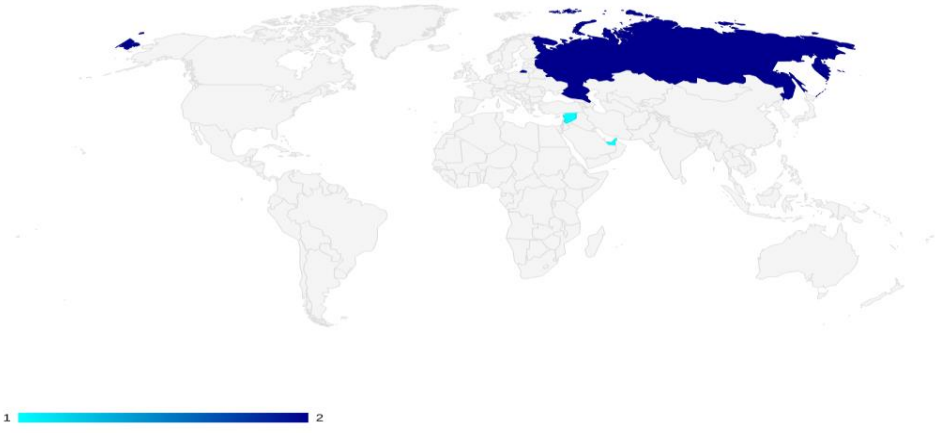
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

NSO Group Sales to Latvia

FinFisher Sales to Latvia

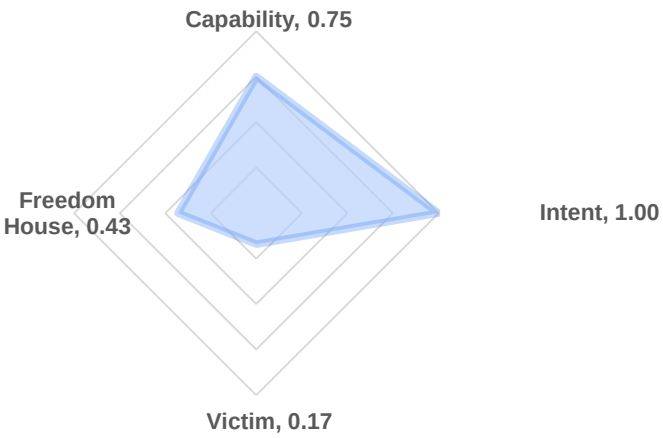
VICTIM PROFILE



LEBANON

COUNTRY PROFILE

Regional Contender



OFFENSIVE ACTIONS

State-Sponsored APTs (3)
Homegrown APTs (3)

CYBER TECH EXCHANGE

Purchases (2)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

Espionage (2), Surveillance (1)

FREEDOM HOUSE

Partly Free (0.43)

VICTIM

Targeted in 15 documents

THREAT ACTORS

State-Sponsored (1)
APT Threat Actors (3)

PRIVATE VENDORS

No private providers found

THREAT ACTORS

Dark Caracal (2007)

Tempting Cedar Spyware (2015)

Volatile Cedar (2012)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

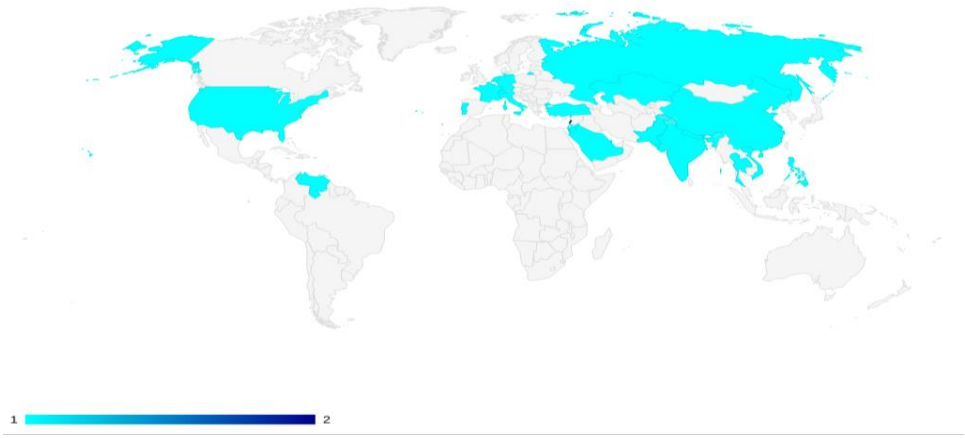
PURCHASED CAPABILITIES

FinFisher Sales to Lebanon (General Directorate of General Security)

FinFisher Sales to Lebanon - 2015

Hacking Team Sales to Lebanon (Lebanon Army Forces / Military) – 2015

TARGETING PROFILE



LIBYA

OFFENSIVE ACTIONS
Homegrown APTs (1)

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

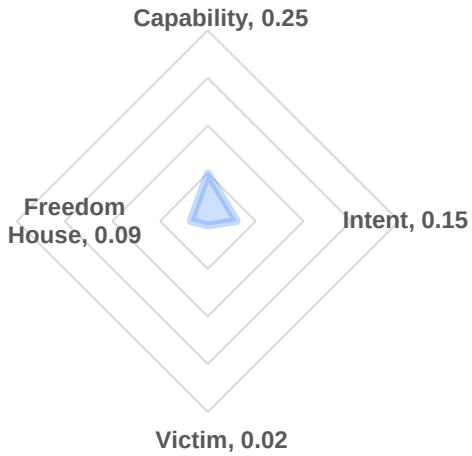
FREEDOM HOUSE
Not Free (0.09)

VICTIM
Targeted in 2 documents

THREAT ACTORS
APT Threat Actors (1)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

Libyan Scorpions (2015)

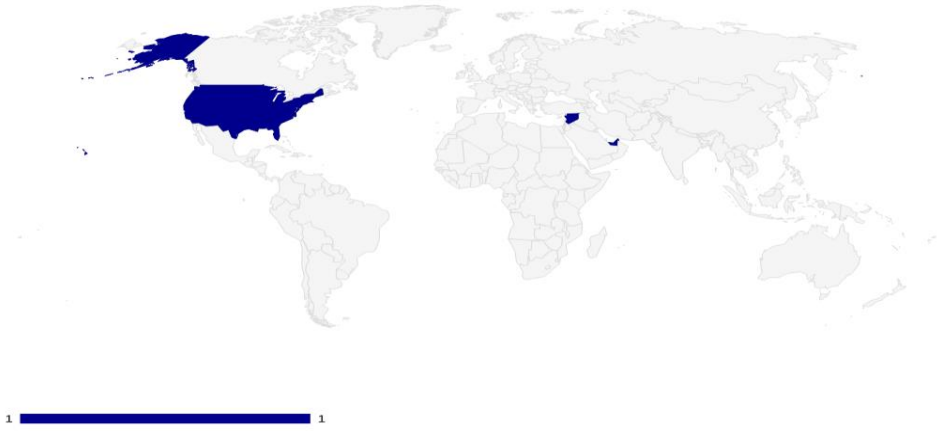
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Amesys Sales to Libya

VICTIM PROFILE



LITHUANIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

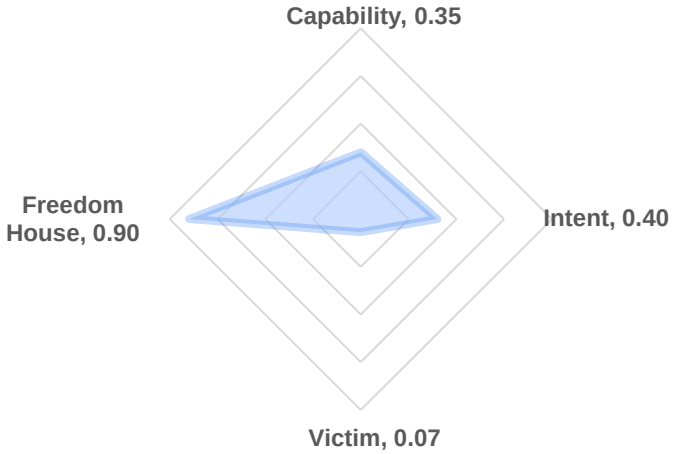
FREEDOM HOUSE
Free (0.9)

VICTIM
Targeted in 6 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 3 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

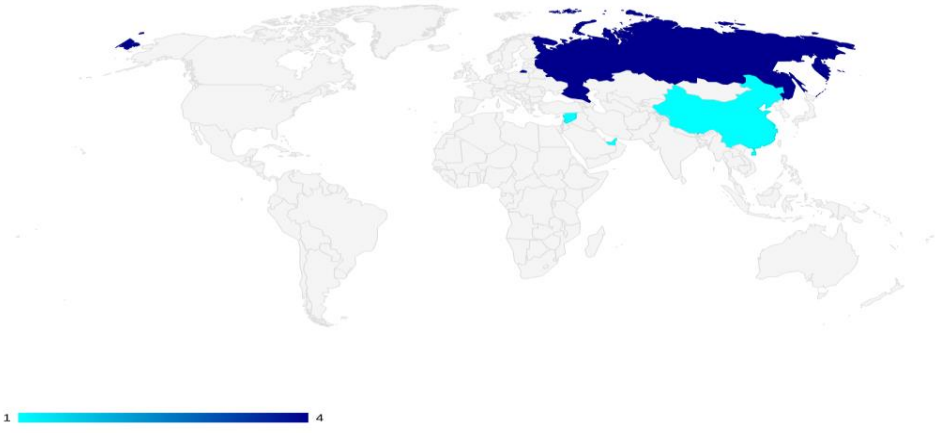
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Lithuania

Hacking Team Sales to Lithuania (Lituania Criminal Police / LEA) - 2014

VICTIM PROFILE



LUXEMBOURG

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

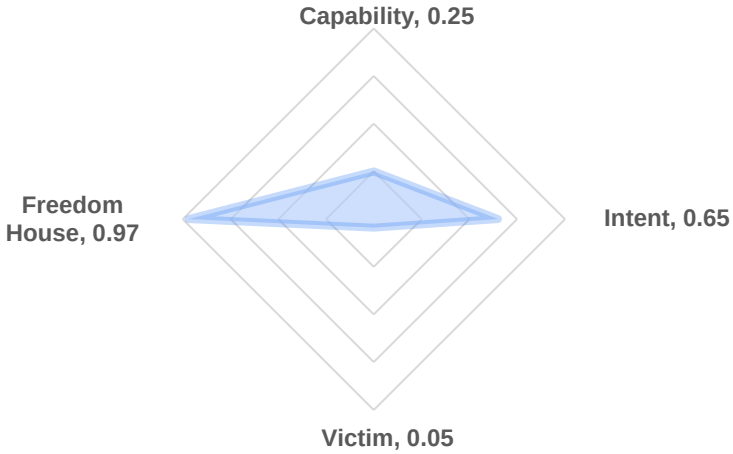
FREEDOM HOUSE
Free (0.97)

VICTIM
Targeted in 4 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

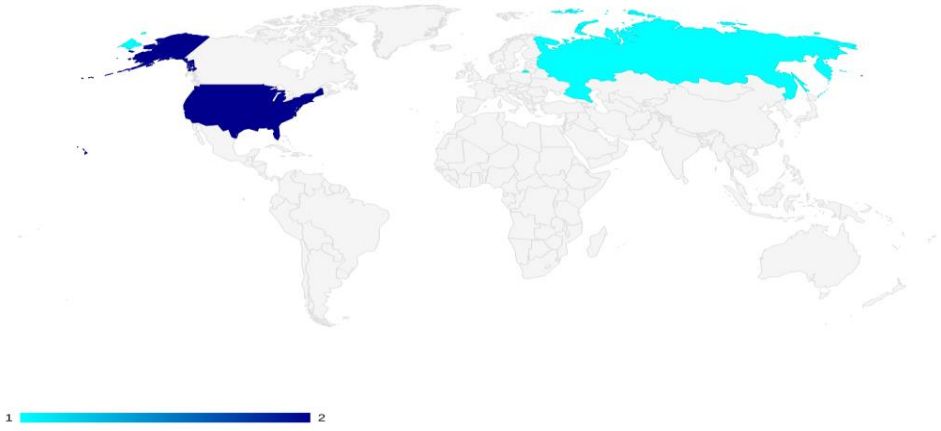
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Luxembourg (IR Authorities (Condor) / Civil) - 2012

Hacking Team Sales to Luxembourg (State security (Falcon) / Intelligence) - 2012

VICTIM PROFILE



NORTH MACEDONIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

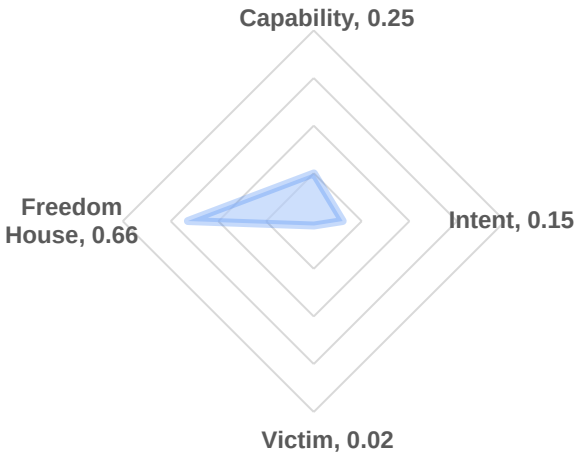
FREEDOM HOUSE
Partly Free (0.66)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

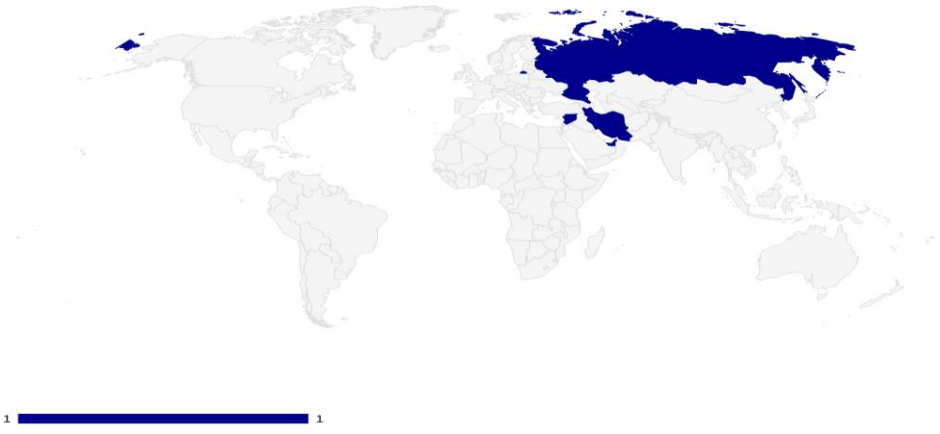
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Macedonia

VICTIM PROFILE



MALAYSIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

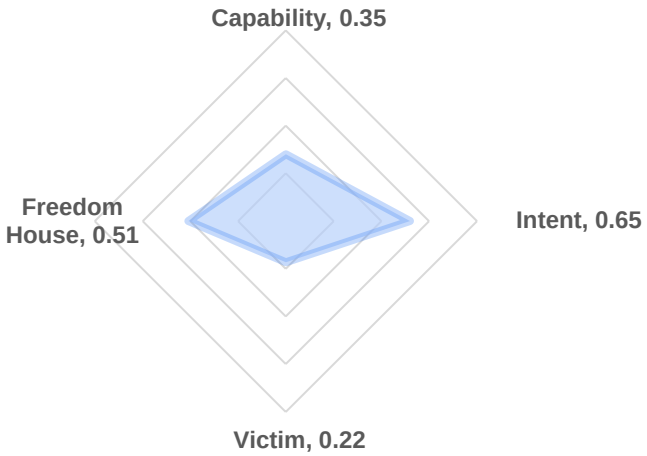
FREEDOM HOUSE
Partly Free (0.51)

VICTIM
Targeted in 19 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 2 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

Motec (Internet Monitoring, Intrusion, Phone Monitoring, Communications Monitoring)

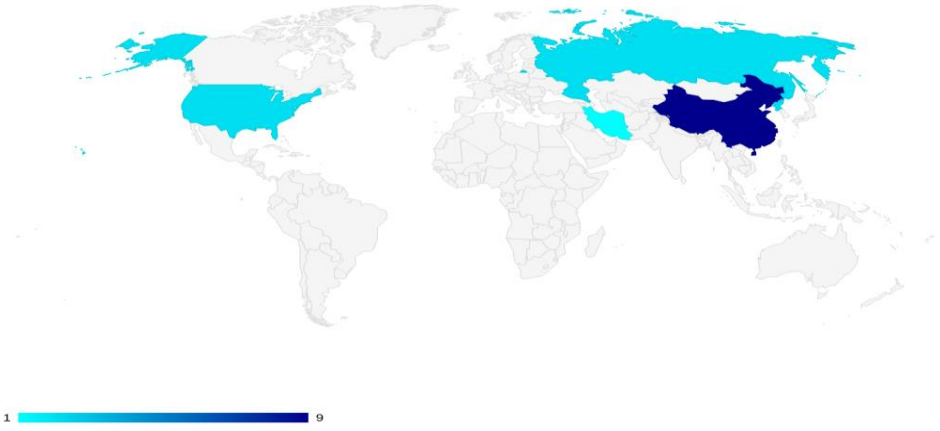
PURCHASED CAPABILITIES

Hacking Team Sales to Malaysia (Malysia K / Intelligence) - 2013

Malaysia Purchase of Intrusion software Techology - 2015

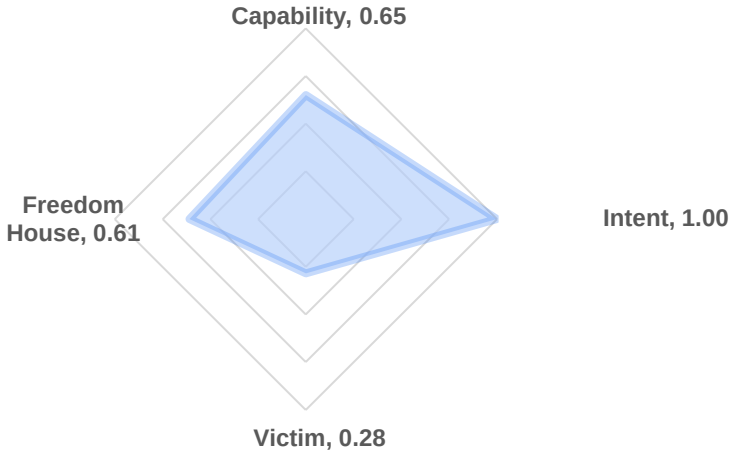
FinFisher Sales to Malaysia

VICTIM PROFILE



COUNTRY PROFILE

Local Player



MEXICO

OFFENSIVE ACTIONS

State-Sponsored APTs (8)
Homegrown APTs (6)

CYBER TECH EXCHANGE

Purchases (13)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

Espionage (1), Surveillance (1)

FREEDOM HOUSE

Partly Free (0.61)

VICTIM

Targeted in 25 documents

THREAT ACTORS

APT Threat Actors (1)

THREAT ACTORS

leetMX (2016)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

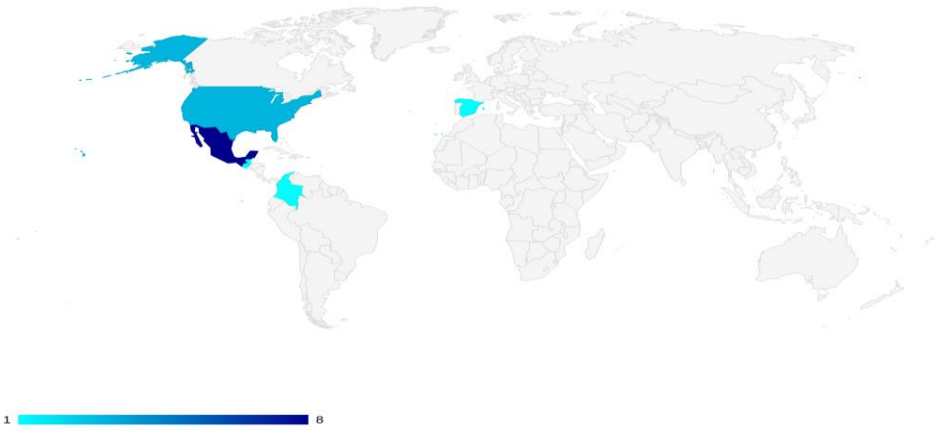
PURCHASED CAPABILITIES

Hacking Team Sales to Mexico (Jalisco Mexico / LEA) - 2014
NSO Group Sales to Mexico - 2013
FinFisher Sales to Mexico
Hacking Team Sales to Mexico (La Dependencia y/o Cisen / Intelligence) - 2010
Hacking Team Sales to Mexico (Estado del Mexico / LEA) - 2012
Hacking Team Sales to Mexico (Estado de Qeretaro / LEA) - 2013
Hacking Team Sales to Mexico (Governo de Puebla / LEA) - 2013
Hacking Team Sales to Mexico (Governo de Campeche / LEA) - 2013
Hacking Team Sales to Mexico (Mexico - pemx / LEA) - 2013
Hacking Team Sales to Mexico (Mex Taumalipas / Civil) - 2014
Hacking Team Sales to Mexico (Sec. De Planeacion y Finanzas / Civil) - 2014
Hacking Team Sales to Mexico (Mexico Yucatan / LEA) - 2014
Hacking Team Sales to Mexico (Mexico Durango / LEA) - 2014

PRIVATE VENDORS

There is 1 private vendor

TARGETING PROFILE



MOLDOVA

OFFENSIVE ACTIONS
Homegrown APTs (2)

CYBER TECH EXCHANGE
No sales or purchases found

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

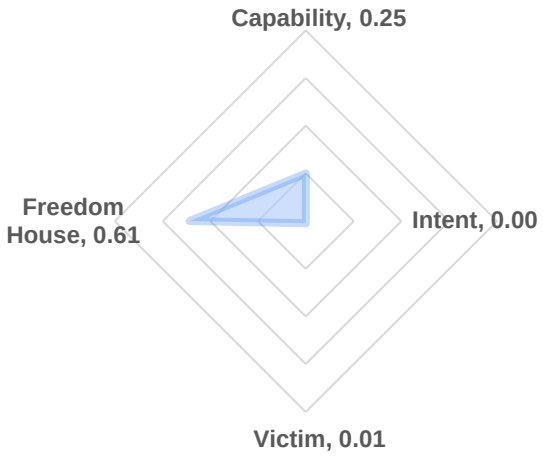
FREEDOM HOUSE
Partly Free (0.61)

VICTIM
Targeted in 1 document

THREAT ACTORS
APT Threat Actors (1)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

Bachosens (2017)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

VICTIM PROFILE

MONGOLIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

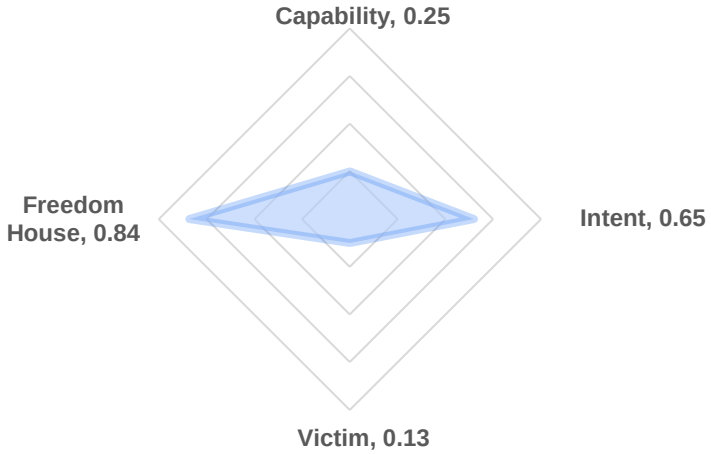
FREEDOM HOUSE
Free (0.84)

VICTIM
Targeted in 11 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

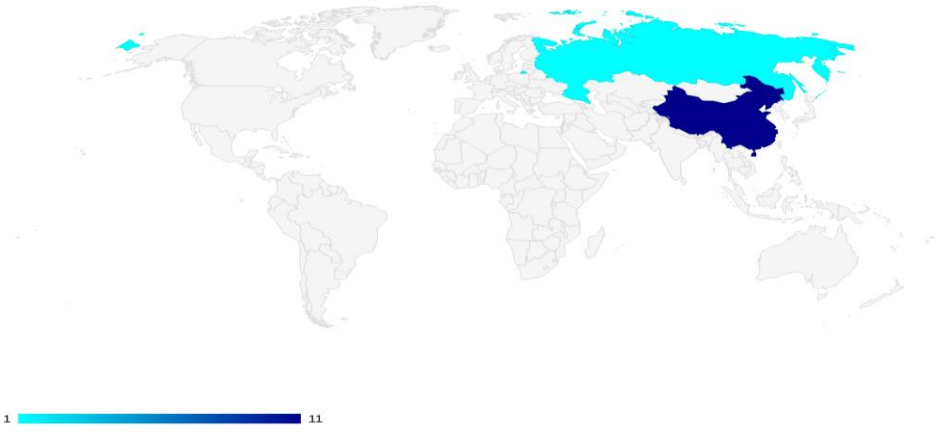
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Mongolia (AC Mongolia / Intelligence) - 2013

FinFisher Sales to Mongolia (Special State Security Department (SSSD) / Intelligence)

VICTIM PROFILE



MOROCCO

OFFENSIVE ACTIONS
State-Sponsored APTs (3)
Homegrown APTs (3)

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Surveillance (1)

FREEDOM HOUSE
Partly Free (0.37)

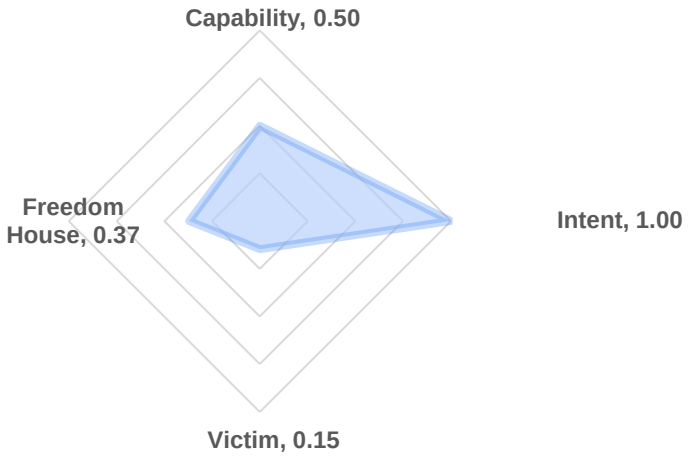
VICTIM
Targeted in 13 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Morocco (Morocco - DST / LEA) - 2012

NSO Group Sales to Morocco

FinFisher Sales to Morocco (Conseil Superieur De La Defense Nationale (CSDN))

TARGETING PROFILE

MOZAMBIQUE

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

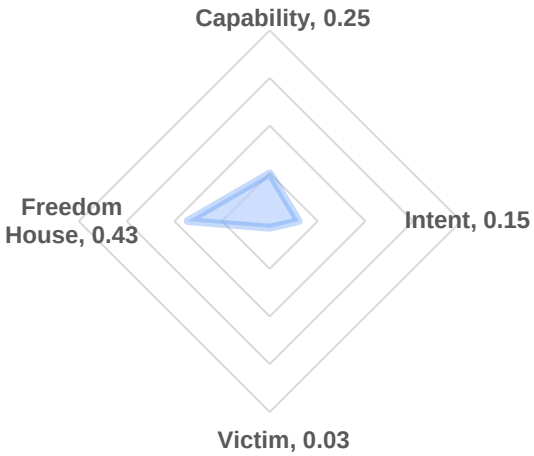
FREEDOM HOUSE
Partly Free (0.43)

VICTIM
Targeted in 3 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

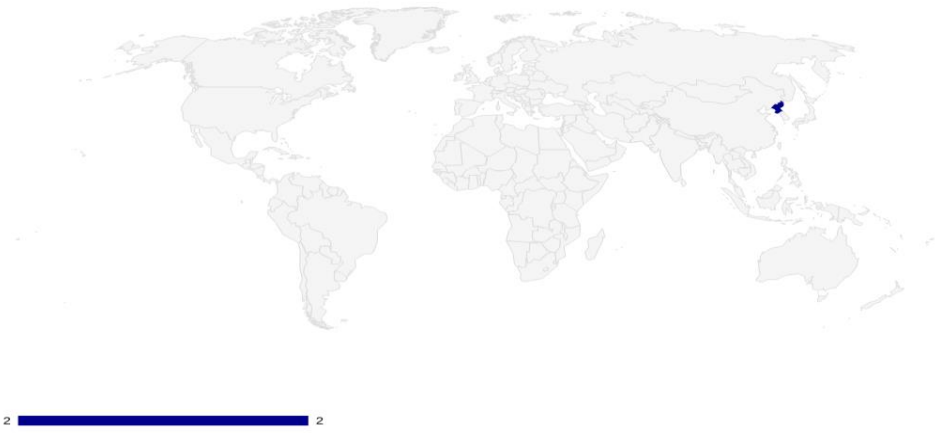
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

NSO Group Sales to Mozambique

VICTIM PROFILE



NETHERLANDS

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (1)
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

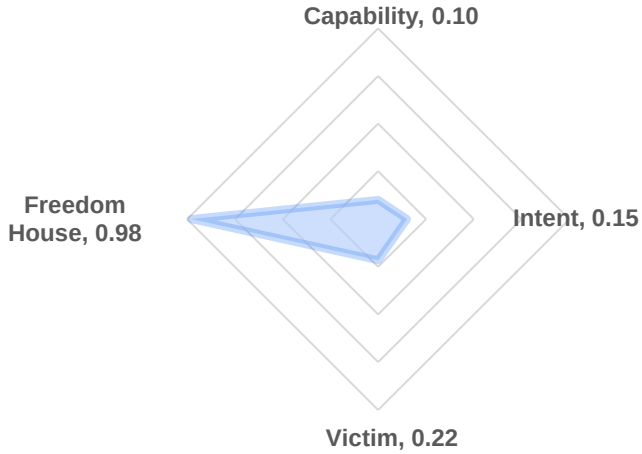
FREEDOM HOUSE
Free (0.98)

VICTIM
Targeted in 19 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 4 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

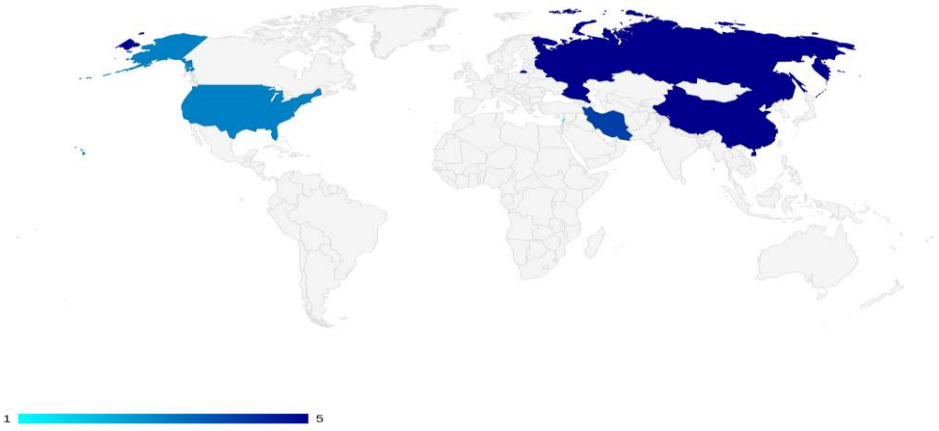
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Netherlands

VICTIM PROFILE



NEW ZEALAND

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (10)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

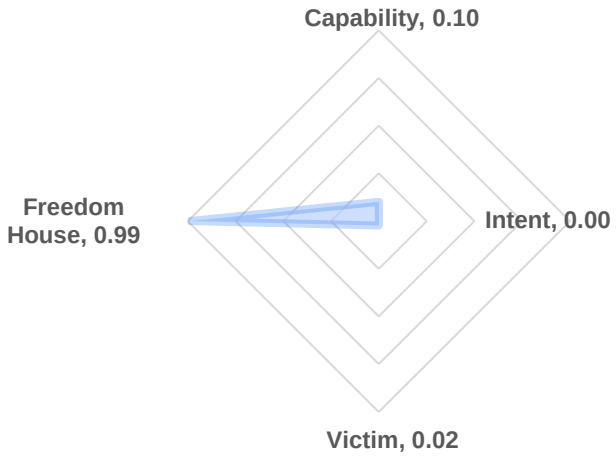
FREEDOM HOUSE
Free (0.99)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 2 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

VICTIM PROFILE

NIGERIA

OFFENSIVE ACTIONS
Homegrown APTs (10)

CYBER TECH EXCHANGE
Purchases (5)

AUTONOMY
Third-Party Capabilities

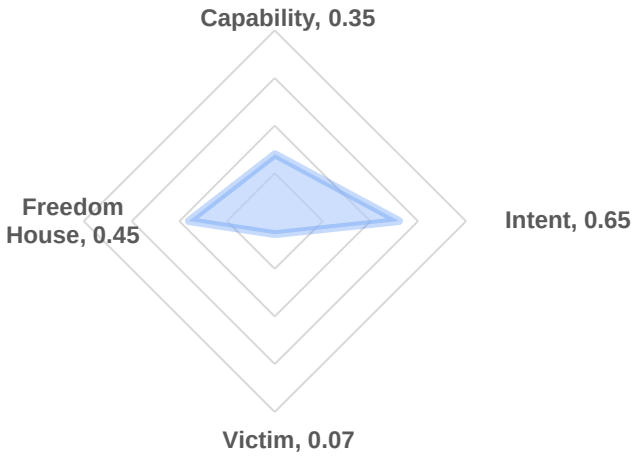
OBJECTIVES
No objectives found

FREEDOM HOUSE
Partly Free (0.45)

VICTIM
Targeted in 6 documents

THREAT ACTORS
APT Threat Actors (1)

COUNTRY PROFILE



THREAT ACTORS

SilverTerrier

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

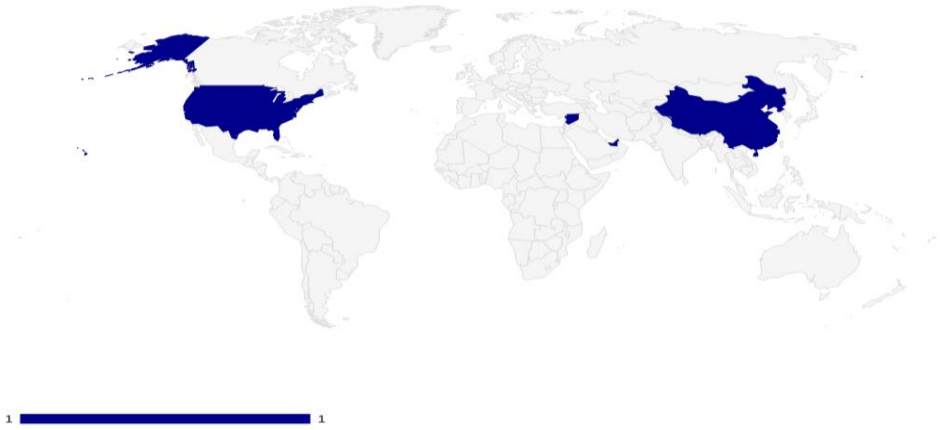
PURCHASED CAPABILITIES

Hacking Team Sales to Nigeria (Bayelsa State Government / Civil) - 2012
NICE Systems Sales to Nigeria (Bayelsa State Government / Civil) - 2012
Elbit Systems Sales to Nigeria (National Security Adviser / Intelligence)
FinFisher Sales to Nigeria (Unknown multiple entities / Civil)
NSO Group Sales to Nigeria (Rivers State, Delta State e Bayelsa State / LEA) – 2012

PRIVATE VENDORS

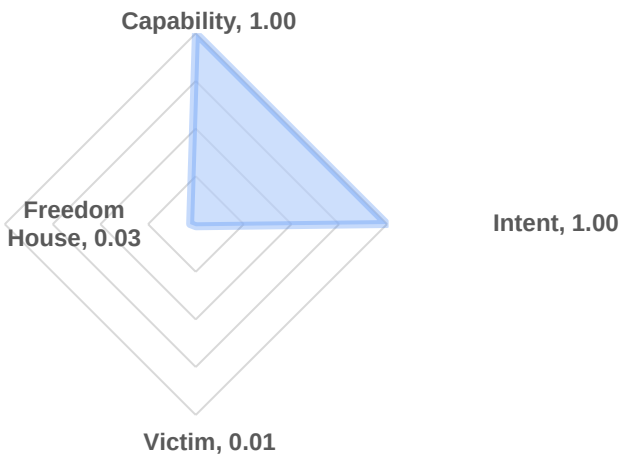
No private providers found

VICTIM PROFILE



COUNTRY PROFILE

Regional Contender



NORTH KOREA

OFFENSIVE ACTIONS

State-Sponsored APTs (32)
Homegrown APTs (42)

CYBER TECH EXCHANGE

No sales or purchases found

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (6), Kinetic (5), Crime (7)

FREEDOM HOUSE

Not Free (0.03)

VICTIM

Targeted in 1 document

THREAT ACTORS

Covellite (2017)
Kimsuky (2012)
Lazarus Group (2007)
Andariel (2014)
BeagleBoyz (2014)
Bluenoroff (2014)
Operation Earth Kitsune (2019)
Operation WizardOpium (2019)
Reaper (2012)
Wassonite (2018)
TEMP.Hermit
FASTCash (2016)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

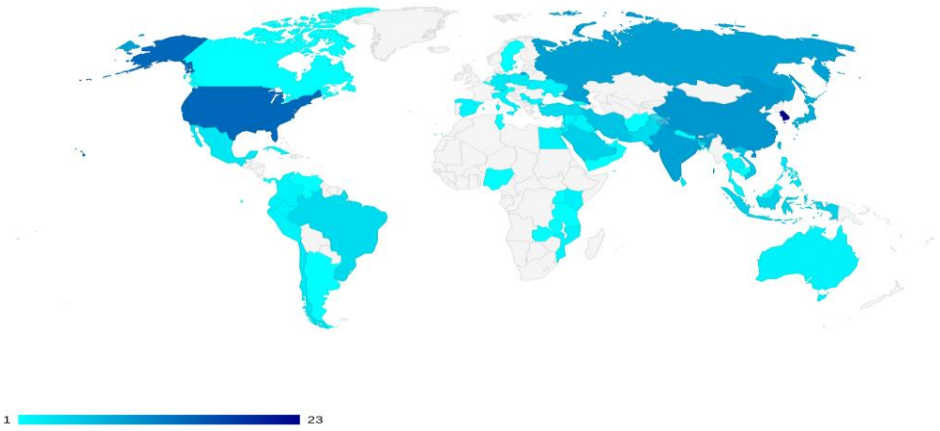
TARGETING PROFILE

THREAT ACTORS

State-Sponsored (4)
APT Threat Actors (12)

PRIVATE VENDORS

No private providers found



OMAN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (5)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

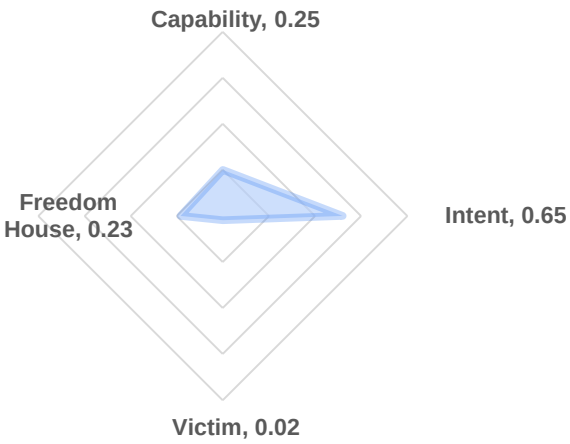
FREEDOM HOUSE
Not Free (0.23)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

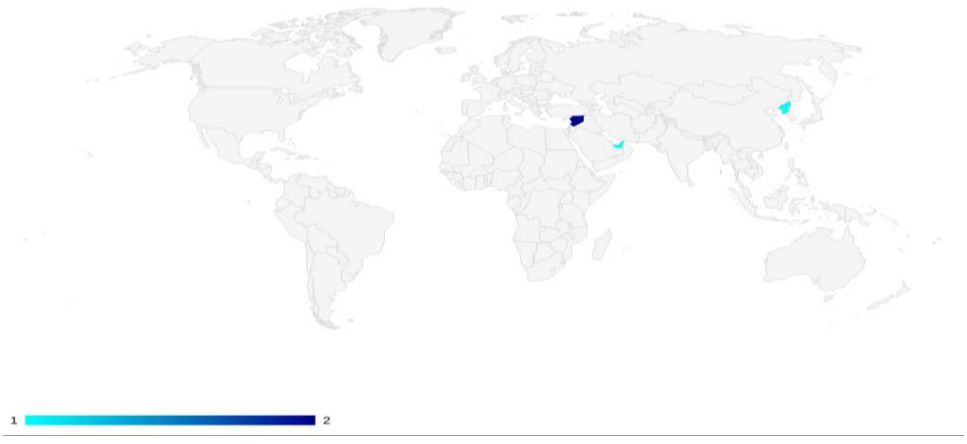
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

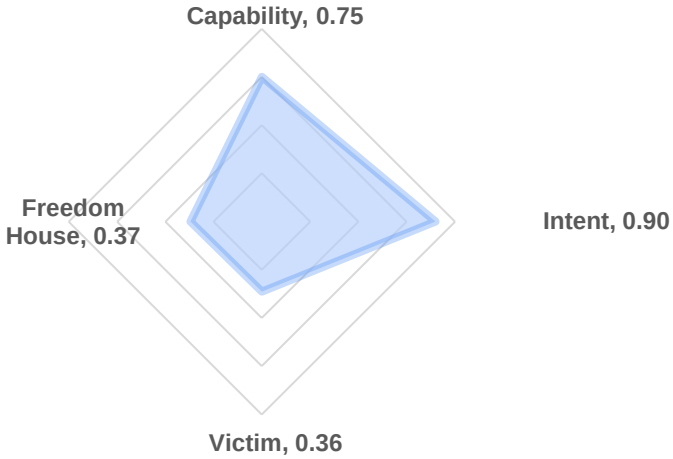
Hacking Team Sales to Oman (Oman - Intelligence / Intelligence) - 2011
Oman Purchase of Intrusion software Techology - 2015
Dreamlab Sales to Oman (Government of Oman / Civil) - 2010
Trovicor Sales to Oman
FinFisher Sales to Oman

VICTIM PROFILE



COUNTRY PROFILE

Regional Contender



PAKISTAN

OFFENSIVE ACTIONS

State-Sponsored APTs (8)
Homegrown APTs (19)

CYBER TECH EXCHANGE

Purchases (3)

AUTONOMY

Third-Party Capabilities

OBJECTIVES

Espionage (4), Crime (2)

FREEDOM HOUSE

Partly Free (0.37)

VICTIM

Targeted in 32 documents

THREAT ACTORS

State-Sponsored (1)
APT Threat Actors (4)

THREAT ACTORS

Gorgon Group (2017)
Transparent Tribe (2013)
Gnosticplayers (2019)
Stealth Mango and Tangelo

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

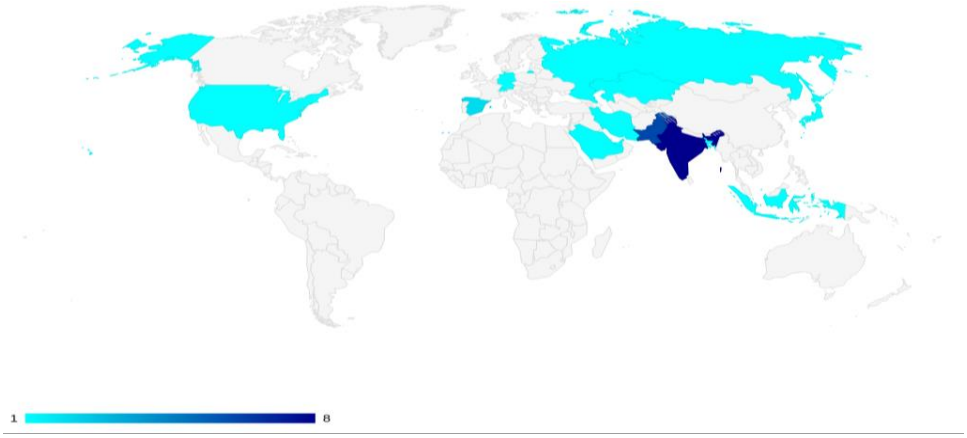
PURCHASED CAPABILITIES

Netsweeper systems Use in Pakistan
SS8 Sales to Pakistan (Ufone)
FinFisher Sales to Pakistan

PRIVATE VENDORS

No private providers found

TARGETING PROFILE



PALESTINIAN TERRITORY

OFFENSIVE ACTIONS
Homegrown APTs (21)

CYBER TECH EXCHANGE
No sales or purchases found

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

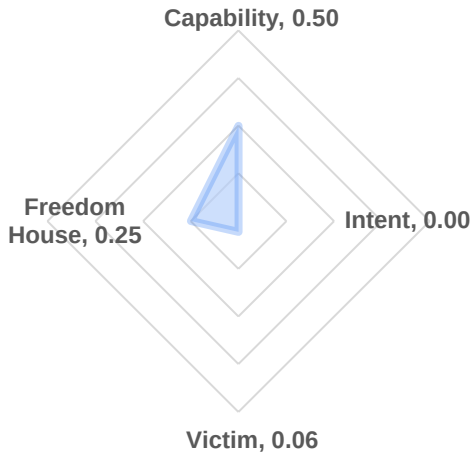
FREEDOM HOUSE
Not Free (0.25)

VICTIM
Targeted in 5 documents

THREAT ACTORS
State-Sponsored (1)
APT Threat Actors (3)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

Desert Falcons (2011)
Molerats (2012)
Operation Dustysky

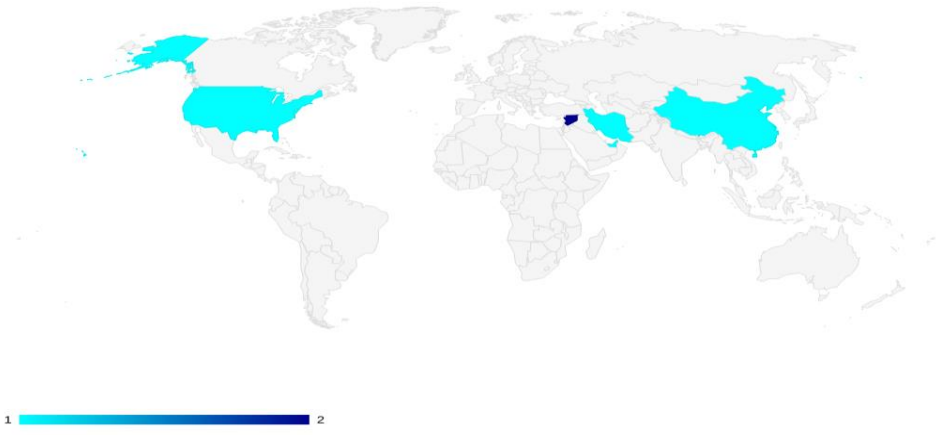
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

VICTIM PROFILE



PANAMA

OFFENSIVE ACTIONS
State-Sponsored APTs (1)
Homegrown APTs (1)

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Surveillance (1)

FREEDOM HOUSE
Free (0.83)

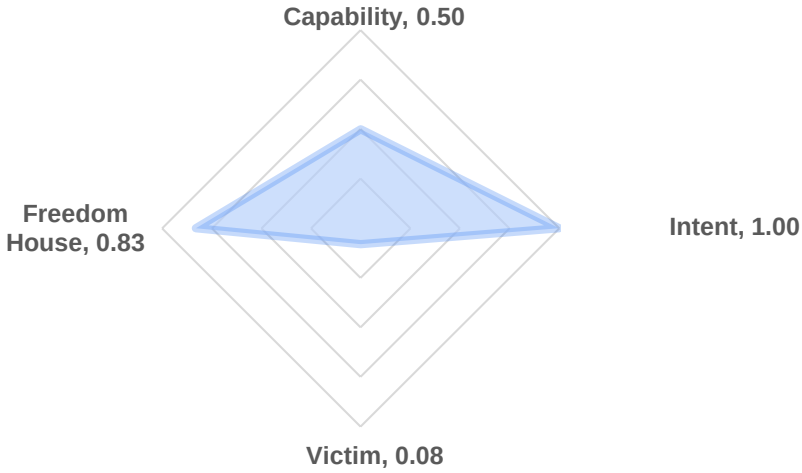
VICTIM
Targeted in 7 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

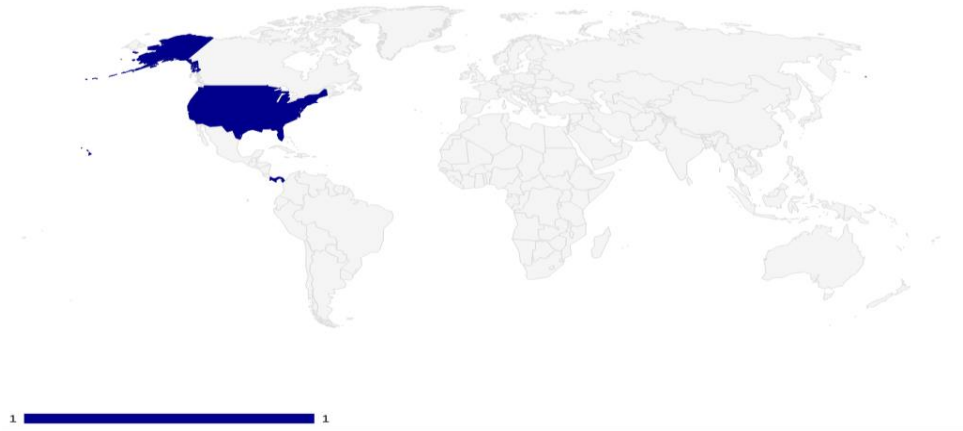
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Panama (President Security / Intelligence) - 2011
NSO Group Sales to Panama
FinFisher Sales to Panama (President Security / Intelligence) – 2009

TARGETING PROFILE



PARAGUAY

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

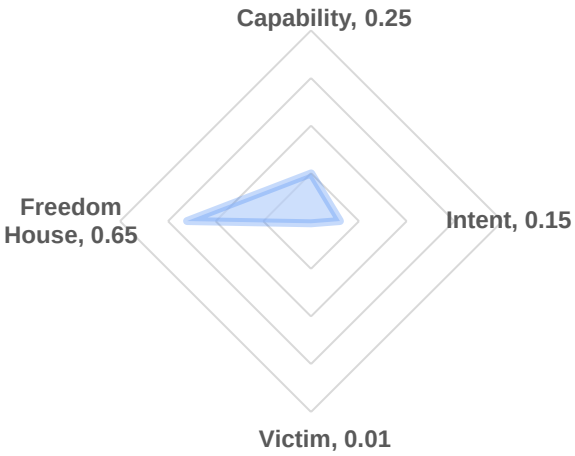
FREEDOM HOUSE
Partly Free (0.65)

VICTIM
Targeted in 1 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Paraguay

VICTIM PROFILE

PHILIPPINES

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
Espionage (1)

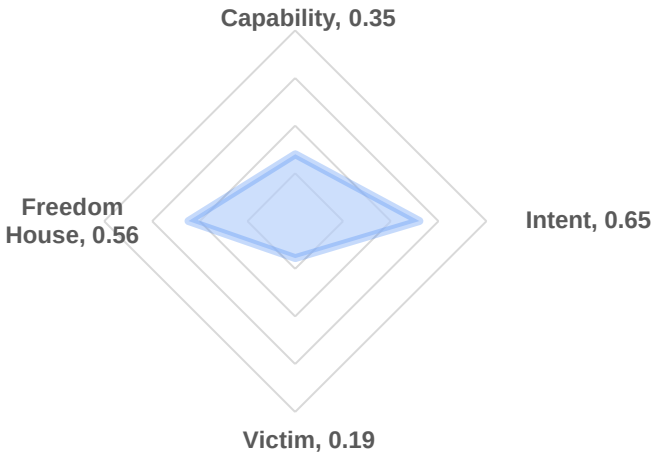
FREEDOM HOUSE
Partly Free (0.56)

VICTIM
Targeted in 17 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

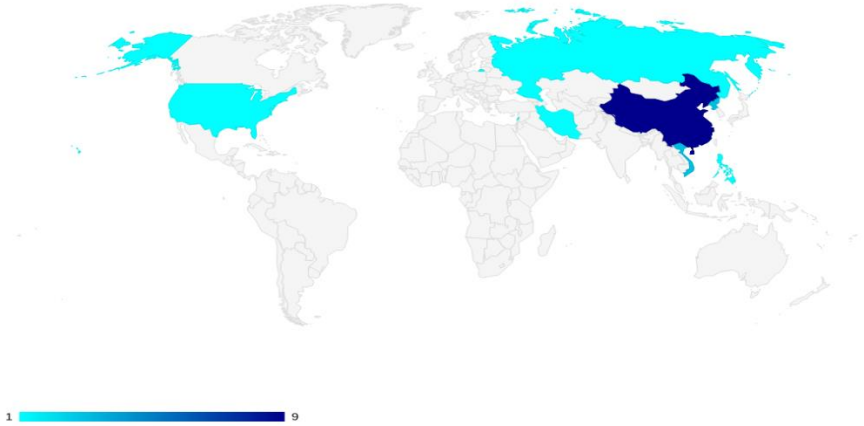
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Cyberbit Sales to Philippines (Philippine President's Malacañang Palace / Intelligence) - 2017

Philippines Purchase of Intrusion software Techology - 2015

VICTIM PROFILE



POLAND

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

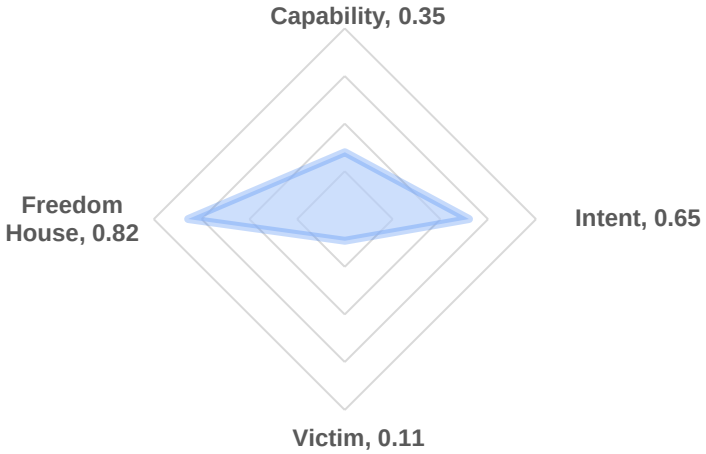
FREEDOM HOUSE
Free (0.82)

VICTIM
Targeted in 10 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 4 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

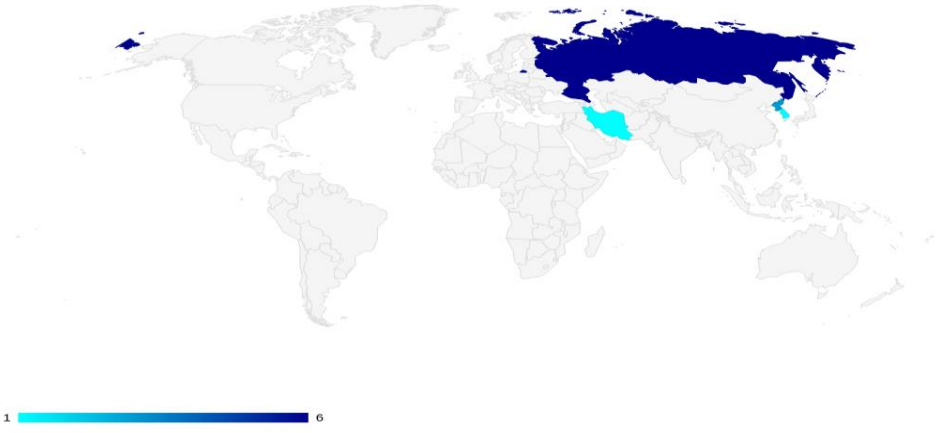
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Poland (CBA Poland / Intelligence) - 2012

NSO Group Sales to Poland

VICTIM PROFILE



QATAR

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

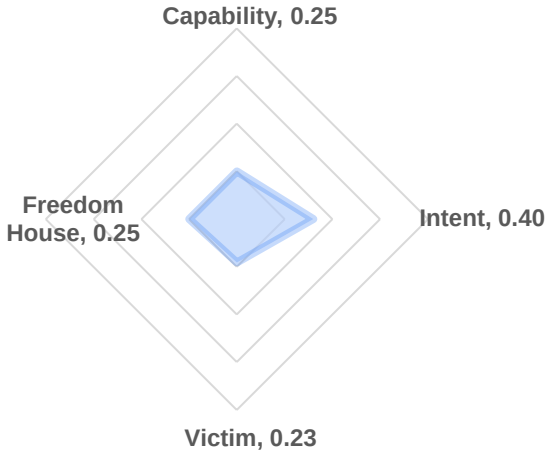
FREEDOM HOUSE
Not Free (0.25)

VICTIM
Targeted in 20 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

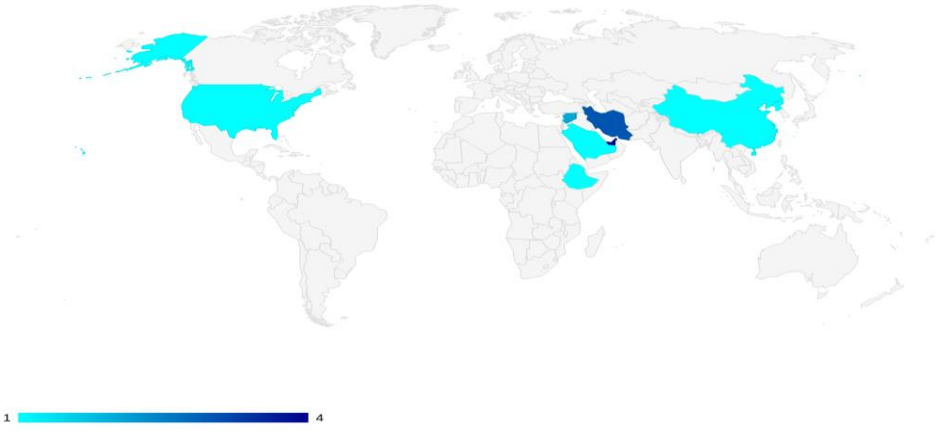
PURCHASED CAPABILITIES

Netsweeper systems Use in Qatar

Qatar Purchase of Intrusion software Techology - 2015

FinFisher Sales to Qatar

VICTIM PROFILE



ROMANIA

OFFENSIVE ACTIONS
Homegrown APTs (3)

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

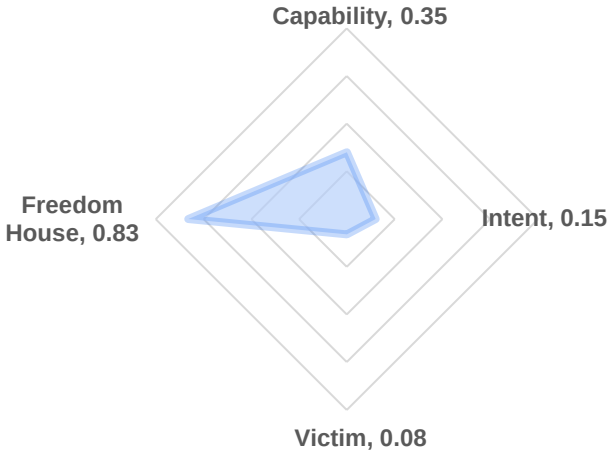
FREEDOM HOUSE
Free (0.83)

VICTIM
Targeted in 7 documents

THREAT ACTORS
APT Threat Actors (2)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

FIN4 (2013)

Outlaw Hacking Group (2018)

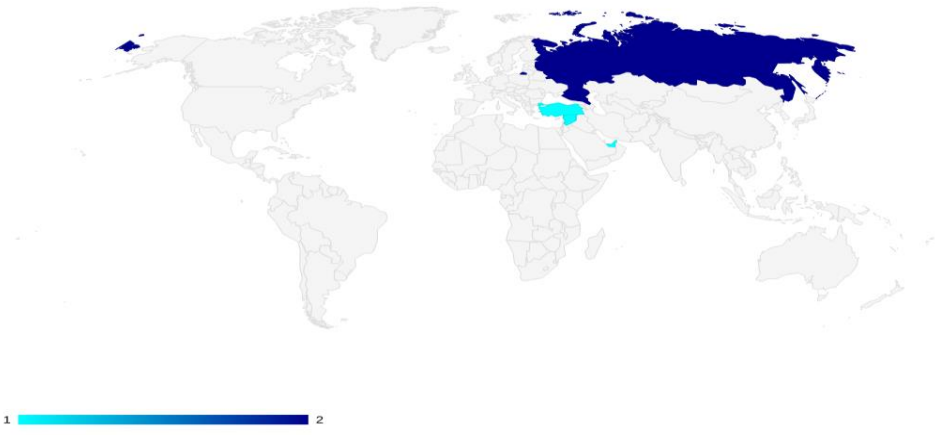
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Romania

VICTIM PROFILE



RUSSIA

OFFENSIVE ACTIONS

State-Sponsored APTs (48)
Homegrown APTs (180)

CYBER TECH EXCHANGE

Sales (4)
Purchases (1)

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (12), Kinetic (6), Disinformation (2), Crime (9)

FREEDOM HOUSE

Not Free (0.2)

VICTIM

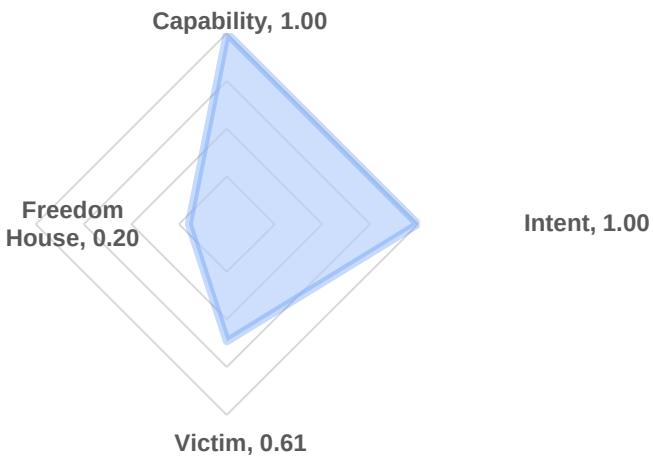
Targeted in 54 documents

THREAT ACTORS

State-Sponsored (10)
APT Threat Actors (47)

COUNTRY PROFILE

Global Power



THREAT ACTORS

APT 29 - 2008

Energetic Bear - 2010

Gamaredon Group (State-sponsored, FSB 16th & 18th Centers) - 2013

Hades - 2017

Sandworm Team - 2009

Fancy Bear (State-sponsored, two GRU units known as Unit 26165 and Unit 74455) - 2004

TeleBots - 2015

TEMP.Veles (State-sponsored, Central Scientific Research Institute of Chemistry and Mechanics) - 2014

Turla - 1996

UNC2452 - 2019

OFFENSIVE PRIVATE VENDORS

Elcomsoft (Analysis, Intrusion, Phone Monitoring)

NORSI TRANS (Analysis, Internet Monitoring, Intrusion, Monitoring Centre)

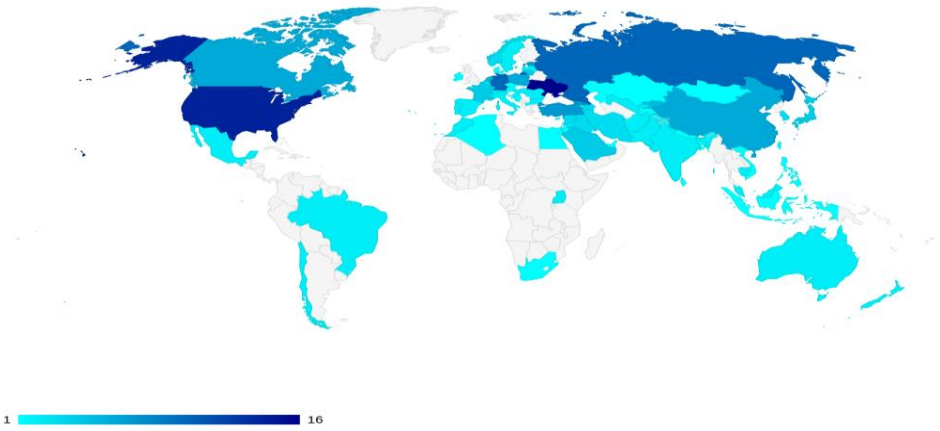
PURCHASED CAPABILITIES

Hacking Team Sales to Russia (Russia - KVANT / Civil) – 2012

TARGETING PROFILE

PRIVATE VENDORS

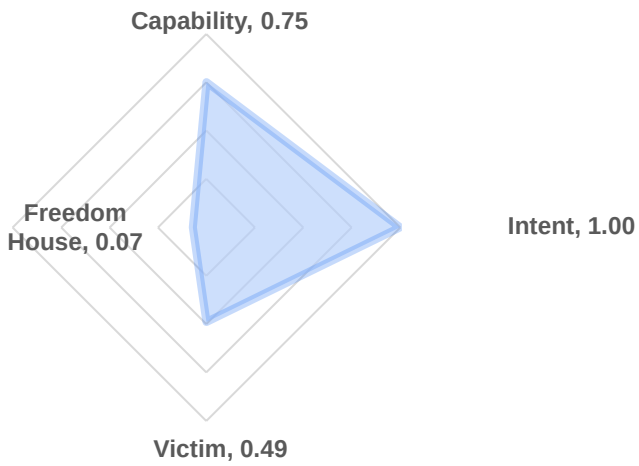
There are 12 private vendors



SAUDI ARABIA

COUNTRY PROFILE

Local Player



OFFENSIVE ACTIONS

State-Sponsored APTs (3)
Homegrown APTs (3)

CYBER TECH EXCHANGE

Purchases (6)

AUTONOMY

Third-Party Capabilities

OBJECTIVES

Espionage (1), Surveillance (1)

FREEDOM HOUSE

Not Free (0.07)

VICTIM

Targeted in 43 documents

THREAT ACTORS

APT Threat Actors (1)

THREAT ACTORS

OurMine (2016)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

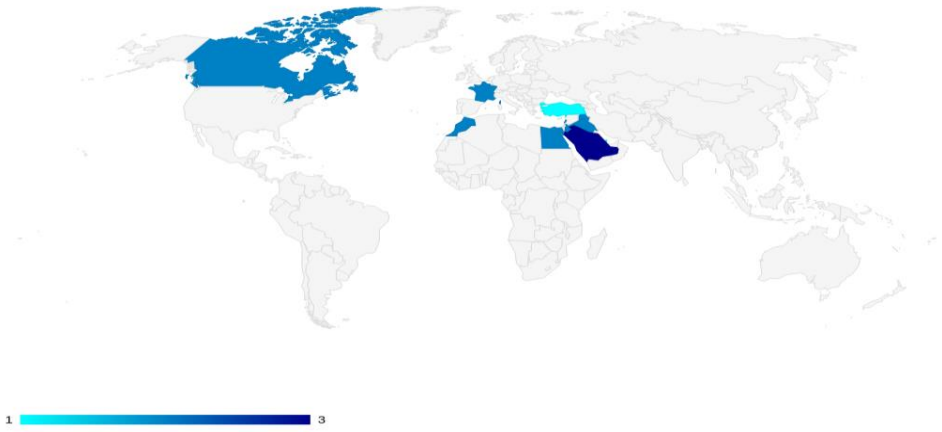
PURCHASED CAPABILITIES

Hacking Team Sales to Saudi Arabia (MOD Saudi / Military) - 2013
NSO Group Sales to Saudi Arabia
Saudi Arabia Purchase of Intrusion software Techology - 2015
FinFisher Sales to Saudi Arabia
Hacking Team Sales to Saudi Arabia (GIP Saudi / Intelligence) - 2013
Hacking Team Sales to Saudi Arabia (Saudi - GID / Intelligence) – 2013

PRIVATE VENDORS

No private providers found

TARGETING PROFILE



SERBIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

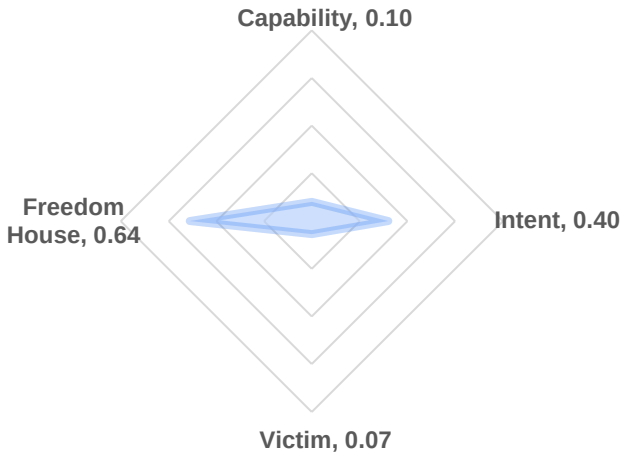
FREEDOM HOUSE
Partly Free (0.64)

VICTIM
Targeted in 6 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

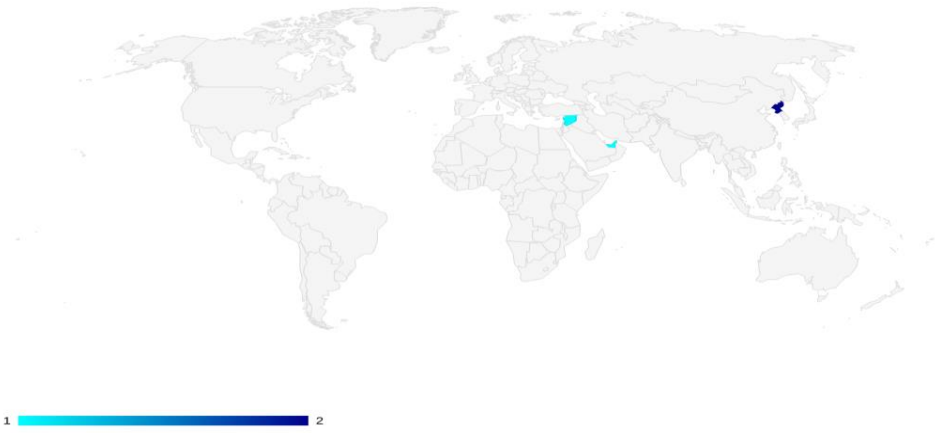
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Serbia (Security Information Agency (BIA) / Intelligence)

VICTIM PROFILE



SINGAPORE

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

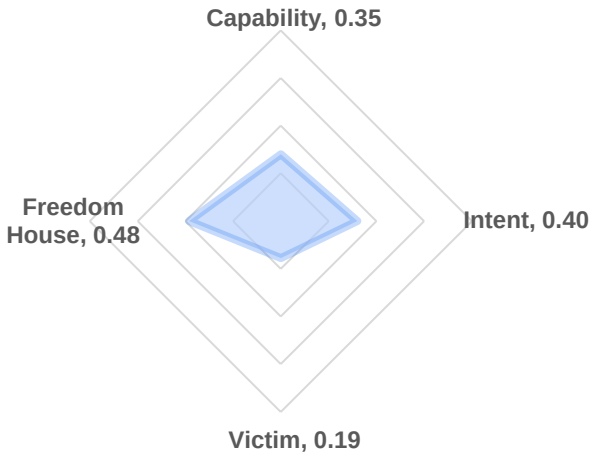
FREEDOM HOUSE
Partly Free (0.48)

VICTIM
Targeted in 17 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 2 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

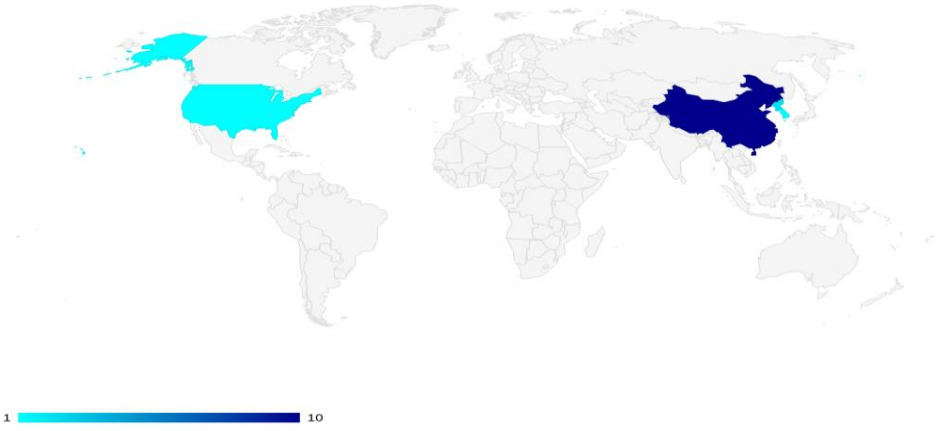
PURCHASED CAPABILITIES

Hacking Team Sales to Singapore (IDA SGP / Civil) - 2008

Singapore Purchase of Intrusion software Techology - 2015

FinFisher Sales to Singapore

VICTIM PROFILE



SLOVENIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (1)
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

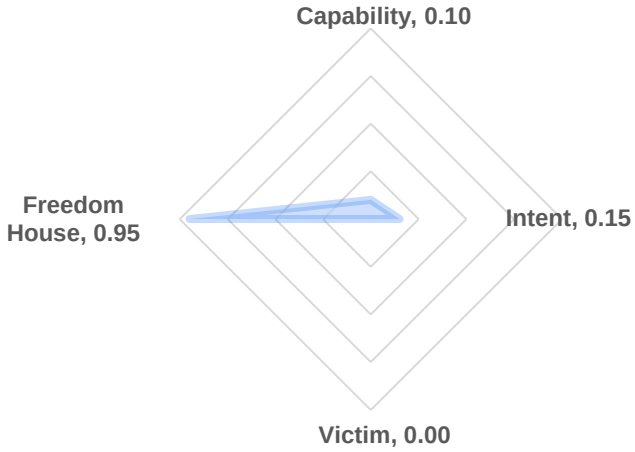
FREEDOM HOUSE
Free (0.95)

VICTIM
Targeted in 0 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 1 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Slovenia

VICTIM PROFILE

SOMALIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

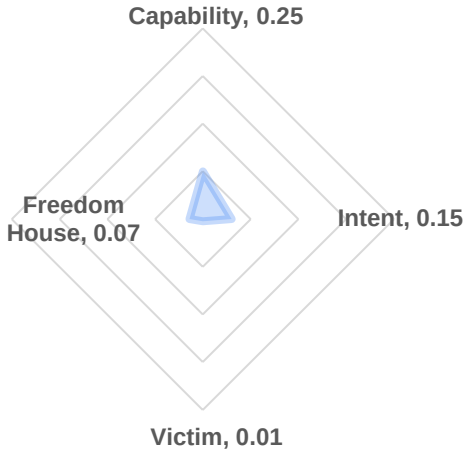
FREEDOM HOUSE
Not Free (0.07)

VICTIM
Targeted in 1 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

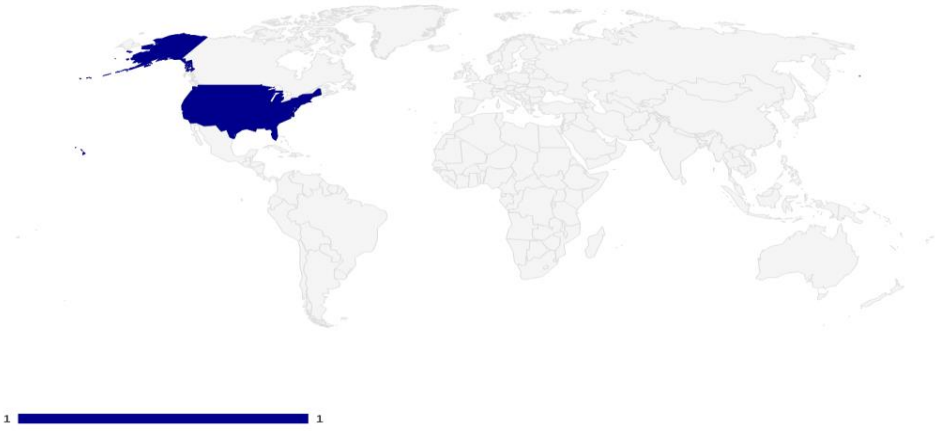
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Netsweeper systems Use in Somalia

VICTIM PROFILE



SOUTH AFRICA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (1)
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

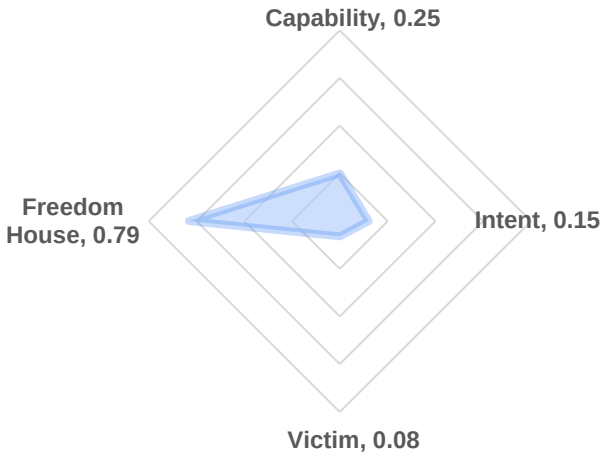
FREEDOM HOUSE
Free (0.79)

VICTIM
Targeted in 7 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 10 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

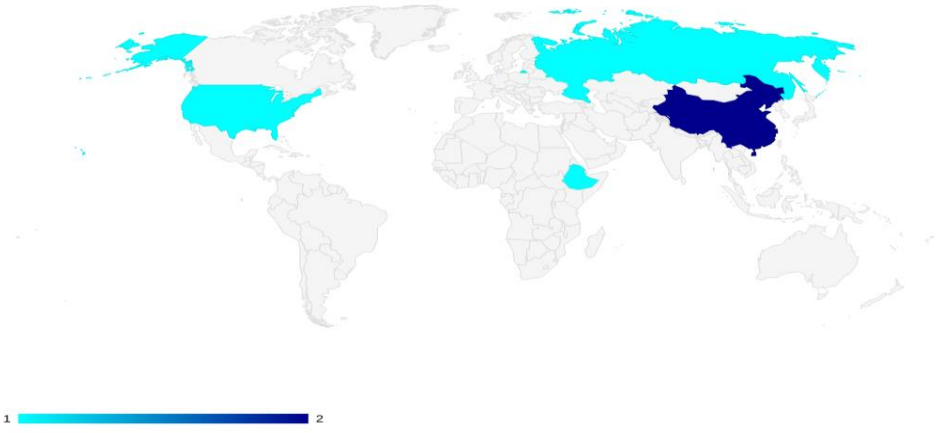
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to South Africa

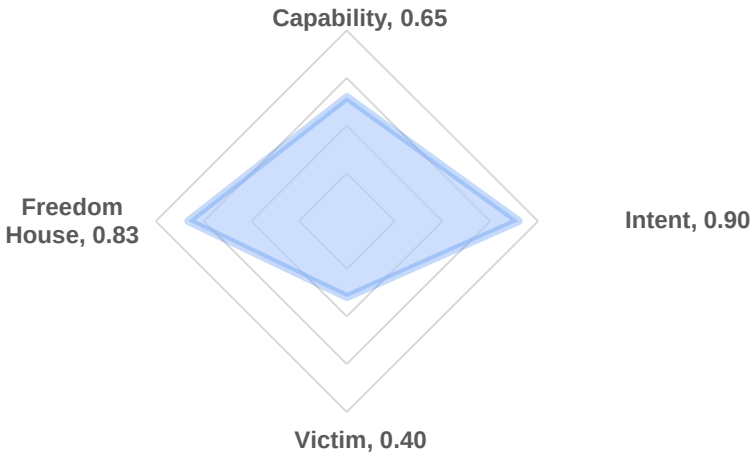
VICTIM PROFILE



SOUTH KOREA

COUNTRY PROFILE

Regional Contender



OFFENSIVE ACTIONS
State-Sponsored APTs (2)

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
Espionage (1)

FREEDOM HOUSE
Free (0.83)

VICTIM
Targeted in 35 documents

THREAT ACTORS
State-Sponsored (2)
APT Threat Actors (1)

PRIVATE VENDORS
There are 2 private vendors

THREAT ACTORS

DarkHotel (2007)

OnionDog (2013)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to South Korea (The 5163 Army Division / Military) - 2012

TARGETING PROFILE

SPAIN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

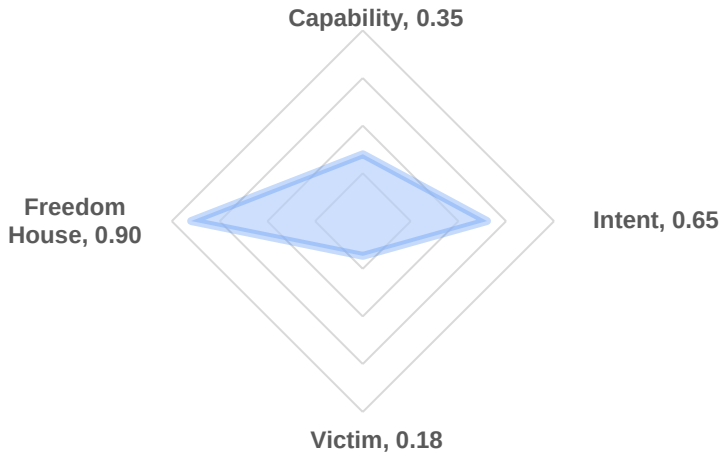
FREEDOM HOUSE
Free (0.9)

VICTIM
Targeted in 16 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 7 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

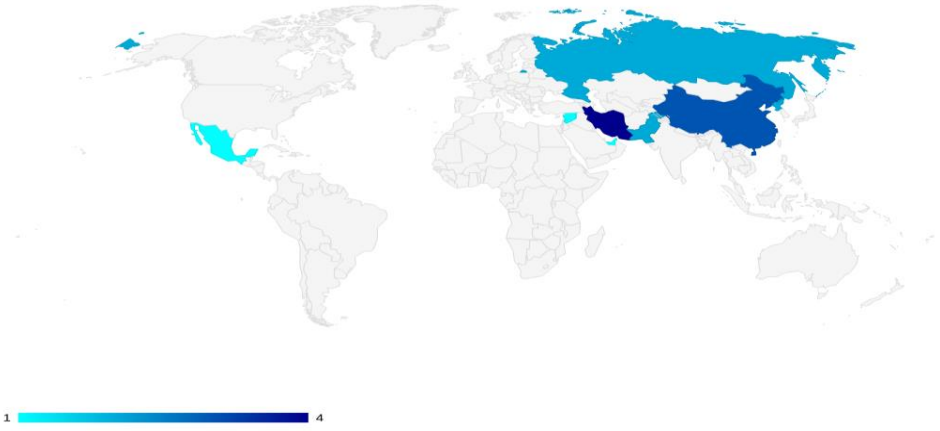
PURCHASED CAPABILITIES

Hacking Team Sales to Spain (CNI / Intelligence) - 2006

FinFisher Sales to Spain

Hacking Team Sales to Spain (CNI / Intelligence) - 2006

VICTIM PROFILE



SUDAN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

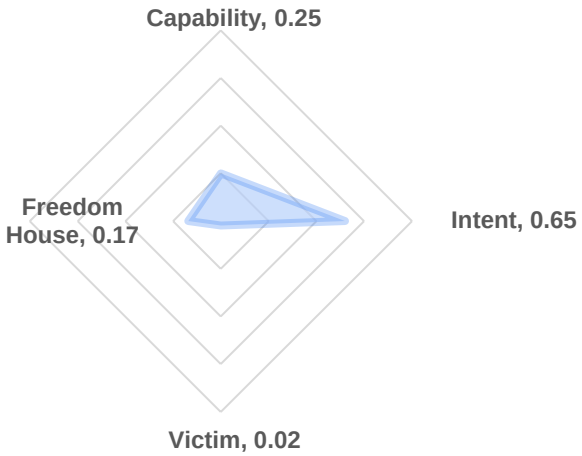
FREEDOM HOUSE
Not Free (0.17)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

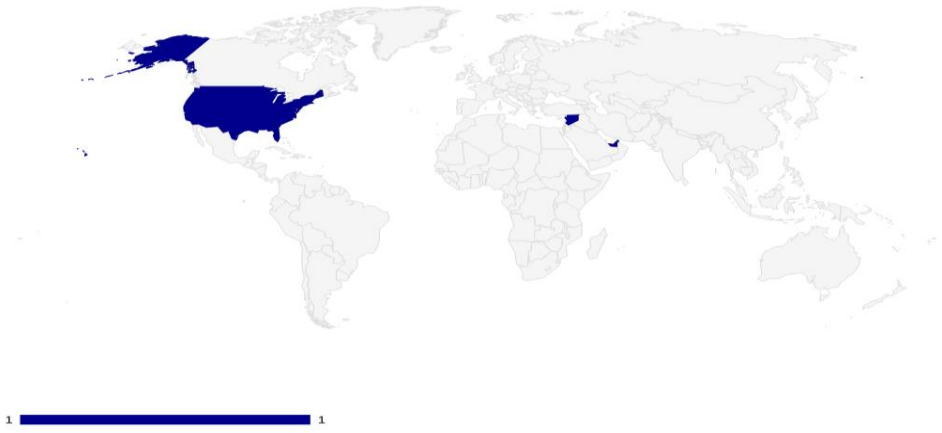
PURCHASED CAPABILITIES

Hacking Team Sales to Sudan (NISS - National Intelligence and Security Services / Intelligence) - 2012

Netsweeper systems Use in Sudan

Hacking Team Sales to Sudan (NISS - National Intelligence and Security Services / Intelligence) - 2012

VICTIM PROFILE



SWEDEN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (7)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

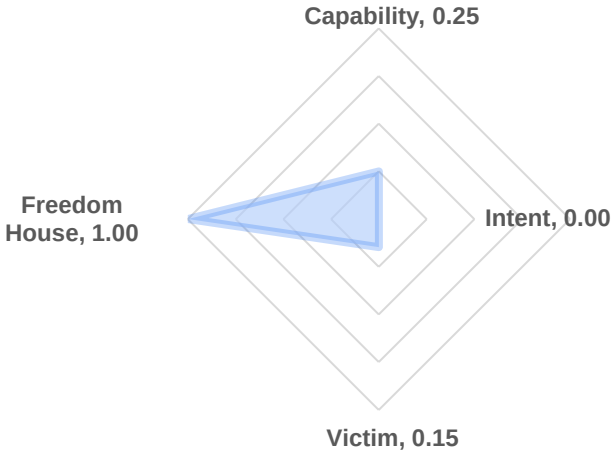
FREEDOM HOUSE
Free (1)

VICTIM
Targeted in 13 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
There are 10 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

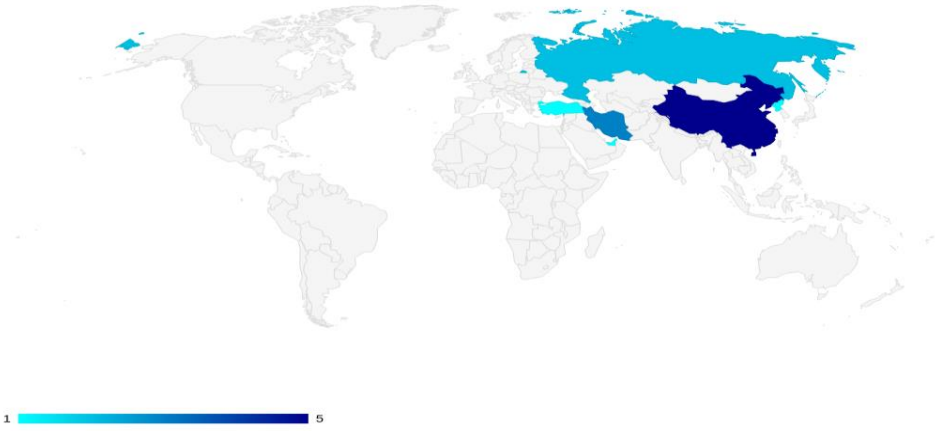
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

No purchases found

VICTIM PROFILE



SWITZERLAND

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Sales (42)
Purchases (2)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

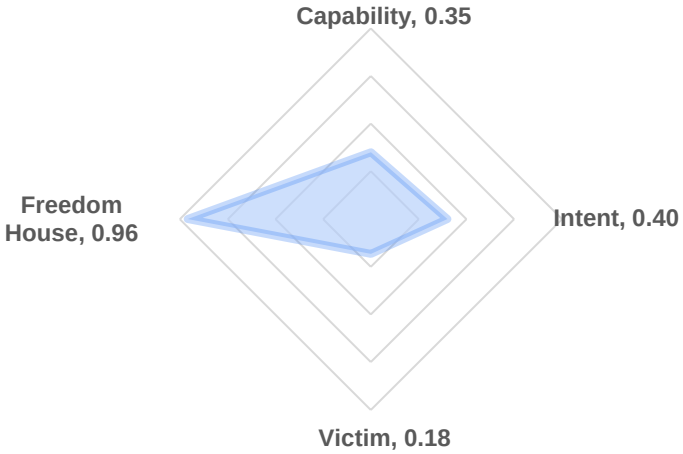
FREEDOM HOUSE
Free (0.96)

VICTIM
Targeted in 16 documents

THREAT ACTORS
APT Threat Actors (1)

PRIVATE VENDORS
There are 9 private vendors

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

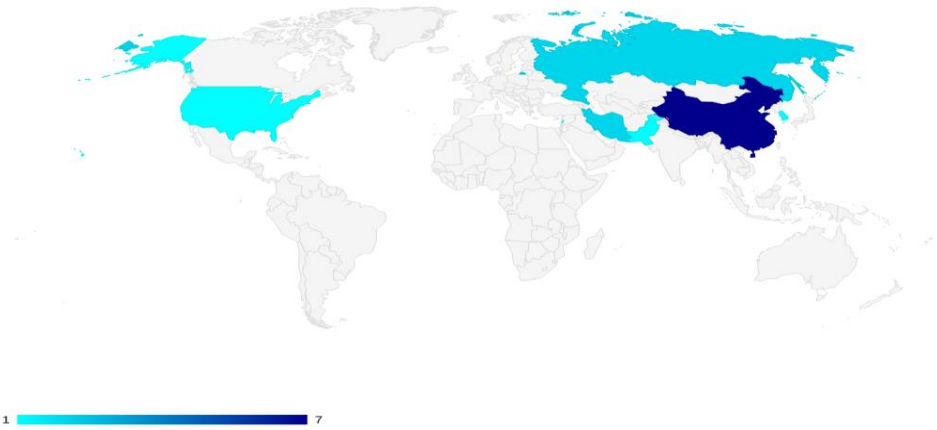
OFFENSIVE PRIVATE VENDORS

3i-MIND (Analysis)
Dreamlab Technologies AG (Lawful Interception, VOIP LI , Trojans)
ERA IT Solutions AG (Trojans)

PURCHASED CAPABILITIES

Hacking Team Sales to Switzerland (Kantonspolizei Zurich / LEA) - 2014
NSO Group Sales to Switzerland

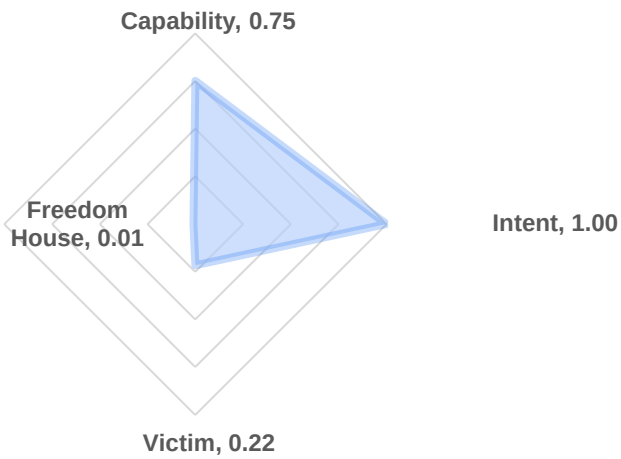
VICTIM PROFILE



COUNTRY PROFILE

Regional Contender

SYRIA



OFFENSIVE ACTIONS

State-Sponsored APTs (3)
Homegrown APTs (6)

CYBER TECH EXCHANGE

Purchases (3)

AUTONOMY

Third-Party Capabilities

OBJECTIVES

Surveillance (1)

FREEDOM HOUSE

Not Free (0.01)

VICTIM

Targeted in 19 documents

THREAT ACTORS

Syrian Electronic Army (2011)
Goldmouse (2014)
Pat Bear (2015)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Amesys Sales to Syria - 2007
Area SpA Sales to Syria (225, Syrian intelligence / Intelligence) - 2009
Trovicor Sales to Syria (Syriatel / Civil) – 2009

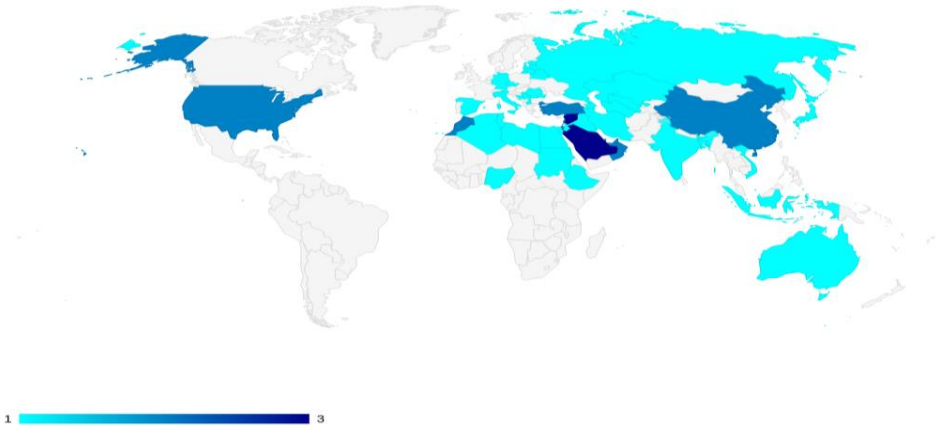
TARGETING PROFILE

THREAT ACTORS

State-Sponsored (2)
APT Threat Actors (3)

PRIVATE VENDORS

No private providers found



TAIWAN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

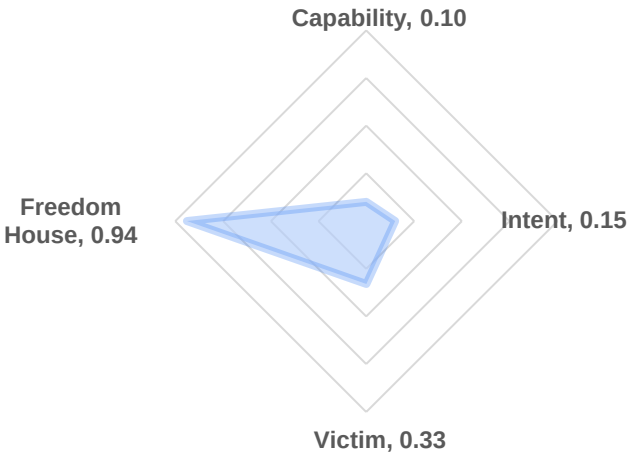
FREEDOM HOUSE
Free (0.94)

VICTIM
Targeted in 29 documents

THREAT ACTORS
APT Threat Actors (1)

PRIVATE VENDORS
There are 2 private vendors

COUNTRY PROFILE



THREAT ACTORS

APT-C-01 (2020)

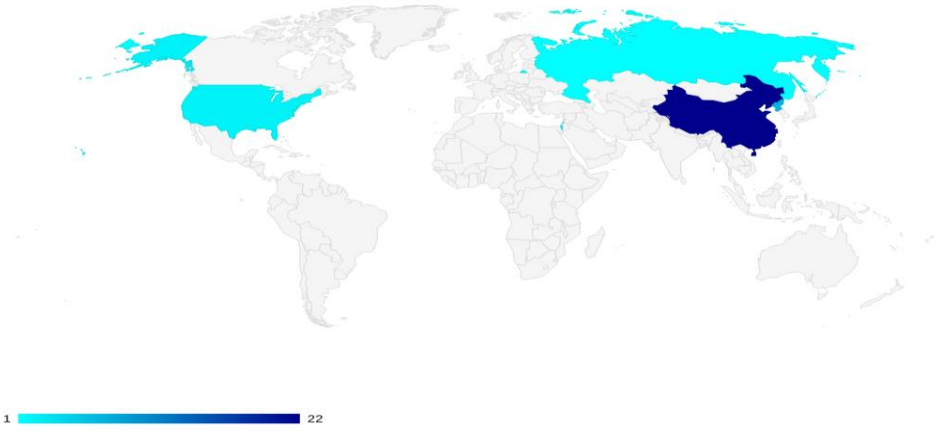
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Taiwan

VICTIM PROFILE



TAJIKISTAN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

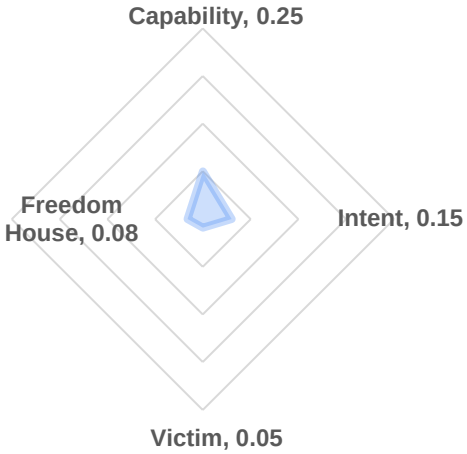
FREEDOM HOUSE
Not Free (0.08)

VICTIM
Targeted in 4 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

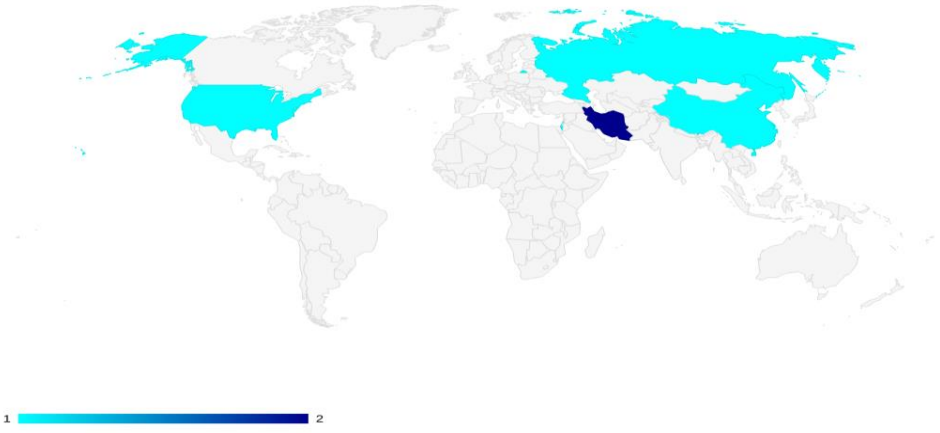
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Trovicor Sales to Tajikistan (Government of Tajikistan / Civil) - 2010

VICTIM PROFILE



THAILAND

OFFENSIVE ACTIONS
State-Sponsored APTs (1)
Homegrown APTs (1)

CYBER TECH EXCHANGE
Purchases (3)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Surveillance (1)

FREEDOM HOUSE
Not Free (0.3)

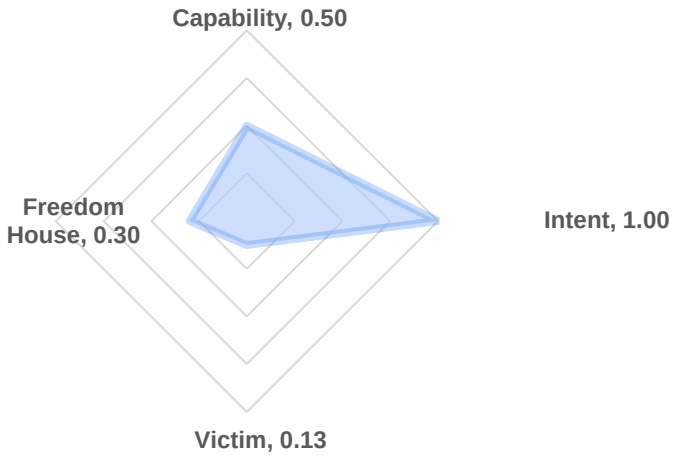
VICTIM
Targeted in 11 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

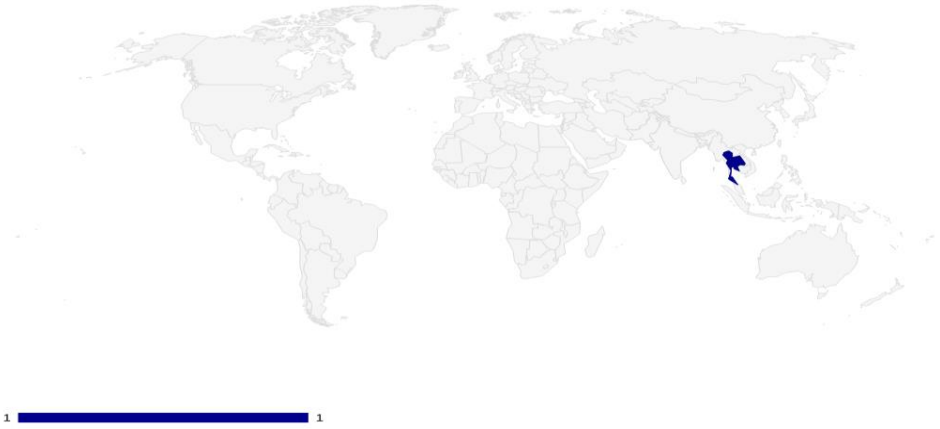
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Thailand (Royal Thai Army / Military) - 2014
Cyberbit Sales to Thailand (Royal Thai Army / Military) - 2017
Hacking Team Sales to Thailand (Dept. of Correction Thai Police / LEA) - 2014

TARGETING PROFILE



TOGO

OFFENSIVE ACTIONS
State-Sponsored APTs (1)

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Surveillance (1)

FREEDOM HOUSE
Partly Free (0.43)

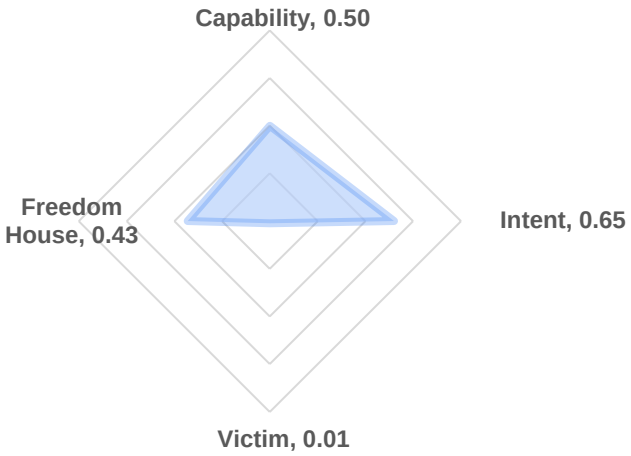
VICTIM
Targeted in 1 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

NSO Group Sales to Togo

TARGETING PROFILE

TUNISIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

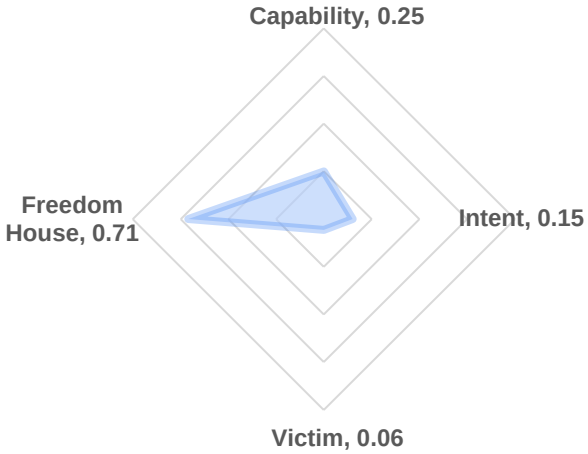
FREEDOM HOUSE
Free (0.71)

VICTIM
Targeted in 5 documents

THREAT ACTORS
APT Threat Actors (2)

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

Corsair Jackal

Rebel Jackal

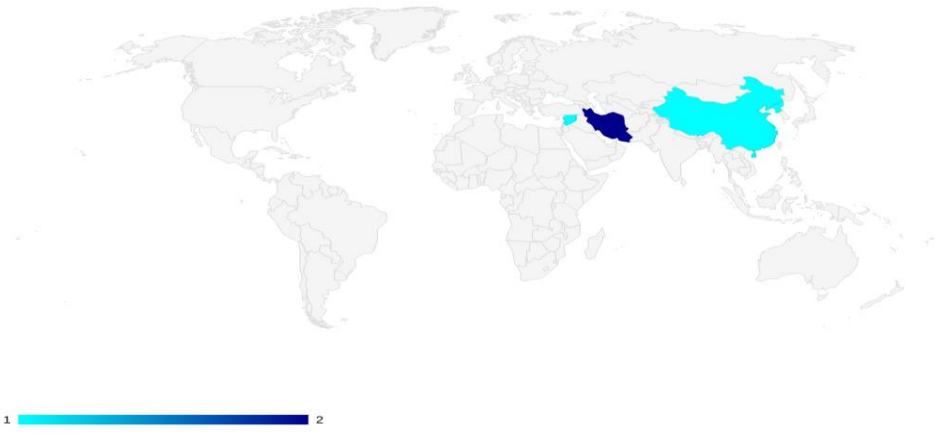
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

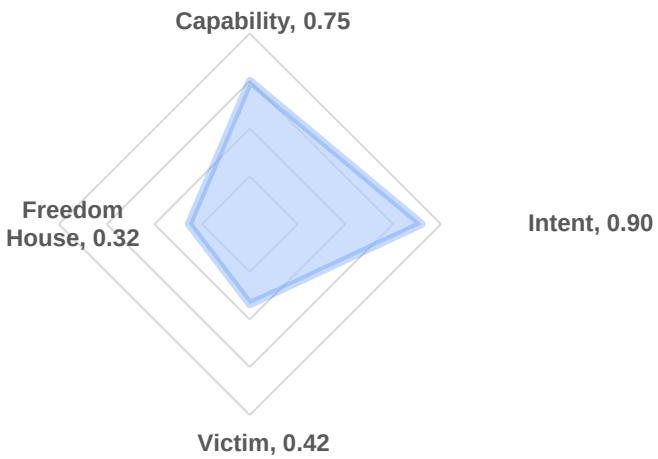
Trovicor Sales to Tunisia (Government of Tunisia / Civil)

VICTIM PROFILE



COUNTRY PROFILE

Regional Contender



TURKEY

OFFENSIVE ACTIONS

State-Sponsored APTs (5)
Homegrown APTs (6)

CYBER TECH EXCHANGE

Purchases (3)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

Espionage (3), Crime (1)

FREEDOM HOUSE

Not Free (0.32)

VICTIM

Targeted in 37 documents

THREAT ACTORS

Neodymium (2016)
StrongPity (2012)
Sea Turtle (2017)
Vendetta (2020)
Sath-Ä± MÃ¼dafaa
Aslan Neferler Tim
AyyÄ±ldÄ±z Tim
TurkHackTeam
KingSqlZ

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Turkey (Turkish National Police / LEA) - 2011
Sandvine Use in Turkey (Türk Telekom's network / Civil)
FinFisher Sales to Turkey

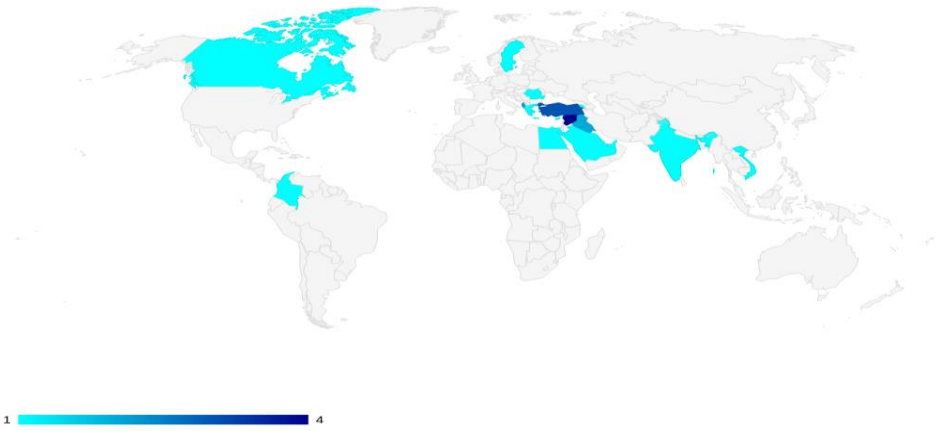
TARGETING PROFILE

THREAT ACTORS

State-Sponsored (2)
APT Threat Actors (9)

PRIVATE VENDORS

There are 6 private vendors



TURKMENISTAN

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

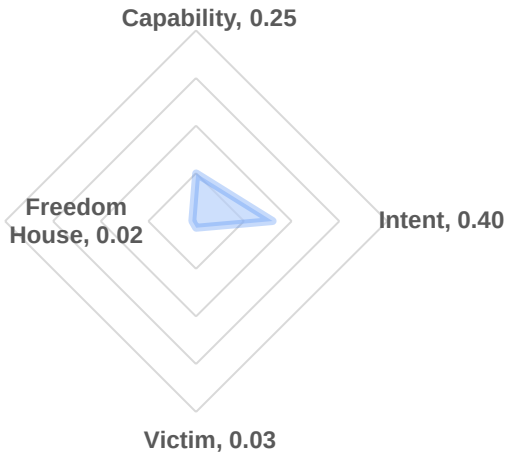
FREEDOM HOUSE
Not Free (0.02)

VICTIM
Targeted in 3 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Dreamlab Sales to Turkmenistan (Government of Turkmenistan / Civil) - 2010

FinFisher Sales to Turkmenistan (Ministry of Communications / Civil)

VICTIM PROFILE

UGANDA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

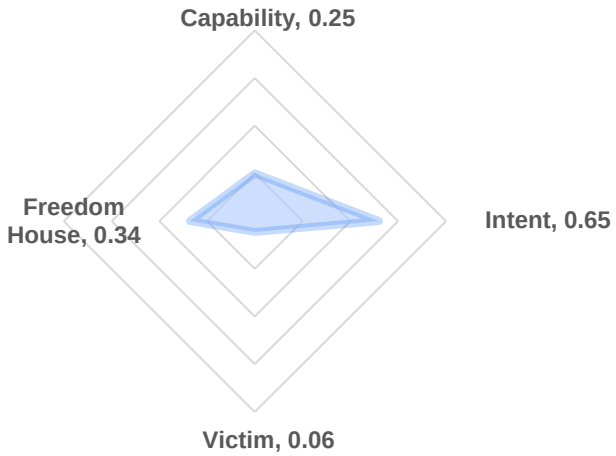
FREEDOM HOUSE
Not Free (0.34)

VICTIM
Targeted in 5 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

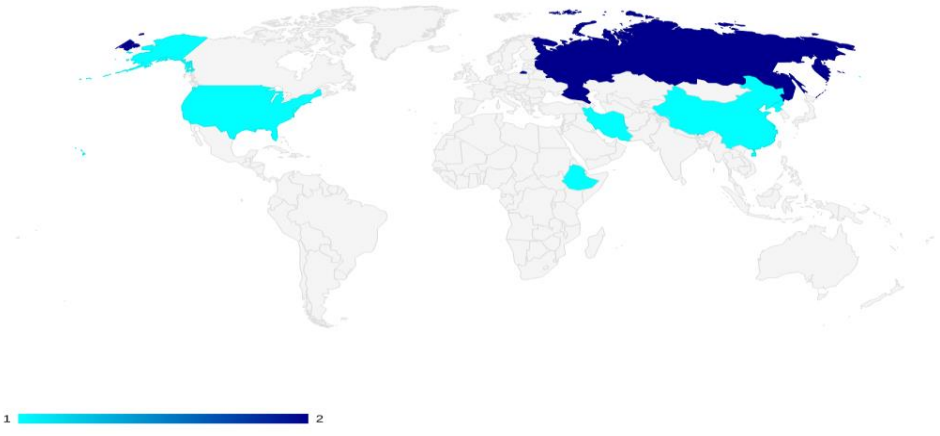
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

NICE Systems Sales to Uganda (Chieftaincy of Military Intelligence, Special Forces Command Counter Intelligence / Intelligence) - 2015

FinFisher Sales to Uganda - 2012

VICTIM PROFILE



UKRAINE

OFFENSIVE ACTIONS
Homegrown APTs (5)

CYBER TECH EXCHANGE
No sales or purchases found

AUTONOMY
Some Indigenous Capabilities

OBJECTIVES
No objectives found

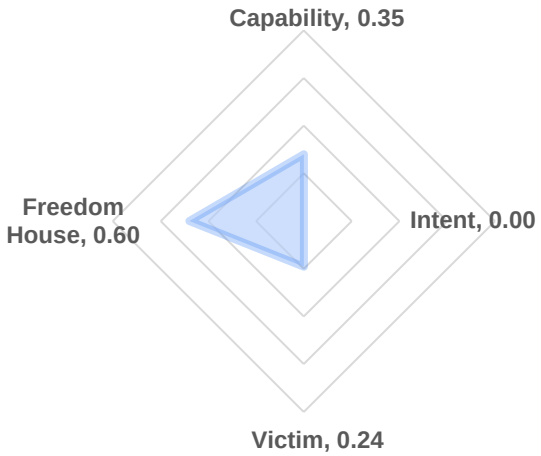
FREEDOM HOUSE
Partly Free (0.6)

VICTIM
Targeted in 21 documents

THREAT ACTORS
APT Threat Actors (4)

PRIVATE VENDORS
There are 4 private vendors

COUNTRY PROFILE



THREAT ACTORS

Carbanak (2013)
Operation Groundbait (2008)
Operation Poison Needles (2018)
Groundbait

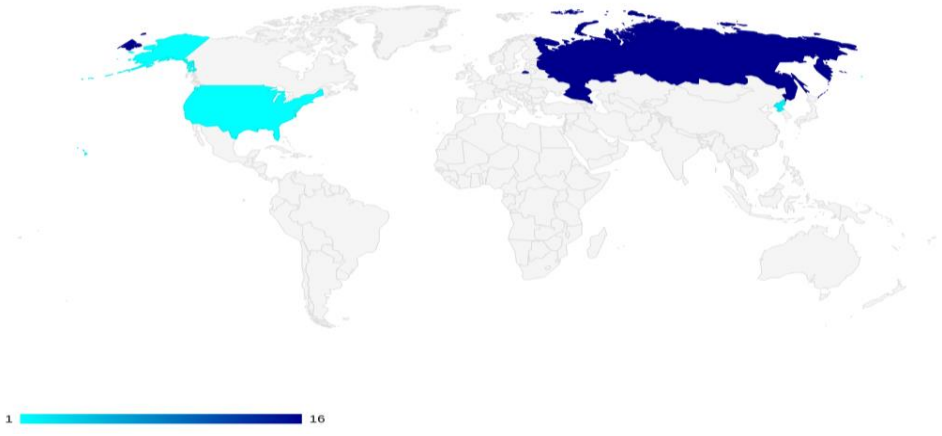
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

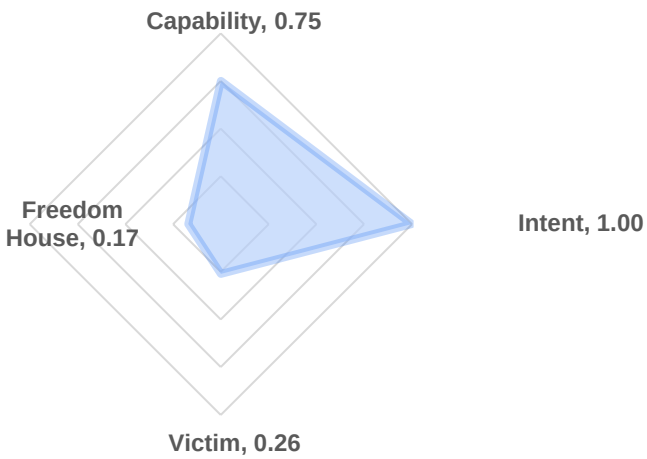
No purchases found

VICTIM PROFILE



COUNTRY PROFILE

Regional Contender



UNITED ARAB EMIRATES

OFFENSIVE ACTIONS

State-Sponsored APTs (4)
Homegrown APTs (7)

CYBER TECH EXCHANGE

Purchases (8)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

Espionage (2), Surveillance (1)

FREEDOM HOUSE

Not Free (0.17)

VICTIM

Targeted in 23 documents

THREAT ACTORS

State-Sponsored (1)

THREAT ACTORS

Viking Jackal

Stealth Falcon (2012)

OFFENSIVE PRIVATE VENDORS

Stratign (Internet Monitoring, Phone Monitoring, Monitoring Centre, Analysis, Counter-Surveillance, Equipment, Intrusion, Monitoring Centres, Communications Monitoring)

PURCHASED CAPABILITIES

Hacking Team Sales to United Arab Emirates (UAE - Intelligence / Intelligence) - 2012

Netsweeper systems Use in UAE

NSO Group Sales to UAE

NSO Group Sales to United Arab Emirates

SS8 Sales to United Arab Emirates - 2009

UAE Purchase of Intrusion software Technology - 2015

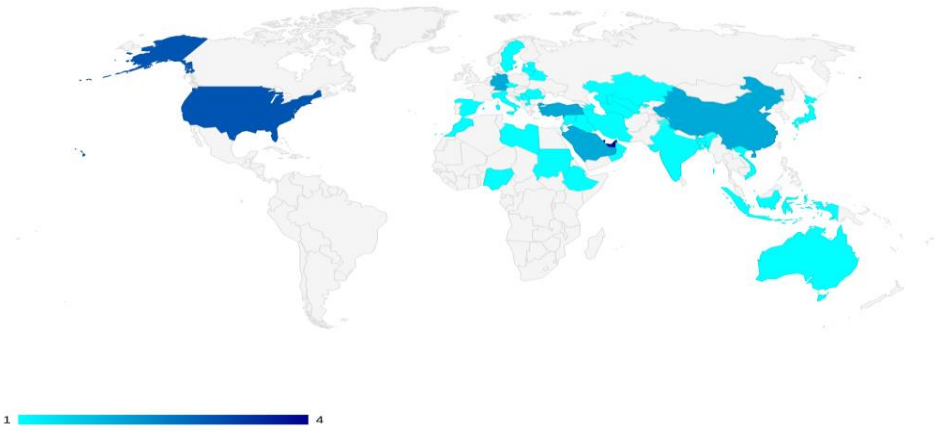
FinFisher Sales to United Arab Emirates

Hacking Team Sales to United Arab Emirates (UAE - MOI / Intelligence) - 2012

TARGETING PROFILE

PRIVATE VENDORS

There are 5 private vendors



UNITED KINGDOM

OFFENSIVE ACTIONS

State-Sponsored APTs (6)
Homegrown APTs (5)

CYBER TECH EXCHANGE

Sales (44)
Purchases (1)

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (5)

FREEDOM HOUSE

Free (0.93)

VICTIM

Targeted in 32 documents

THREAT ACTORS

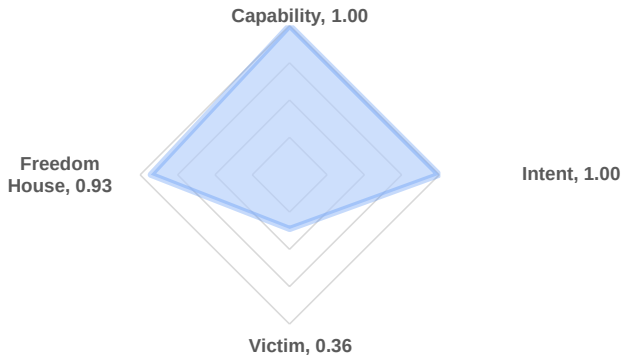
State-Sponsored (1)
APT Threat Actors (2)

PRIVATE VENDORS

There are 102 private vendors

COUNTRY PROFILE

Global Power



THREAT ACTORS

GCHQ (1919) – Equation Group

OFFENSIVE PRIVATE VENDORS

Gamma Group (Intrusion, Phone Monitoring, Internet Monitoring, Monitoring Centre, Analysis, Audio Surveillance, Video Surveillance, Counter-Surveillance, Equipment, Monitoring Centres, Communications Monitoring, Technical Surveillance)

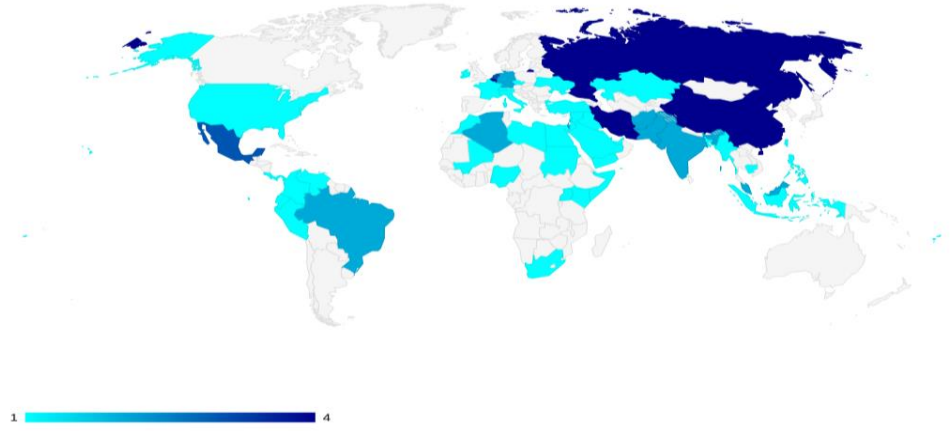
Roke Manor Research (Internet Monitoring, Monitoring Centre, Video Surveillance, Audio Surveillance, Equipment, Location Monitoring, Analysis, Counter-Surveillance, Intrusion, Monitoring Centres, Technical Surveillance)

Sure (Video Surveillance, Audio Surveillance, Phone Monitoring, Location Monitoring, Technical Surveillance, Intrusion)

PURCHASED CAPABILITIES

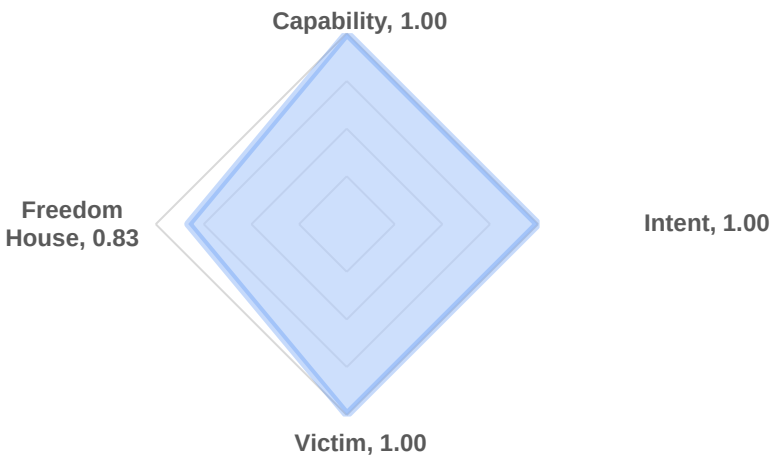
FinFisher Sales to United Kingdom

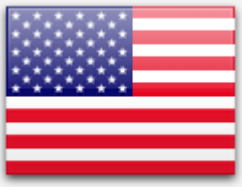
TARGETING PROFILE



COUNTRY PROFILE

Global Power





UNITED STATES

OFFENSIVE ACTIONS

State-Sponsored APTs (13)
Homegrown APTs (8)

CYBER TECH EXCHANGE

Sales (117)
Purchases (5)

AUTONOMY

State Indigenous Capabilities

OBJECTIVES

Espionage (6), Kinetic (1)

FREEDOM HOUSE

Free (0.83)

VICTIM

Targeted in 88 documents

THREAT ACTORS

State-Sponsored (6)
APT Threat Actors (10)

THREAT ACTORS

Longhorn (2009)

Equation Group (2001)

Operation Olympic Games (2007)

Strider (2011)

Shadow Brokers (2016)

Vault 7/8 (2017)

Pizzo Spider

OFFENSIVE PRIVATE VENDORS

BlueCoat (Intelligence Centers, Deep Packet Inspection, Internet Filtering)

Endgame Systems (Intrusion)

Harris (Phone Monitoring, Video Surveillance, Equipment, Intrusion)

SS8 Networks (Internet Monitoring, Phone Monitoring, Analysis, Intrusion)

TeleStrategies (Internet Monitoring, Location Monitoring, Analysis, Intrusion, Biometrics, Monitoring Centre, Communications Monitoring, Monitoring Centres)

Verint (Phone Monitoring, Monitoring Centre, Internet Monitoring, Video Surveillance, Analysis, Location Monitoring, Communications Monitoring)

PURCHASED CAPABILITIES

Hacking Team Sales to United States of America (Drug Enforcement Administration / LEA) - 2012

SS8 Sales to United States of America (Drug Enforcement Administration / LEA) - 2010

FinFisher Sales to United States of America

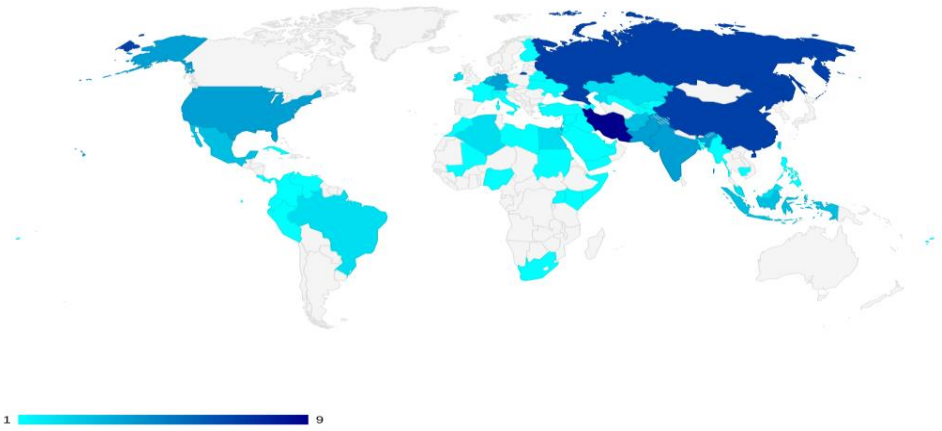
Hacking Team Sales to United States of America (DOD / Military) - 2011

Hacking Team Sales to United States of America (FBI / LEA) - 2011

TARGETING PROFILE

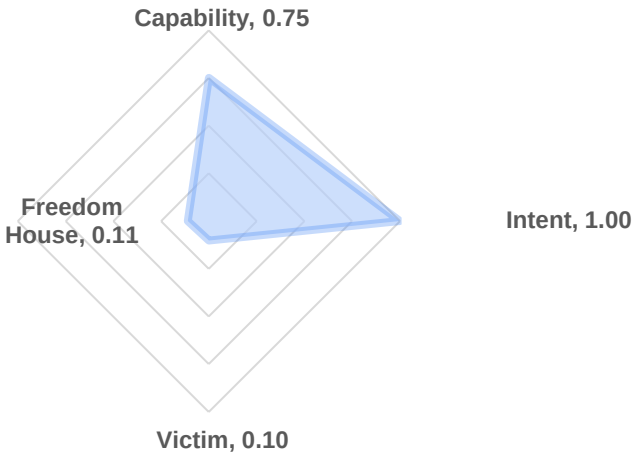
PRIVATE VENDORS

There are 126 private vendors



COUNTRY PROFILE

Local Player



UZBEKISTAN

OFFENSIVE ACTIONS

State-Sponsored APTs (2)
Homegrown APTs (3)

CYBER TECH EXCHANGE

Purchases (4)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

Espionage (1), Surveillance (1)

FREEDOM HOUSE

Not Free (0.11)

VICTIM

Targeted in 9 documents

THREAT ACTORS

State-Sponsored (1)

THREAT ACTORS

SandCat (2018)

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Uzbekistan (NSS / Intelligence) - 2011

NICE Systems Sales to Uzbekistan (National Security Service (SNB) / Intelligence)

NSO Group Sales to Uzbekistan

Cyberbit Sales to Uzbekistan (Uzbekistan's National Security Service / Intelligence) – 2017

APT Threat Actors (1)

PRIVATE VENDORS

No private providers found

TARGETING PROFILE

VENEZUELA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (1)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
No objectives found

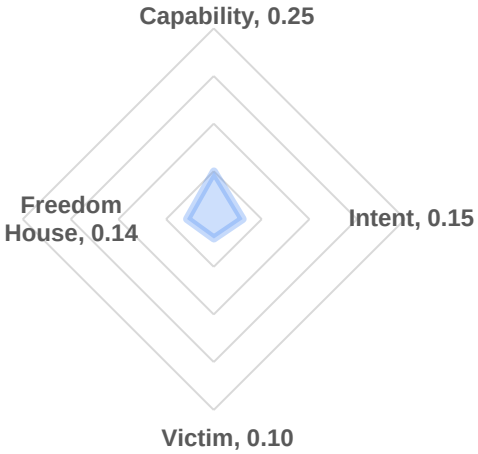
FREEDOM HOUSE
Not Free (0.14)

VICTIM
Targeted in 9 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

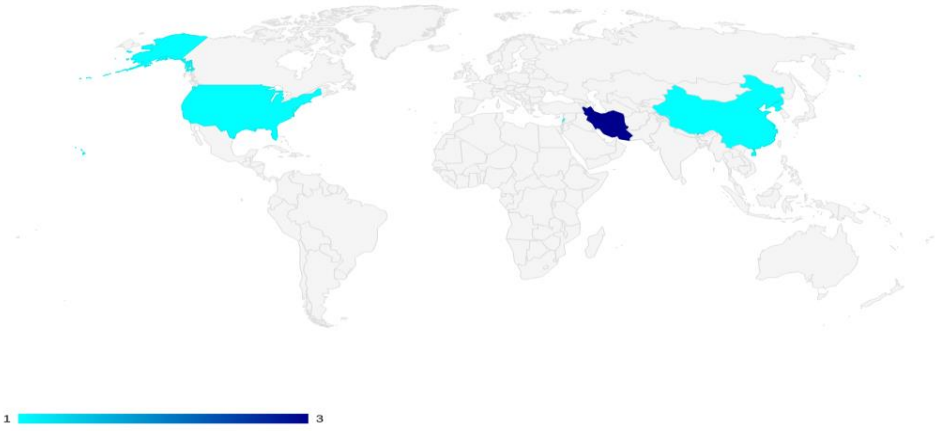
OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

FinFisher Sales to Venezuela

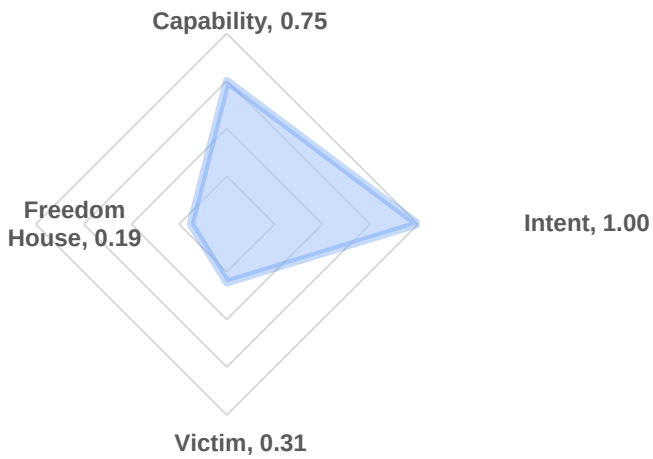
VICTIM PROFILE



VIET NAM

COUNTRY PROFILE

Regional Contender



OFFENSIVE ACTIONS

State-Sponsored APTs (5)
Homegrown APTs (14)

CYBER TECH EXCHANGE

Purchases (2)

AUTONOMY

Some Indigenous Capabilities

OBJECTIVES

Espionage (1), Surveillance (1)

FREEDOM HOUSE

Not Free (0.19)

VICTIM

Targeted in 27 documents

THREAT ACTORS

State-Sponsored (1)
APT Threat Actors (2)

PRIVATE VENDORS

No private providers found

THREAT ACTORS

APT 32 (2013)

Bismuth (2012)

OFFENSIVE PRIVATE VENDORS

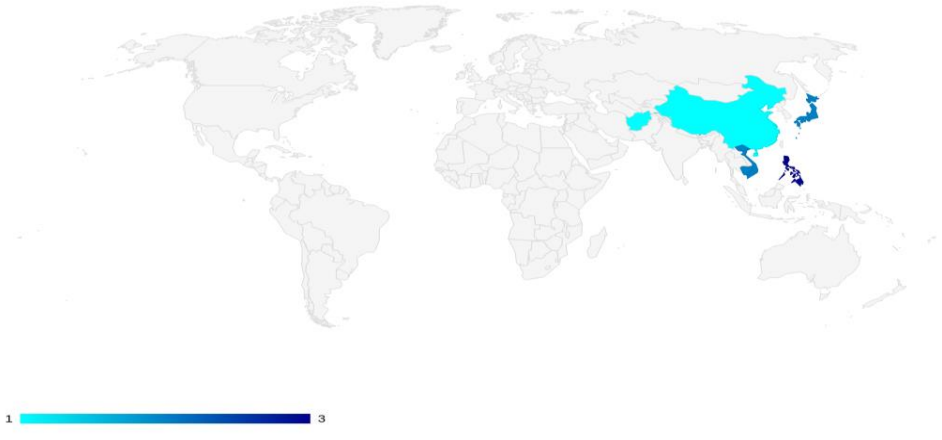
No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Hacking Team Sales to Vietnam (Vietnam GD1 / Intelligence) - 2015

FinFisher Sales to Vietnam

TARGETING PROFILE



YEMEN

OFFENSIVE ACTIONS
State-Sponsored APTs (2)

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Surveillance (2)

FREEDOM HOUSE
Not Free (0.11)

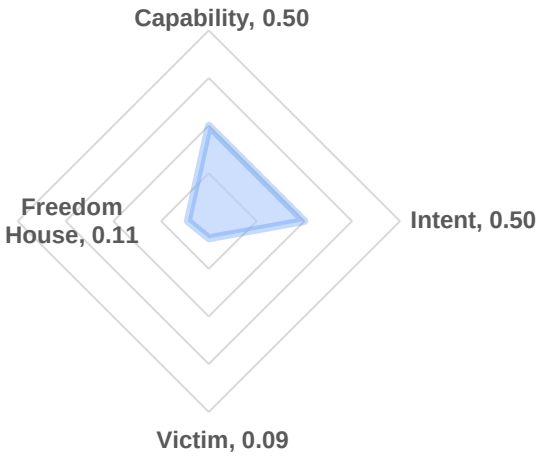
VICTIM
Targeted in 8 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE

Local Player



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

Netsweeper systems Use in Yemen

Trovicor Sales to Yemen - 2009

TARGETING PROFILE

ZAMBIA

OFFENSIVE ACTIONS
No offensive actions found

CYBER TECH EXCHANGE
Purchases (2)

AUTONOMY
Third-Party Capabilities

OBJECTIVES
Espionage (1)

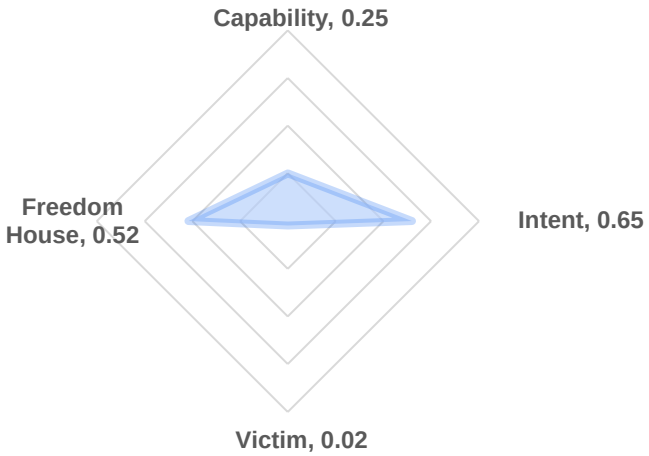
FREEDOM HOUSE
Partly Free (0.52)

VICTIM
Targeted in 2 documents

THREAT ACTORS
No threat-actors found

PRIVATE VENDORS
No private providers found

COUNTRY PROFILE



THREAT ACTORS

No threat-actors found

OFFENSIVE PRIVATE VENDORS

No cyber offensive capabilities private vendors found

PURCHASED CAPABILITIES

NSO Group Sales to Zambia

Cyberbit Sales to Zambia (Zambia's Financial Intelligence Centre / Intelligence) - 2017

TARGETING PROFILE

APPENDIX D - DICTIONARIES

Aeroespacial	aeb
Aeroespacial	aeronautical
Aeroespacial	aerospace
Aeroespacial	astronomy
Aeroespacial	avionic
Aeroespacial	ballistic
Aeroespacial	blue origin
Aeroespacial	european space agency
Aeroespacial	geostationary
Aeroespacial	isro
Aeroespacial	nasa
Aeroespacial	orbit
Aeroespacial	pockocmoc
Aeroespacial	roskosmos
Aeroespacial	satellite
Aeroespacial	space program
Aeroespacial	space travel
Aeroespacial	spacecraft
Aeroespacial	spaceflight
Aeroespacial	spacex
Aeroespacial	terrestrial
Aeroespacial	unmanned
Aeroespacial	virgin galactic
Aviação	aeroplane
Aviação	airbus
Aviação	aircraft
Aviação	airline
Aviação	airplane
Aviação	airport
Aviação	aviation
Aviação	bae systems
Aviação	boeing
Aviação	bombardier
Aviação	embraer
Aviação	jet
Aviação	jetliner
Aviação	lockheed martin
Aviação	northrop group
Aviação	plane
Aviação	qantas
Aviação	raytheon
Aviação	safran
Aviação	travel ban
Financeiro	Agricultural Bank of China
Financeiro	atm jackpot
Financeiro	atm malware
Financeiro	Banco do Brasil
Financeiro	Banco Inter
Financeiro	Banco Safra
Financeiro	Banco Santander
Financeiro	Bank of America
Financeiro	Bank of China
Financeiro	Bank of Communications
Financeiro	banking companies
Financeiro	banking instituitions
Financeiro	Banrisul
Financeiro	Barclays
Financeiro	BBVA
Financeiro	Bilbao Vizcaya
Financeiro	BMG
Financeiro	BNP Paribas
Financeiro	BPI
Financeiro	Bradesco
Financeiro	BTG
Financeiro	Caixa Economica
Financeiro	Caixa Geral
Financeiro	cash-out scheme
Financeiro	central bank
Financeiro	Cetelem
Financeiro	China Construction Bank
Financeiro	China Merchants Bank
Financeiro	Citibank
Financeiro	Citigroup Inc.
Financeiro	Crédit Agricole
Financeiro	Deutsche Bank
Financeiro	ebanx

Financeiro	electronic debit
Financeiro	exchange currency
Financeiro	Febraban
Financeiro	finance sector
Financeiro	financial
Financeiro	financial entities
Financeiro	financial industries
Financeiro	financial industry
Financeiro	financial instituitions
Financeiro	financial sector
Financeiro	financial services
Financeiro	fintech
Financeiro	Groupe BPCE
Financeiro	HSBC
Financeiro	Industrial and Commercial Bank of China
Financeiro	ING Group
Financeiro	insurance
Financeiro	investment
Financeiro	Itau
Financeiro	Japan Post Bank
Financeiro	JP Morgan
Financeiro	Lloyds Banking Group
Financeiro	loans
Financeiro	Mitsubishi UFJ Financial Group
Financeiro	Mizuho Financial Group
Financeiro	mortgage
Financeiro	Postal Savings Bank of China
Financeiro	Royal Bank of Canada
Financeiro	Santander
Financeiro	Scotiabank
Financeiro	Sicoob
Financeiro	Sicredi
Financeiro	Société Générale
Financeiro	Sofisa
Financeiro	stocks
Financeiro	Sumitomo Mitsui Financial Group
Financeiro	Toronto-Dominion Bank
Financeiro	Unibanco
Financeiro	Wells Fargo
Alvos Políticos	activist
Alvos Políticos	civil society
Alvos Políticos	clashes
Alvos Políticos	crackdown
Alvos Políticos	demonstrator
Alvos Políticos	dissident
Alvos Políticos	extremist
Alvos Políticos	human rights
Alvos Políticos	labor unions
Alvos Políticos	militant
Alvos Políticos	nationalist
Alvos Políticos	ngo
Alvos Políticos	non-governmental organization
Alvos Políticos	opposition
Alvos Políticos	political organization
Alvos Políticos	political party
Alvos Políticos	pro-democracy
Alvos Políticos	protest
Alvos Políticos	rebels
Alvos Políticos	refugee
Alvos Políticos	revolt
Alvos Políticos	riot
Alvos Políticos	separatist
Alvos Políticos	unrest
Alvos Políticos	uprising
Diplomacia	ambassador
Diplomacia	asean
Diplomacia	consul
Diplomacia	diplomacy
Diplomacia	diplomat
Diplomacia	embassy
Diplomacia	envoy
Diplomacia	Food and Agriculture Organization
Diplomacia	foreign affairs
Diplomacia	humanitarian
Diplomacia	ICAO

Diplomacia IMF

Diplomacia International Labour Organization

Diplomacia International Maritime Organization

Diplomacia international organization

Diplomacia international political groups

Diplomacia International Telecommunication Union

Diplomacia Joint United Nations Programme on HIV

Diplomacia monitary fund

Diplomacia multilateral

Diplomacia multinational

Diplomacia oas

Diplomacia ocde

Diplomacia peacekeepers

Diplomacia peacekeeping

Diplomacia trade bodies

Diplomacia UNESCO

Diplomacia UNHRC

Diplomacia UNICEF

Diplomacia UNISDR

Diplomacia united nations

Diplomacia United Nations Capital Development Fund

Diplomacia United Nations Development Programme

Diplomacia United Nations Educational

Diplomacia United Nations Environment Programme

Diplomacia United Nations Human Settlements Programme

Diplomacia United Nations Industrial Development Organization

Diplomacia Universal Postal Union

Diplomacia UNODC

Diplomacia world bank

Diplomacia World Food Programme

Diplomacia World Health Organization (WHO)

Diplomacia World Intellectual Property Organization

Diplomacia World Meteorological Organization

Diplomacia World Tourism Organization

Diplomacia WTO

Educação academia

Educação academic

Educação college

Educação curriculum

Educação education

Educação faculty

Educação graduate

Educação Harvard

Educação higher education

Educação humanities

Educação Instituto Federal

Educação MIT

Educação Princeton

Educação professors

Educação scholarship

Educação school

Educação Stamford

Educação student

Educação undergraduate

Educação Universidade Federal

Educação university

Energia blackouts

Energia brownouts

Energia Cemig

Energia Copel

Energia CPFL

Energia disruptions

Energia EDP

Energia electric

Energia electric corporation

Energia electric power

Energia electric utility

Energia electrical

Energia electrical power

Energia electricity

Energia electricity distribution

Energia ENEL

Energia	Energisa
Energia	energy
Energia	energy sector
Energia	hydro plant
Energia	Itaipu
Energia	Neoenergia
Energia	outage
Energia	power grid
Energia	power outages
Energia	renewable
Energia	shortages
Energia	solarpower
Energia	surge
Alimentação	agribusiness
Alimentação	Ambev
Alimentação	aquaculture
Alimentação	BASF
Alimentação	Bayer
Alimentação	biodiversity
Alimentação	Bunge
Alimentação	Cargill
Alimentação	Coamo
Alimentação	Cocamar
Alimentação	crop
Alimentação	cultivation
Alimentação	dairy
Alimentação	DuPont
Alimentação	Embrapa
Alimentação	fisheries
Alimentação	food crops
Alimentação	forestry
Alimentação	horticulture
Alimentação	husbandry
Alimentação	iFood
Alimentação	JBS
Alimentação	live stock
Alimentação	livestock
Alimentação	Maggi
Alimentação	Monsanto
Alimentação	Piracanjuba
Alimentação	Rappi
Alimentação	Syngenta
Governo	citizen
Governo	constitution
Governo	democracy
Governo	dictator
Governo	executive branch
Governo	executive order
Governo agencies	government
Governo agency	government
Governo departments	government
Governo entities	government
Governo institutions	government
Governo interests	government
Governo	government office
Governo official	government
Governo target	government
Governo agency	intelligence
Governo	judicial
Governo	jurisdiction
Governo	law enforcement
Governo	legislative
Governo	ministry
Governo	municipal
Governo	municipality
Governo	municipio
Governo	political figure
Governo	prime minister
Governo	provincia
Governo	secretaria
Governo	security actors
Governo	Senate
Governo	the president
Saúde	biomedical
Saúde	Capemisa
Saúde	clinic
Saúde	Corona
Saúde	Covid
Saúde	Covid-19

Saúde	doctor
Saúde	exams
Saúde	Golden Cross
Saúde	health
Saúde	health care
Saúde	healthcare
Saúde	hospital
Saúde	Johns Hopkins
Saúde	Mapfre
Saúde	medical
Saúde	medical records
Saúde	medication
Saúde	medicine
Saúde	nursing
Saúde	oncology
Saúde	Outbreak
Saúde	patient
Saúde	pediatric
Saúde	pharmaceutical
Saúde	physician
Saúde	Santa Casa
Saúde	surgical
Saúde	therapy
Saúde	treatment
Saúde	Unimed
Turismo	accommodation
Turismo	accorhotels
Turismo	agoda
Turismo	airbnb
Turismo	aman resorts
Turismo	apa group
Turismo	ascott
Turismo	avari
Turismo	avid hotel
Turismo	banyan tree
Turismo	barriere
Turismo	belmond
Turismo	best western
Turismo	blackstone
Turismo	booking
Turismo	booking.com
Turismo	BTG Homeinn
Turismo	candlewood
Turismo	Centara
Turismo	China Lodging
Turismo	Choice Hotels
Turismo	crowne plaza
Turismo	dalata
Turismo	dorchester
Turismo	drury
Turismo	dusti thani
Turismo	elite hotel
Turismo	expedia
Turismo	extended stay
Turismo	First Hotels
Turismo	formule 1
Turismo	four seasons
Turismo	general hotel
Turismo	greentree
Turismo	hilton
Turismo	holiday inn
Turismo	holiday inn express
Turismo	hoshino
Turismo	hospitality
Turismo	hotel
Turismo	hotel indigo
Turismo	hotels.com
Turismo	hualuxe
Turismo	Huazhu Hotels
Turismo	hyatt
Turismo	indian hotels
Turismo	intercontinental hotel
Turismo	jinjian international
Turismo	Jumeirah
Turismo	Kempinski
Turismo	kimpton
Turismo	Langham
Turismo	ligula
Turismo	lodging
Turismo	Loews Hotels
Turismo	lotte
Turismo	louvre hotels

Turismo	magnuson	Turismo	shillo inn	Indústria	textile
Turismo	marriott	Turismo	soneva	Indústria	Usiminas
Turismo	melia	Turismo	starwood	Indústria	Votorantim
Turismo	motel	Turismo	tokyu hotel	Mídia	broadsheet
Turismo	nh hotel	Turismo	tourism	Mídia	columnist
Turismo	nordic choice	Turismo	tourist	Mídia	commentator
Turismo	novo hotel	Turismo	toyoko	Mídia	correspondent
Turismo	oberoi	Turismo	travel	Mídia	critic
Turismo	okura	Turismo	travelocity	Mídia	editorial
Turismo	omni	Turismo	travelodge	Mídia	headlines
Turismo	oyo	Turismo	treebo	Mídia	investigative
Turismo	pan pacific	Turismo	vacation	Mídia	journalism
Turismo	premier inn	Turismo	voco	Mídia	journalist
Turismo	prince hotel	Turismo	warwick hotel	Mídia	media companies
Turismo	principal hotel	Turismo	westgate	Mídia	media organizations
Turismo	radisson	Turismo	wyndham	Mídia	media outlets
Turismo	red lion	Indústria	Alunorte	Mídia	national media
Turismo	red roof	Indústria	Bosch	Mídia	news organization
Turismo	regent hotel	Indústria	Braskem	Mídia	newspaper
Turismo	ritz carlton	Indústria	factory	Mídia	public relations
Turismo	riu hotel	Indústria	Gerdau	Mídia	publishing
Turismo	rocco forte	Indústria	heavy industry	Mídia	reporter
Turismo	room_number	Indústria	heavyindustry	Mídia	Sony
Turismo	rosewood	Indústria	industrial	Mídia	tabloid
Turismo	scandic hotel	Indústria	Klabin	Militar	armed
Turismo	shahpura	Indústria	machinery	Militar	artillery
Turismo	shangri-la hotel	Indústria	manufacture	Militar	battalion
Turismo	sheraton	Indústria	steel	Militar	combat

Militar	corps
Militar	defence
Militar	defense
Militar	defense contractor
Militar	defense force
Militar	defense industrial base
Militar	defense industries
Militar	defense industry
Militar	defense supply chain
Militar	infantry
Militar	marines
Militar	military
Militar	military entities
Militar	military institutions
Militar	military officials
Militar	military target
Militar	nato
Militar	squadron
Militar	troop
Militar	weaponry
Mineração	alcoa
Mineração	Anglo American plc
Mineração	BHP Billiton
Mineração	China Coal Energy
Mineração	China Shenhua Energy
Mineração	Coal India
Mineração	digging
Mineração	diging
Mineração	enerald
Mineração	excavate
Mineração	Glencore
Mineração	mineral
Mineração	quarry
Mineração	Rio Tinto
Mineração	Shaanxi Coal
Mineração	smelting
Mineração	trenching
Mineração	vale do rio doce
Mineração	vale sa
Mineração	Vattenfal
Mineração	Yanzhou Coal
Mineração	Zijin Mining
Pesquisa e Desenvolvimento	cryptography
Pesquisa e Desenvolvimento	futuristic
Pesquisa e Desenvolvimento	high tech
Pesquisa e Desenvolvimento	high-tech
Pesquisa e Desenvolvimento	intelectual property
Pesquisa e Desenvolvimento	propulsion
Pesquisa e Desenvolvimento	prototype
Pesquisa e Desenvolvimento	quantum computing
Pesquisa e Desenvolvimento	quantum research
Pesquisa e Desenvolvimento	research & development
Pesquisa e Desenvolvimento	research and development
Pesquisa e Desenvolvimento	research lab
Pesquisa e Desenvolvimento	scientific research
Pesquisa e Desenvolvimento	technological
Pesquisa e Desenvolvimento	think tanks
Varejo	Atacadão
Varejo	Bompreço
Varejo	carrefour
Varejo	Casas Bahia
Varejo	costco
Varejo	department store
Varejo	grocery
Varejo	Maxxi
Varejo	Mercadorama
Varejo	merchandising
Varejo	Pão de Açúcar
Varejo	Ponto Frio
Varejo	retail
Varejo	RicardoEletro
Varejo	Sam's Club

Varejo	tesco
Varejo	walmart
Varejo	warehouse
Transporte	bus
Transporte	bus terminal
Transporte	cabify
Transporte	commuter
Transporte	highway
Transporte	highways
Transporte	Infraero
Transporte	intercity
Transporte	road
Transporte	streetcar
Transporte	Uber
Petróleo e Gas	aramco
Petróleo e Gas	Bharat Petroleum
Petróleo e Gas	british petroleum
Petróleo e Gas	Centrica
Petróleo e Gas	CEPSA
Petróleo e Gas	Chevron
Petróleo e Gas	China National Offshore Oil
Petróleo e Gas	China National Petroleum
Petróleo e Gas	ConocoPhillips
Petróleo e Gas	deepwater
Petróleo e Gas	Ecopetrol
Petróleo e Gas	Engie
Petróleo e Gas	Enterprise Products
Petróleo e Gas	Equinor
Petróleo e Gas	Exxon Mobil
Petróleo e Gas	fuel
Petróleo e Gas	gasoline
Petróleo e Gas	Gazprom
Petróleo e Gas	GS Caltex
Petróleo e Gas	Hellenic Petroleum
Petróleo e Gas	Hindustan Petroleum
Petróleo e Gas	hydrocarbon
Petróleo e Gas	Idemitsu Kosan
Petróleo e Gas	Indian Oil
Petróleo e Gas	JX Holdings
Petróleo e Gas	Kuwait Petroleum
Petróleo e Gas	Lukoil
Petróleo e Gas	Marathon Petroleum
Petróleo e Gas	MOL
Petróleo e Gas	Motor Oil Hellas
Petróleo e Gas	National Iranian Oil
Petróleo e Gas	nonrenewable
Petróleo e Gas	oil
Petróleo e Gas	oil & gas
Petróleo e Gas	oil and gas
Petróleo e Gas	oil companies
Petróleo e Gas	oil company
Petróleo e Gas	oil/gas
Petróleo e Gas	oil&gas
Petróleo e Gas	oilfield
Petróleo e Gas	oilwell
Petróleo e Gas	OMV Group
Petróleo e Gas	ONGC
Petróleo e Gas	opep
Petróleo e Gas	PDVSA
Petróleo e Gas	Pemex
Petróleo e Gas	Pertamina
Petróleo e Gas	petro
Petróleo e Gas	Petrobras
Petróleo e Gas	petrochemical
Petróleo e Gas	petroleum
Petróleo e Gas	petrolium
Petróleo e Gas	Petronas
Petróleo e Gas	Phillips 66
Petróleo e Gas	PKN Orlen
Petróleo e Gas	PTT
Petróleo e Gas	refinery
Petróleo e Gas	Reliance Industries
Petróleo e Gas	Repsol
Petróleo e Gas	Rosneft
Petróleo e Gas	Royal Dutch Shell
Petróleo e Gas	Saudi Aramco
Petróleo e Gas	Schlumberger
Petróleo e Gas	SOCAR

Petróleo e Gas	Sonatrach
Petróleo e Gas	Suncor Energy
Petróleo e Gas	Total SA
Petróleo e Gas	Valero Energy
Telecom	5g
Telecom	A1 Telekom
Telecom	Advanced Info Service
Telecom	América Móvil
Telecom	AT&T
Telecom	BCE
Telecom	Bharti Airtel
Telecom	Brasil Telecom
Telecom	BT Group
Telecom	Cable One
Telecom	CenturyLink
Telecom	Charter Communications
Telecom	China Communications Services
Telecom	China Telecom
Telecom	China Unicom
Telecom	Chunghwa Telecom
Telecom	Cincinnati Bell
Telecom	claro
Telecom	Comcast
Telecom	Cox Communications
Telecom	critical information infrastructures
Telecom	Crown Castle International
Telecom	Dataprev
Telecom	Deutsche Telekom
Telecom	digital infrastructure
Telecom	digital services
Telecom	Eir
Telecom	Etisalat
Telecom	Frontier Communications
Telecom	Granite Telecommunications
Telecom	GTT Communications
Telecom	IDT Corporation
Telecom	internet exchange point
Telecom	internet infrastructure
Telecom	Jio
Telecom	KDDI
Telecom	KPN
Telecom	KT Corporation
Telecom	LG Uplus
Telecom	Maxis Communications
Telecom	Mediacom
Telecom	MegaFon
Telecom	Millicom
Telecom	Mobile TeleSystems
Telecom	MTN Group
Telecom	Nippon Telegraph and Telephone
Telecom	Oi Telecom
Telecom	Ooredoo
Telecom	Optus
Telecom	Orange
Telecom	OTE
Telecom	PLDT
Telecom	Proximus
Telecom	RCS&RDS
Telecom	Rogers Communications
Telecom	satellite communication
Telecom	Saudi Telecom
Telecom	Serpro
Telecom	SingTel
Telecom	SK Telecom
Telecom	Softbank
Telecom	Sprint
Telecom	Swisscom
Telecom	Taiwan Mobile
Telecom	Tata Communications
Telecom	Telecom Argentina

Telecom	telecom company
Telecom	Telecom Italia
Telecom	telecom provider
Telecom	telecommunication provider
Telecom	Telefónica
Telecom	Telemar
Telecom	Telenor
Telecom	Telephone and Data Systems
Telecom	Telia Company
Telecom	Telkom Indonesia
Telecom	Telstra
Telecom	Telus
Telecom	Turk Telekom
Telecom	Turkcell
Telecom	United Internet
Telecom	Verizon Communications
Telecom	VimpelCom
Telecom	Virgin Media
Telecom	Vivendi
Telecom	Vivo
Telecom	Vocus Group
Telecom	Vodafone
Telecom	Vonage
Telecom	Windstream Holdings
Telecom	Zain
Telecom	Zayo Group
Automotivo	audi
Automotivo	automobile
Automotivo	automotive
Automotivo	BAIC
Automotivo	bmw
Automotivo	Changan
Automotivo	chevrolet
Automotivo	chrysler
Automotivo	citroen
Automotivo	Daimler
Automotivo	Dongfeng Motor
Automotivo	electric car
Automotivo	FCA
Automotivo	ford
Automotivo	Geely
Automotivo	General Motors
Automotivo	Groupe PSA
Automotivo	Honda
Automotivo	Hyundai
Automotivo	mazda
Automotivo	mitsubishi
Automotivo	motor
Automotivo	nissan
Automotivo	peugeot
Automotivo	renault
Automotivo	SAIC
Automotivo	smart car
Automotivo	subaru
Automotivo	suzuki
Automotivo	tesla
Automotivo	toyota
Automotivo	volkswagen
Transporte Ferroviário	freight
Transporte Ferroviário	locomotive
Transporte Ferroviário	railway
Transporte Ferroviário	terminus
Transporte Ferroviário	train
Transporte Ferroviário	train station
Transporte Ferroviário	tram
Transporte Ferroviário	tramway
Transporte Ferroviário	viaduct
Água	Aegea
Água	Cedae
Água	contaminated
Água	Copasa
Água	drain
Água	effluent
Água	groundwater
Água	irrigation
Água	landfill
Água	pond
Água	potable
Água	rainwater
Água	reservoir

Água	sabesp
Água	Saneago
Água	Sanepar
Água	sediment
Água	septic
Água	stormwater
Água	sump
Água	wastewater
Água	water dam
Água	water treatment
Esportes	athletic
Esportes	baseball
Esportes	basket
Esportes	basketball
Esportes	championship
Esportes	football
Esportes	gymnastics
Esportes	handball
Esportes	hockey
Esportes	lacrosse
Esportes	nba
Esportes	ncaa
Esportes	nfl
Esportes	olympic
Esportes	olympics
Esportes	pan-american
Esportes	rugby
Esportes	soccer
Esportes	softball
Esportes	tennis
Esportes	volleyball
Esportes	world cup
Esportes	wrestling
Eleição	ballot
Eleição	candidate
Eleição	caucus
Eleição	democratic
Eleição	democratic national committee
Eleição	democratic party
Eleição	elected
Eleição	election
Eleição	electoral
Eleição	polling
Eleição	polls
Eleição	primaries
Eleição	reelection
Eleição	referendum
Eleição	republican
Eleição	vote
Eleição	voting poll
Nuclear	atomic
Nuclear	beryllium
Nuclear	cesium
Nuclear	deuterium
Nuclear	fissile
Nuclear	fission
Nuclear	isotope
Nuclear	neutron
Nuclear	nuclar energy
Nuclear	nuclear
Nuclear	nuclear plant
Nuclear	nuclear power
Nuclear	nuclear reactor
Nuclear	plutonium
Nuclear	radioactive
Nuclear	radionuclides
Nuclear	reactor
Nuclear	thermonuclear
Nuclear	thorium
Nuclear	tritium
Nuclear	uranium
Nuclear	warhead
Nuclear	yellow cake
Criptomoedas	bitcoin
Criptomoedas	bitcoin-cash
Criptomoedas	bnktothefuture
Criptomoedas	btc
Criptomoedas	cashless
Criptomoedas	crypto trader
Criptomoedas	crypto wallet
Criptomoedas	cryptocurrency
Criptomoedas	cryptocurrency companies

Criptomoedas	cryptocurrency exchanges
Criptomoedas	dash
Criptomoedas	eth
Criptomoedas	ethereum
Criptomoedas	foxbit
Criptomoedas	keepkey
Criptomoedas	ledger
Criptomoedas	litecoin
Criptomoedas	mercado bitcoin
Criptomoedas	micropayments
Criptomoedas	monero
Criptomoedas	padlock
Criptomoedas	stash
Criptomoedas	trezor
Criptomoedas	wallet
Criptomoedas	xmr
Criptomoedas	zcash

Ataque Estatal	government-affiliated
Ataque Estatal	state-sponsored
Ataque Estatal	state sponsored
Ataque Estatal	nation-state
Ataque Estatal	state-directed
Ataque Estatal	state directed

Vitimas attacked

Vitimas number of attacks

Vitimas attacks per user

Vitimas targeted

Vitimas victim

Vitimas victims

Vitimas target

Vitimas targets

Campanhas	1.Php Group
Campanhas	Agent.Btz
Campanhas	Aided Frame Aided Direction
Campanhas	Anthem Hack
Campanhas	Anunak
Campanhas	APT1
Campanhas	APT12
Campanhas	APT17
Campanhas	APT2
Campanhas	APT28
Campanhas	APT29
Campanhas	APT3
Campanhas	APT30
Campanhas	APT Anunak
Campanhas	APT Banechant
Campanhas	APT Blue Termite
Campanhas	APT Case RUAG
Campanhas	APT Etso
Campanhas	APT Farm
Campanhas	APT Hellsing
Campanhas	APT Icefog
Campanhas	APT Inception
Campanhas	APT Naikon
Campanhas	APT Pacifier
Campanhas	APT ProjectSauron
Campanhas	APT Seinup
Campanhas	APT TOCS
Campanhas	APT Turla
Campanhas	Arachnophobia
Campanhas	Arid Viper
Campanhas	Armageddon
Campanhas	Asruex
Campanhas	Aurora
Campanhas	Axiom
Campanhas	Backdoor Cadelspy and Remexi
Campanhas	Banechant
Campanhas	BBSRAT
Campanhas	Beebus
Campanhas	Belling the BEAR
Campanhas	Bigboss and Sillygoose
Campanhas	BLACKCOFFEE
Campanhas	Blackenergy
Campanhas	BlackEnergy
Campanhas	Blackfly
Campanhas	BlackGear
Campanhas	Black Vine

Campanhas Black Vine Group
Campanhas Blockbuster
Campanhas Blue Termite
Campanhas Bookworm Trojan
Campanhas Buckeye
Campanhas Buckeye Group
Campanhas Bugdrop
Campanhas Butterfly
Campanhas Byebye Shell
Campanhas Cadelspy
Campanhas Carbanak
Campanhas Careto
Campanhas Case RUAG
Campanhas CC Blog Malware
Campanhas ChChes
Campanhas Chinastrats
Campanhas Clandestine Fox
Campanhas Clandestine Wolf
Campanhas Cleaver
Campanhas Cloud Atlas
Campanhas CloudyOmega
Campanhas C-Major
Campanhas Cmstar Downloader
Campanhas Comfoo
Campanhas Comment Crew
Campanhas Comment Group
Campanhas Comment Panda
Campanhas CopyKitten
Campanhas Cozy Bear
Campanhas Cozycar
Campanhas Cozyduke
Campanhas Crouching Tiger
Campanhas Crude Faux
Campanhas Dances of White Elephant
Campanhas Darkcomet
Campanhas DarkHotel
Campanhas DarkSeoul
Campanhas DeathClick
Campanhas Deception Project
Campanhas Deep Panda
Campanhas Deputydog
Campanhas Derusbi
Campanhas Desert Falcons
Campanhas Dino
Campanhas DNC Intrusion
Campanhas Double Tap
Campanhas Dragonfly
Campanhas DragonOK
Campanhas Dropping Elephant
Campanhas Dukes
Campanhas Duqu
Campanhas Duqu 2.0
Campanhas Duststorm
Campanhas Dusty Sky
Campanhas DynCalc
Campanhas Elderwood Project
Campanhas Electric Powder
Campanhas Elirks Variants
Campanhas Emissary Panda
Campanhas Emissary Trojan
Campanhas Energetic Bear
Campanhas Ephemeral Hydra
Campanhas Equation
Campanhas Equationdrug
Campanhas Equation Group
Campanhas Etso
Campanhas Etumbot
Campanhas Evil Bunny
Campanhas Fakem RAT
Campanhas Fancy Bear
Campanhas Farm
Campanhas Fin4
Campanhas FIN7
Campanhas FinFisher
Campanhas Flamer
Campanhas Flying Kitten
Campanhas Four Element Sword Engagement Group
Campanhas Gamaredon Group
Campanhas Gauss
Campanhas Gaza Cybergang Group

Campanhas Georbot
Campanhas Georbot Botnet
Campanhas Gh0st RAT
Campanhas Gholee
Campanhas Ghost Dragon
Campanhas Ghostnet
Campanhas GlassRAT
Campanhas Gothic Panda
Campanhas Grabit
Campanhas Greedywonk
Campanhas Grizzly Steppe
Campanhas Groundbait
Campanhas Group-3390
Campanhas Group5
Campanhas Group 72
Campanhas Group Nitro
Campanhas Group Wekby
Campanhas HackingTeam
Campanhas Hammertoss
Campanhas Hangover
Campanhas Havex Trojan
Campanhas Heartbeat
Campanhas Hellsing
Campanhas Hidden Dragon
Campanhas Hidden Lynx
Campanhas Hikit
Campanhas Hong Kong Attacks
Campanhas Hopscotch
Campanhas Hopscotch And Legspin
Campanhas Houdini
Campanhas Htran
Campanhas Hunting Libyan Scorpions
Campanhas Hunting The Shadows
Campanhas Hydraq
Campanhas Icefog
Campanhas IDF Phishing
Campanhas Iexpl0Re
Campanhas IHEATE
Campanhas Inception
Campanhas Inception Framework
Campanhas INOCNATION
Campanhas Iranian Threat Agent
Campanhas Iron Dome
Campanhas Irongate
Campanhas Iron Twilight
Campanhas Ixeshe
Campanhas Ke3chang
Campanhas KeyBoy
Campanhas Kimsuky
Campanhas KingSlayer
Campanhas Kittens
Campanhas Korean Maldoc
Campanhas Korplug
Campanhas Kraken
Campanhas KungFu
Campanhas Lazarus
Campanhas Legspin
Campanhas Linux Moose
Campanhas Lotusblossom
Campanhas Lotus Blossom
Campanhas Luckycat
Campanhas Lurid Downloader
Campanhas Mac A4
Campanhas Machete
Campanhas Madi Infostealers
Campanhas Magic Hound
Campanhas Manul
Campanhas Mask
Campanhas Maudi
Campanhas MBR Destruction
Campanhas menuPass
Campanhas Miniduke
Campanhas Mirage
Campanhas Mirage Campaign
Campanhas Moafee
Campanhas Modified Binaries Tor
Campanhas Mofang
Campanhas Molerats
Campanhas Monju Incident

Campanhas Moonlight
Campanhas Moonsoon
Campanhas Msnmm
Campanhas Msnmm Campaigns
Campanhas MSUpdater
Campanhas Msupdater Trojan
Campanhas Naikon
Campanhas Neodymium
Campanhas NetTraveler
Campanhas New MoonWind
Campanhas Night Dragon
Campanhas njRAT
Campanhas NSO Group
Campanhas Numbered Panda
Campanhas Oceanlotus
Campanhas Oil Tanker
Campanhas Operation Arachnophobia
Campanhas Operation Arid Viper
Campanhas Operation Armageddon
Campanhas Operation Aurora
Campanhas Operation Beebus
Campanhas Operation Blockbuster
Campanhas Operation Bugdrop
Campanhas Operation Clandestine Fox
Campanhas Operation Clandestine Wolf
Campanhas Operation Cleaver
Campanhas Operation CloudyOmega
Campanhas Operation C-Major
Campanhas Operation DeathClick
Campanhas Operation Deputydog
Campanhas Operation Double Tap
Campanhas Operation Duststorm
Campanhas Operation Electric Powder
Campanhas Operation Ephemeral Hydra
Campanhas Operation Greedywonk
Campanhas Operation Groundbait
Campanhas Operation Hangover
Campanhas Operation Ke3chang
Campanhas Operation Ke3Chang
Campanhas Operation Kimsuky
Campanhas Operation Lotus Blossom
Campanhas Operation Manul
Campanhas Operation Maudi
Campanhas Operation Oil Tanker
Campanhas Operation Poisoned Handover
Campanhas Operation Poisoned Helmand
Campanhas Operation Poisoned Hurricane
Campanhas Operation Potao Express
Campanhas Operation Quantum Entanglement
Campanhas Operation Russiandoll
Campanhas Operation Saffron Rose
Campanhas Operation Snowman
Campanhas Operation Stteam
Campanhas Operation Toohash
Campanhas Operation Tropic Trooper
Campanhas OrcaRAT
Campanhas Pacifier
Campanhas Packrat
Campanhas Patchwork
Campanhas Pawn Storm
Campanhas Penquin
Campanhas PinkPanther
Campanhas Pirpi
Campanhas Pitty Tiger

Campanhas Platinum
Campanhas Plugx
Campanhas Handover Poisoned
Campanhas Helmand Poisoned
Campanhas Hurricane Poisoned
Campanhas Poison Ivy
Campanhas Poseidon Group
Campanhas Potao Express
Campanhas Prince of Persia
Campanhas Camerashy Project
Campanhas Project Cobra
Campanhas ProjectSauron
Campanhas Promethium
Campanhas Neodymium Promethium and
Campanhas PupyRAT
Campanhas Putter Panda
Campanhas Entanglement Quantum
Campanhas Quedagh
Campanhas Rat In A Jar
Campanhas Red October
Campanhas Regin
Campanhas Regin Plataform
Campanhas Remexi
Campanhas Roaming Tiger
Campanhas Rocket Kitten
Campanhas Rotten Tomato
Campanhas Response RSA Incident
Campanhas RUAG
Campanhas Russiandoll
Campanhas SafeNet
Campanhas Saffron Rose
Campanhas Sakula
Campanhas Sakula Malware
Campanhas Sakula Reloaded
Campanhas Sandworm
Campanhas SBDH Toolkit
Campanhas Scanbox
Campanhas Scarab
Campanhas ScarCruft Group
Campanhas Scarlet Mimic
Campanhas Sednit
Campanhas Seinup
Campanhas Dagger Seven Pointed
Campanhas Cloud Shadows In The
Campanhas Shady RAT
Campanhas Shamoon
Campanhas Shell Crew
Campanhas Shiqiang Gang
Campanhas Elephants Shooting
Campanhas Sidewinder
Campanhas Siesta
Campanhas Sin Digoo Affair
Campanhas Skeleton Key
Campanhas Sk Hack
Campanhas Skywiper
Campanhas SMB Worm
Campanhas SMB Worm Tool
Campanhas Snake Campaign
Campanhas Trojan Sneakernet
Campanhas Snowman
Campanhas Sofacy
Campanhas Stealth Falcon
Campanhas StrongPity
Campanhas STRONTIUM
Campanhas Stteam
Campanhas Stuxnet
Campanhas Suckfly
Campanhas Campaign Sunshop
Campanhas Surtr
Campanhas Syrian Malware
Campanhas T9000
Campanhas Taidoor Trojan
Campanhas Teamspy Story
Campanhas Terminator RAT
Campanhas Terracotta VPN
Campanhas TG-0110
Campanhas TG-2889

Campanhas	TG-4127	Campanhas	Trochilus	Campanhas	WebMasters
Campanhas	Thamar Reservoir	Campanhas	Trochilus and New MoonWind RAT	Campanhas	Wekby
Campanhas 0110	Threat Group-	Campanhas	Tropic Trooper	Campanhas Mac A4	Whitepaper APT
Campanhas 2889	Threat Group	Campanhas	Tsar Team	Campanhas	Wicked Rose
Campanhas 4127	Threat Group-	Campanhas	Turla	Campanhas	Wild Neutron
Campanhas	Tibetan Attacks	Campanhas	UPS Team	Campanhas	Winnti
Campanhas	TOCS	Campanhas	Uroburos	Campanhas	Wiper Malware
Campanhas	Toohash	Campanhas	Vinself	Campanhas	WitchCoven
Campanhas and SLServer	Tracking UP007	Campanhas	Voho	Campanhas	Xslcmd Backdoor
Campanhas	Transparent Tribe	Campanhas	Voho Campaign	Campanhas	XtremeRat
Campanhas	Travnet	Campanhas	Volatile Cedar	Campanhas	Zombie Zero
		Campanhas	Waterbug	Campanhas	Zoxpng
		Campanhas	Waterbug Group	Campanhas	Zxshell

APPENDIX E - REFERENCED TECHNICAL REPORTS

‘Cloud Snooper’ Attack Bypasses Firewall Security Measures (2020). Source: SophosLabs. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.02.25_Cloud_Snooper/CloudSnooper_report.pdf

‘DMSniff’ POS Malware Actively Leveraged to Target Small-, Medium-Sized Businesses (2019). Source: Flashpoint. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.13.DMSniff_POS_Malware/DMSniff_POS_Malware.pdf

‘Heatstroke’ Campaign Uses Multistage Phishing Attack to Steal PayPal and Credit Card Information (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.29.Heatstroke_Campaign/Heatstroke%20Campaign%20Uses%20Multistage%20Phishing%20Attack%20to%20Steal%20PayPal%20and%20Credit%20Card%20Information.pdf

‘Operation Sharpshooter’ Targets Global Defense, Critical Infrastructure (2020). Source: Intel Security-McAfee. Link: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

"Green Spot" action - an attack that lasts for many years (2018). Source: Antiy Labs. Link: https://www.antiy.cn/research/notice&report/research_report/20180919.html

"Poisonous Needle" Action - 0day attack against "Russian Presidential Office" (2018). Source: 360 SkyEye System. Link: http://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982.html

“Bad Tidings” Phishing Campaign Impersonates Saudi Government Agencies and a Saudi Financial Institution (2019). Source: Anomali. Link: https://www.anomali.com/blog/bad-tidings-phishing-campaign-impersonates-saudi-government-agencies-and-a-saudi-financial-institution#When:19:11:00Z

“Cyber Conflict” Decoy Document Used In Real Cyber Conflict (2017). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html

“Funky malware format” found in Ocean Lotus sample (2019). Source: MalwareBytes. Link: https://blog.malwarebytes.com/threat-analysis/2019/04/funky-malware-format-found-in-ocean-lotus-sample/

“Lebanese Cedar” APT – Global Lebanese Espionage Campaign Leveraging Web Servers (2021). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/cedar/

“Sin”-ful SPIDERS: WIZARD SPIDER and LUNAR SPIDER Sharing the Same Web (2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/

“Tick” Group Continues Attacks (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/07/unit42-tick-group-continues-attacks/

(CN) OceanLotus new malware analysis (2018). Source: Tencent. Link: https://s.tencent.com/research/report/471.html

#9 Blitzanalysis: Embassy Of Greece Beijing - Compromise (2014). Source: PhysicalDrive. Link: https://app.box.com/s/j108s0yjga3w42lm7wifklqilr4l35ld

10 years of virtual dynamite: A high-level retrospective of ATM malware (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html

2018 Mid-Year Review (2018). Source: CrowdStrike. Link: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018OverwatchReport.pdf

2018 Winter Cyber Olympics: Code Similarities with Cyber Attacks in Pyeongchang (2018). Source: Intezer. Link: http://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/

2019 Mid-Year Observations From the Front Lines (2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/resources/reports/observations-from-the-front-lines-of-threat-hunting-2019/

2Q Report On Targeted Attack Campaigns (2013). Source: Trend Micro. Link: https://app.box.com/s/bwgb7uhh6p4bdkyvlw94dpq19tq0fvbv

360 capture of cyber spy groups targeting China for 8 years (2018). Source: 360 SkyEye System. Link: https://mp.weixin.qq.com/s/S-hiGFNC6WXGrkjytAVbpA

419 Evolution (2014). Source: Palo Alto Networks. Link: https://www.paloaltonetworks.com/resources/research/419evolution

A Call To Harm: New Malware Attacks Target The Syrian Opposition (2013). Source: Citizen Lab. Link: https://app.box.com/s/hydmfjuajj44kezw77k9nwj5qormpp9y

A close look at the advanced techniques used in a Malaysian-focused APT campaign (2020). Source: Elastic. Link: https://www.elastic.co/blog/advanced-techniques-used-in-malaysian-focused-apt-campaign

A Closer Look At Miniduke (2013). Source: BitDefender. Link: https://app.box.com/s/cfkwk5mocm6ckxmaiv8hfe73k2bl1u10

A Closer Look at North Korea's Internet (2017). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-north-koreas-internet/

A Deep Dive into Lokibot Infection Chain (2021). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2021/01/a-deep-dive-into-lokibot-infection-chain.html

A Deep Dive Into Patchwork APT Group (2021). Source: Cybie. Link: https://cybleinc.com/2021/01/20/a-deep-dive-into-patchwork-apt-group/

A Detailed Timeline of a Chinese APT Espionage Attack Targeting South Eastern Asian Government Institutions (2020). Source: BitDefender. Link: https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

A dive into APT34 (aka OilRig, aka Cobalt Gypsy) "TwoFace" webshell (2019). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/a-dive-into-apt34-aka-oilrig-aka-cobalt-gypsy-twoface-webshell/

A dive into MuddyWater APT targeting Middle-East (2017). Source: REAQTA. Link: https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/

A dive into Turla PowerShell usage (2019). Source: ESET WeLiveSecurity. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.29.Turla_PowerShell/A%20dive%20into%20Turla%20PowerShell%20usage.pdf

A journey to Zebrocy land (2019). Source: ESET WeLiveSecurity. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.22.Zebrocy_Land/A%20journey%20to%20Zebrocy%20land.pdf

A look into APT36's (Transparent Tribe) tradecraft (2020). Source: Cyberstanc. Link: https://cyberstanc.com/blog/a-look-into-apt36-transparent-tribe/

A Look Into Fysbis: Sofacy's Linux Backdoor (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

A Nasty Trick: From Credential Theft Malware to Business Disruption (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

A new APT uses DLL side-loads to “KilllSomeOne” (2020). Source: SophosLabs. Link: https://news.sophos.com/en-us/2020/11/04/a-new-apt-uses-dll-side-loads-to-killlsomeone/

A new Equation Editor exploit goes commercial, as maldoc attacks using it spike (2019). Source: SophosLabs. Link: https://news.sophos.com/en-us/2019/07/18/a-new-equation-editor-exploit-goes-commercial-as-maldoc-attacks-using-it-spike/

A Peek into BRONZE UNION’s Toolbox (2019). Source: Dell Secureworks. Link: https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox

A Pretty Dope Story About Bears: Early Indicators of Continued World Anti-Doping Agency (WADA) Targeting (2017). Source: tr1adx. Link: https://www.tr1adx.net/intel/TIB-00004.html

A Quick Dip into MuddyWater's Recent Activity (2018). Source: Security 0wnage. Link: https://sec0wn.blogspot.tw/2018/03/a-quick-dip-into-muddywaters-recent.html

A review of the evolution of Andromeda over the years before we say goodbye (2018). Source: Virus Bulletin. Link: https://www.virusbulletin.com/virusbulletin/2018/02/review-evolution-andromeda-over-years-we-say-goodbye/

A Shortcut to Compromise: Cobalt Gang phishing campaign (2019). Source: Group-IB. Link: https://www.group-ib.com/blog/cobaltphishing

A study of Machete cyber espionage operations in Latin America (2019). Source: Virus Bulletin. Link: https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Valeros-etal.pdf

A Totally Tubular Treatise on TRITON and TriStation (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html

AA21-048A: AppleJeus: Analysis of North Korea’s Cryptocurrency Malware (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/alerts/aa21-048a

Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria (2019). Source: C4ADS. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/Above+Us+Only+Stars.pdf

Abusing cloud services to fly under the radar (2021). Source: NCCGroup. Link: https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/

ACAD/Medre.A 10000's of AutoCAD files leaked in suspected industrial espionage (2012). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2012/06/21/acadmedre-10000s-of-autocad-files-leaked-in-suspected-industrial-espionage/

ACAD/Medre.A Technical Analysis (2012). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2012/06/21/acadmedre-a-technical-analysis-2/

AcidBox: Rare Malware Repurposing Turla Group Exploit Targeted Russian Organizations (2020). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/acidbox-rare-malware/

Active Exploitation of Newly Patched ColdFusion Vulnerability (2018). Source: Volexity. Link: https://www.volexity.com/blog/2018/11/08/active-exploitation-of-newly-patched-coldfusion-vulnerability-cve-2018-15961/

Actors Still Exploiting SharePoint Vulnerability to Attack Middle East Government Organizations (2020). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/actors-still-exploiting-sharepoint-vulnerability/

Additional Insights on Shamoon2 (2017). Source: Arbor Networks. Link: https://app.box.com/s/dt59pijmmnxc3no13g55jbdr325fpnhs

admin@338 (2013). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

ADOBE FLASH ZERO-DAY LEVERAGED FOR TARGETED ATTACK IN MIDDLE EAST (2018). Source: Iceberg. Link: https://www.icebrg.io/blog/adobe-flash-zero-day-targeted-attack

Advanced Mobile Malware Campaign in India uses Malicious MDM (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

Advanced Persistent Threat Actors Targeting U.S. Think Tanks (2020). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/alerts/aa20-336a

Advanced Persistent Threats: A Decade In Review (2011). Source: Command Five. Link: https://app.box.com/s/tl13bx0ek04liinz7btbc3f47jpvpbxj

Advisory for Malicious Targeted Attack Campaign (2017). Source: NIC-CERT. Link: https://nic-cert.nic.in/NIC_CERT/pdf/13-Advisory%20for%20Malicious%20Targeted%20Attack%20Campaign.pdf

Advisory: APT29 targets COVID-19 vaccine development (2020). Source: National Cyber Security Centre. Link: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

Adwind - a cross plataform RAT (2016). Source: Kaspersky Lab. Link: https://securelist.com/securelist/files/2016/02/KL_AdwindPublicReport_2016.pdf

Aggah Campaign: Bit.ly, BlogSpot, and Pastebin Used for C2 in Large Scale Campaign (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/

Aided Frame, Aided Direction (Because It's A Redirect) (2014). Source: FireEye. Link: https://app.box.com/s/c0vmfv396d3lej8g37mxbhjgbjen1m21

Alert (AA21-042A) (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/alerts/aa21-042a

Alert (Ta14-353A) Targeted Destructive Malware (2014). Source: US-CERT. Link: https://app.box.com/s/lldbbamo2r9d59jf9ztlif93d6o2p2uw

Allanite (2019). Source: Dragos. Link: https://dragos.com/resource/allanite/

Alleged Apt Intrusion Set: 1.Php Group (2011). Source: Zscaler. Link: https://app.box.com/s/rqv5wirqhfc3zht1p2kouk8i0ymnmr92

American hackers helped UAE spy on Al Jazeera chairman, BBC host (2019). Source: Reuters. Link: https://www.reuters.com/investigates/special-report/usa-raven-media/

Amnesty International Among Targets of NSO-powered Campaign (2018). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

An Analysis of KONNI APT's Attack Activity Disguised as a Korean Android Chat Application (2019). Source: 360 SkyEye System. Link: https://ti.qianxin.com/blog/articles/analysis-of-konni-apt-organization-attack-activities-disguised-as-korean-android-chat-application/

An Analysis Of Regin's Hopscotch And Legspin (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/yezsypczjmt973gpcqfqh5yf9po4zr3c

An APT Blueprint: Gaining New Visibility into Financial Threats (2019). Source: BitDefender. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf

An In-Depth Look at How Pawn Storm’s Java Zero-Day Was Used (2015). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/an-in-depth-look-at-how-pawn-storms-java-zero-day-was-used/

An intrusion campaign targeting Chinese language news sites (2017). Source: Citizen Lab. Link: https://app.box.com/s/kbror3u3vgqkn7u167u34fg41dtxwfpy

An Iranian Cyber-Attack Campaign Against Targets In The Middle East (2015). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/mf27ius5sdlorh8nl4h4fr643g2i9orb

An Updated ServHelper Tunnel Variant (2019). Source: Binary Defense. Link: https://www.binarydefense.com/an-updated-servhelper-tunnel-variant/

Analysis and Disclosure of the US Central Intelligence Agency Network Weapons Database (2019). Source: 360 SkyEye System. Link: https://ti.qianxin.com/blog/articles/network-weapons-of-cia/

Analysis Of A Plugx Variant (Plugx Version 7.0) (2013). Source: Computer Incident Response Center Luxembourg (CIRCL). Link: https://app.box.com/s/90qhti3jwdmthbz7fd1l49n9y2cp8ffq

Analysis Of A Recent Plugx Variant - P2P Plugx (2015). Source: JPCERT. Link: https://app.box.com/s/outg1oalwwfvd86eopmgv2pskekzmr4t

Analysis Of A Stage 3 Miniduke Sample (2013). Source: Computer Incident Response Center Luxembourg (CIRCL). Link: https://app.box.com/s/c95me2uocwoothfnapxrcjwfmynue4ri

Analysis of APT attack on 'Operation Onezero' conducted as a document on Panmunjom Declaration (2018). Source: ESTsecurity. Link: https://blog.alyac.co.kr/1710

Analysis Of Chinese Mitm On Google (2014). Source: NETRESEC. Link: https://app.box.com/s/rpig9c10mj8wdri1ulftjxbabm543mxa

Analysis of Clop Ransomware suspiciously related to the Recent Incident (2020). Source: S2W Lab. Link: https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-English-088056baf01242409a6e9f844f0c5f2e

Analysis of Code4HK (2014). Source: malware.lu. Link: https://malware.lu/articles/2014/09/29/analysis-of-code4hk.html

Analysis of CVE-2018-8174 VBScript 0day and APT actor related to Office targeted attack (2018). Source: 360 SkyEye System. Link: http://blogs.360.cn/blog/cve-2018-8174-en/

Analysis of MuddyC3, a New Weapon Used by MuddyWater (2019). Source: Qianxin. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.06.25.MuddyC3/MuddyC3.pdf

Analysis Of Project Cobra (2015). Source: G Data Software. Link: https://app.box.com/s/vuxbnmnptzygbuxkqbaq90vgm35hpcdv

Analysis of Safety System Targeted Malware (2017). Source: Dragos. Link: https://dragos.com/blog/trisis

Analysis Of Targeted Attack Against Pakistan By Exploiting InPage Vulnerability And Related APT Groups (2018). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/

Analysis of the APT Campaign 'Smoke Screen' targeting to Korea and US (2019). Source: ESTsecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/2_5224432166275908829.pdf

Analysis of the Attacks of Domestic Universities and Colleges in the Early Stage of Suspected "Sea Lotus" Organization (2018). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/oceanlotus-targets-chinese-university/

Analysis of the CVE-2018-8373 0day vulnerability attack related to the Darkhotel gang (2018). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/analyzing-attack-of-cve-2018-8373-and-darkhotel/

Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case (2016). Source: SANS Institute. Link: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Analysis of the FinFisher Lawful Interception Malware (2012). Source: Rapid7. Link: https://community.rapid7.com/community/infosec/blog/2012/08/08/finfisher

Analysis On APT-To-Be Attack That Focusing On China's Government Agency (2015). Source: Antiy Labs. Link: https://app.box.com/s/zeacvn2ae7aunrlsfjm8kbt4nbf6yn0z

Analyzing a Molerats spear phishing campaing (2019). Source: S2 Grupo. Link: https://lab52.io/blog/analyzing-a-molerats-spear-phising-campaing/

Analyzing a New Variant of BlackEnergy 3 Likely Insider-Based Execution (2016). Source: SentinelOne. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/BlackEnergy3_WP_012716_1c.pdf

Analyzing Digital Quartermasters in Asia – Do Chinese and Indian APTs Have a Shared Supply Chain? (2019). Source: Anomali. Link: https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain

Analyzing new malware of China Panda hacker group used to attack supply chain against Vietnam Government Certification Authority (2020). Source: VinCSS. Link: https://blog.vincss.net/2020/12/re018-1-analyzing-new-malware-of-china-panda-hacker-group-used-to-attack-supply-chain-against-vietnam-government-certification-authority.html?m=1

Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

Analyzing the TRITON industrial malware (2018). Source: Midnight Blue Labs. Link: https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

Anatomy of a Gh0st RAT (2012). Source: Intel Security-McAfee. Link: http://www.mcafee.com/us/resources/white-papers/foundstone/wp-know-your-digital-enemy.pdf

Anatomy Of The Attack: Zombie Zero (2014). Source: TrapX Security. Link: https://app.box.com/s/r95pew4gb5gi1qw40l6s0jbzw5lfwqbm

Anchor Panda (2013). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/whois-anchor-panda/

Anchor Project: The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT (2019). Source: SentinelOne. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.12.10_TrickBot_Planeswalker/sentinel-one-sentine-6.pdf

And then there were 6: A story of cyberspionage incident response by DART that uncovered five additional threat actors in one environment (2020). Source: Microsoft. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/And_then_there_were_6.pdf

Andariel Group - KR (2018). Source: AhnLab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/Andariel_Threat_Group.pdf

Andariel Group Trend Report (2018). Source: AhnLab. Link: http://download.ahnlab.com/kr/site/library/%5BReport%5DAndariel_Threat_Group.pdf

Andromeda under the microscope (2016). Source: Avast. Link: https://blog.avast.com/andromeda-under-the-microscope

Animals in the APT Farm (2016). Source: Kaspersky Lab. Link: http://securelist.com/blog/research/69114/animals-in-the-apt-farm/

Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/

Anunak: Apt Against Financial Institutions (2014). Source: Group-IB. Link: https://app.box.com/s/exmsfcvad1sjqtmvtzbiil9k52js62ir

Appendix B: Moonlight Maze Technical Report (2017). Source: Kaspersky Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Penquins_Moonlit_Maze_AppendixB.pdf

APT 12 (2014). Source: Trend Micro. Link: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

APT 18 (2014). Source: Dell Secureworks. Link: https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems

APT 3 (2015). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

APT 40 in Malaysia (2020). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/apt-40-in-malaysia-61ed9c9642e9

APT attack against the reporters of the Unification Ministry, Operation Cobra Venom (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2066

APT Attack In the Middle East: The Big Bang (2018). Source: Check Point. Link: https://research.checkpoint.com/apt-attack-middle-east-big-bang/

APT attacks aimed at security, diplomatic and unification related fields, Operation Black Limousine (2018). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2004

APT Case RUAG Technical Report (2016). Source: GovCERT.ch. Link: https://app.box.com/s/rabwkf8pmoxndj0n0nlktvc2eti2381k

APT Group (APT-C-01) New Utilization Vulnerability Sample Analysis and Association Mining (2018). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/analysis-of-apt-c-01/

APT Group Planted Backdoors Targeting High Profile Networks in Central Asia (2020). Source: Avast. Link: https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/

APT Group Sends Spear Phishing Emails to Indian Government Officials (2016). Source: FireEye. Link: https://app.box.com/s/s0yj8qsfhkf81hpyrtdmhpv3lrmd5p5n

APT Group Targeting Governmental Agencies in East Asia (2020). Source: Avast. Link: https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/

APT Group UPS Targets US Government with Hacking Team Flash Exploit (2015). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2015/07/apt-group-ups-targets-us-government-with-hacking-team-flash-exploit/

APT Group Wekby Leveraging Adobe Flash Exploit CVE-2015-5119 (2015). Source: Volexity. Link: http://www.volexity.com/blog/?p=158

APT on Taiwan - insight into advances of adversary TTPs (2015). Source: Dragon Threat Labs. Link: http://blog.dragonthreatlabs.com/2015/07/dtl-06282015-01-apt-on-taiwan-insight.html

Apt Reports And Opsec Evolution, Or: These Are Not The Apt Reports You Are Looking For (2016). Source: Cymmetria. Link: https://app.box.com/s/6kow9e7d5ogd1qxskl5krels702fwyon

APT Sidewinder changes theirs TTPs to install their backdoor (2018). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/apt-sidewinder-changes-theirs-ttps-to-install-their-backdoor-f92604a2739

APT Sidewinder complicates theirs malwares (2018). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/apt-sidewinder-complicates-theirs-malwares-4e15683e7e26

APT Targeting Energy and Other Critical Infrastructure Sectors (2017). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA17-293A

APT Targets Financial Analysts with CVE-2017-0199 (2017). Source: Proofpoint. Link: https://app.box.com/s/thla4hs15c78z638bw7g5fmjlixmex9b

APT Trends Report Q2 2018 (2018). Source: Kaspersky Lab. Link: https://securelist.com/apt-trends-report-q2-2018/86487/

APT trends report Q3 2019 (2019). Source: Kaspersky Lab. Link: https://securelist.com/apt-trends-report-q3-2019/94530/?utm_source=twitter&utm_medium=social&utm_campaign=uk_securelist_db0077&utm_content=sm-post&utm_term=uk_twitter__db0077_sm-post_social_securelist

APT Turla (2017). Source: National Cyber Security Centre. Link: https://www.ncsc.gov.uk/alerts/turla-group-malware

APT-C-09 Reappeared as Conflict Intensified Between India and Pakistan (2019). Source: 360 SkyEye System. Link: https://ti.qianxin.com/blog/articles/apt-c-09-reappeared-as-conflict-intensified-between-india-and-pakistan/

APT-C-23 middle East (2020). Source: 360 SkyEye System. Link: https://blogs.360.cn/post/APT-C-23_target_at_Middle_East.html

APT-C-27 (Goldmouse): Suspected Target Attack against the Middle East with WinRAR Exploit (2019). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/apt-c-27-(goldmouse):-suspected-target-attack-against-the-middle-east-with-winrar-exploit-en/

APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations (2019). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

APT-C-37 campaign in the Middle East (2019). Source: CyberThreatIntel. Link: https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Unknown/APT-C-37/26-08-19/APT-C-37%20analysis.md#APT

APT-C-38 (2019). Source: 360 SkyEye System. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.27.APT-C-38/APT-C-38_cn.pdf

APT-C-43 steals Venezuelan military secrets to provide intelligence support for the reactionaries — HpReact campaign (2020). Source: 360 SkyEye System. Link: https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

APT-C-44 NAFox (2020). Source: 360 SkyEye System. Link: https://blogs.360.cn/post/APT-C-44.html

APT-C-47 ClickOnce Operation (2020). Source: Qianxin. Link: https://mp.weixin.qq.com/s/h_MUJfa3QGM9SqT_kzcdHQ

APT-C-23 group evolves its Android spyware (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

Apt1 Exposing One Of China's Cyber Espionage Units (2013). Source: Mandiant. Link: https://app.box.com/s/t8w9gavaci6jye519zp13tjdicnd7xzu

Apt1: Technical Backstage (2013). Source: malware.lu. Link: https://app.box.com/s/x2jgr4j1bgfas2h2b4h09mam9nn4qwu3

APT1's GLASSES: Watching a Human Rights Organization (2013). Source: Citizen Lab. Link: https://citizenlab.org/wp-content/uploads/2009/10/APT1s-GLASSES-Watching-a-Human-Rights-Organization_websitepdf.pdf

APT10 - Operation Cloud Hopper (2017). Source: BAE Systems Detica. Link: https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html

APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign (2019). Source: Recorded Future. Link: https://www.recordedfuture.com/apt10-cyberespionage-campaign/

APT10 Targeting Japanese Corporations Using Updated TTPs (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

APT10 Threat Analysis Report (2020). Source: Recorded Future. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/apt10.pdf

APT10 was managed by the Tianjin bureau of the Chinese Ministry of State Security (2018). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/

APT15 is alive and strong: An analysis of RoyalCli and RoyalDNS (2018). Source: NCCGroup. Link: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

APT17 is run by the Jinan bureau of the Chinese Ministry of State Security (2019). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/

"APT27 ZxShell RootKit module updates

(2020). Source: S2 Grupo. Link: https://lab52.io/blog/apt27-rootkit-updates/"

APT28 / Fancy Bear still targeting military institutions (2018). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/apt28-targeting-military-institutions/

APT28 / Sofacy – SedUploader under the Christmas tree (2018). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/apt28-sofacy-seduploader-under-the-christmas-tree/

APT28 Targets Hospitality Sector, Presents Threat to Travelers (2017). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

APT28: A Window Into Russia's Cyber Espionage Operations (2014). Source: FireEye. Link: https://app.box.com/s/2e7s0j3cuuswoplyvaqdz4kdudvvr7x7

APT28: At the center of the storm. Russia strategically evolves its cyber operations (2018). Source: CrowdStrike. Link: https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html

APT29 Domain Fronting With TOR (2017). Source: FireEye. Link: https://app.box.com/s/8ytb4nym7whlldfvsaivnmsut9ole32h

APT29 targets COVID-19 vaccine development (2020). Source: National Cyber Security Centre. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

APT29 threat group seems to be back targeting US public / gov /defense sector (2018). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/apt29-cozybear-is-back-targeting-us-public-defense-sector/

APT3 Adversary Emulation Plan (2017). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/APT3_Adversary_Emulation_Plan.pdf

APT3 is Boyusec, a Chinese Intelligence Contractor (2017). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/

APT30 And The Mechanics Of A Long-Running Cyber Espionage Operation (2015). Source: FireEye. Link: https://app.box.com/s/5jjomo7k001inllirt5lj83lu92ath7d

APT32 / OceanLotus on ASEAN Affairs (2019). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/apt32-oceanlotus-on-asean-affairs/

APT32 Continues ASEAN Targeting (2018). Source: RSA Security. Link: https://community.rsa.com/community/products/netwitness/blog/2018/01/30/apt32-continues-asean-targeting

APT33 Targets Aerospace and Energy Sectors (2017). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

APT34 (AKA OILRIG, AKA HELIX KITTEN) ATTACKS LEBANON GOVERNMENT ENTITIES WITH MAILDROPPER IMPLANTS (2020). Source: Telsy. Link: https://blog.telsy.com/apt34-aka-oilrig-attacks-lebanon-government-entities-with-maildropper-implant/

APT34: NEW LEAKED TOOL NAMED JASON IS AVAILABLE FOR THE MASS (2019). Source: Telsy. Link: https://blog.telsy.com/apt34-new-leaked-tool-named-jason-is-available-for-the-mass/

APT36 jumps on the coronavirus bandwagon, delivers Crimson RAT (2020). Source: Binary Defense. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.15_APT36_Crimson_RAT/APT36%20jumps%20on%20the%20coronavirus%20bandwagon%2C%20delivers%20Crimson%20RAT%20_%20Malwarebytes%20Labs.pdf

APT37 (REAPER) - The Overlooked North Korean Actor (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html

APT38 Un-usual Suspects (2018). Source: FireEye. Link: https://content.fireeye.com/apt/rpt-apt38

APT38: Details on New North Korean Regime-Backed Threat Group (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html

APT39: An Iranian Cyber Espionage Group Focused on Personal Information (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

APT40 is run by the Hainan department of the Chinese Ministry of State Security (2019). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/

APT40: Examining a China-Nexus Espionage Actor (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

APT41: A Dual Espionage and Cyber Crime Operation (2019). Source: FireEye. Link: https://content.fireeye.com/apt-41/rpt-apt41/

APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure (2020). Source: MalwareBytes. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/200407-MWB-COVID-White-Paper_Final.pdf

ArmaRat: Espionage for Iranian users for two years (2018). Source: 360 SkyEye System. Link: http://blogs.360.cn/post/analysis_of_ArmaRat.html

Arrests Put New Focus on CARBON SPIDER Adversary Group (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

Asruex Backdoor Variant Infects Word Documents and PDFs Through Old MS Office and Adobe Vulnerabilities (2019). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/asruex-backdoor-variant-infects-word-documents-and-pdfs-through-old-ms-office-and-adobe-vulnerabilities/

Asruex: Malware Infecting through Shortcut Files (2016). Source: JPCERT. Link: https://app.box.com/s/mxvgs6dx4kixjv5s29yc6m81kii8opbw

AT commands, Tor-based communications: meet ATTOR, A fantasy creature and also a Spy platform (2020). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/ESET_Attor_102019.pdf

At the Center of the Storm: Russia's APT28 Strategically Evolves its Cyber Operations (2017). Source: FireEye. Link: https://www2.fireeye.com/WEB-2017-RPT-APT28.html

ATMitch: New Evidence Spotted In The Wild (2019). Source: Yoroi. Link: https://blog.yoroi.company/research/atmitch-new-evidence-spotted-in-the-wild/

Attack Campaign on the Government of Thailand Delivers Bookworm Trojan (2015). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2015/11/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/

Attack Delivers '9002' Trojan Through Google Drive (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/07/unit-42-attack-delivers-9002-trojan-through-google-drive/

Attack on a German steel plant (2014). Source: Anomali. Link: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3

Attack On French Diplomat Linked To Operation Lotus Blossom (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/cbxo6pdyf8xua2eg5dn44ni47wbs0le0

Attack on the Syrian Air Force (2007). Source: AGARI. Link: https://web.archive.org/web/20101007181725/http://www.haaretz.com/news/report-iran-worried-over-syrian-air-defense-failure-in-iaf-strike-1.230487

Attackers Deploy New ICS Attack Framework (2017). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Attackers Deploy New ICS Attack Framework TRITON and Cause Operational Disruption to Critical Infrastructure (2017). Source: FireEye. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Fireeye_ICS-Attack-Framework-TRITON.pdf

Attackers Increasingly Targeting Oracle WebLogic Server Vulnerability for XMRig and Ransomware (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/attackers-increasingly-targeting-oracle-weblogic-server-vulnerability-for-xmrig-and-ransomware/

Attacking the Heart of the German Industry (2019). Source: Bayerische Rundfunk. Link: https://web.br.de/interaktiv/winnti/english/

Attacks Against Israeli & Palestinian Interests (2015). Source: PWC. Link: https://app.box.com/s/aaai5lu6q5wy0wp25m34oh383wmtg54m

Attacks Of The Lazarus Cybercriminal Group Attended To Organizations In Russia (2019). Source: Secure Soft. Link: https://app.box.com/s/7vam6qq35nn1a7se265galj9i2tyzhwo

Attacks on SWIFT Banking System Benefit From Insider Knowledge (2016). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/attacks-swift-banking-system-benefit-insider-knowledge/

Attempted compromise of Australian and New Zealand government computers (2007). Source: Electronic Frontier Foundation. Link: https://wikileaks.org/gifiles/docs/35/355203_-os-china-australia-new-zealand-china-s-cyber-raid-on.html

Attempted compromise of the Dutch organization investigating the crash of flight MH17 (2015). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/

Attor, a spy platform with curious GSM fingerprinting (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform/

Attribution of Russian Cyber Activity Targeting COVID-19 Vaccine Development by Australia, Canada, the UK, and the U.S. (2020). Source: US-CERT. Link: https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/Attribution/Attribution+of+Russian+Cyber+Activity+Targeting+COVID-19+Vaccine+Development+by+Australia%2C+Canada%2C+the+UK%2C+and+the+U.S..pdf

Autumn Aperture: Threat Campaign Highlights New Evasion Technique using an Antiquated File Format (2019). Source: Prevailion. Link: https://blog.prevailion.com/2019/09/autumn-aperture-report.html

Avast tracks down Tempting Cedar Spyware (2018). Source: Avast. Link: https://blog.avast.com/avast-tracks-down-tempting-cedar-spyware

Ave_Maria Malware: there's more than meets the eye (2019). Source: REAQTA. Link: https://reaqta.com/2019/04/ave_maria-malware-part1/

Aveo Malware Family Targets Japanese Speaking Users (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/08/unit42-aveo-malware-family-targets-japanese-speaking-users/

AVIVORE – Hunting Global Aerospace through the Supply Chain (2019). Source: Context IS. Link: https://www.contextis.com/en/blog/avivore

AWS Shield Threat Landscape Report Q1 2020 (2020). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5420404162418443992.pdf

Babar: espionage software finally found and put under the microscope (2015). Source: G Data Software. Link: https://blog.gdatasoftware.com/blog/article/babar-espionage-software-finally-found-and-put-under-the-microscope.html

BabyShark Malware Part Two – Attacks Continue Using KimJongRAT and PCRat (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/

Bachosens: Highly-skilled petty cyber criminal with lofty ambitions targeting large organizations (2017). Source: Symantec. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Bachosens.pdf

"Back in BlackEnergy *: 2014 Targeted Attacks in Ukraine

and Poland (2014). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/"

Back to School: COBALT DICKENS Targets Universities (2018). Source: Dell Secureworks. Link: https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities

Backdoor as a Software Suite: How TinyLoader Distributes and Upgrades PoS Threats (2016). Source: Trend Micro. Link: http://documents.trendmicro.com/assets/tinypos-abaddonpos-ties-to-tinyloader.pdf

Backdoor.Winnti Attackers Have A Skeleton In Their Closet? (2015). Source: Symantec. Link: https://app.box.com/s/89pqnoimwdkrmyhxwqj5pp17jtjm4lmc

Backdoors are Forever Hacking Team and the Targeting of Dissent? (2012). Source: Citizen Lab. Link: https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

BadPatch (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/10/unit42-badpatch/

Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia (2017). Source: Bellingcat. Link: https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

Bahamut, Pursuing a Cyber Espionage Actor in the Middle East (2017). Source: Bellingcat. Link: https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/

Baldr vs The World: A SophosLabs report (2019). Source: SophosLabs. Link: https://news.sophos.com/en-us/2019/08/06/baldr-vs-the-world-a-sophoslabs-report/

Bandook: Signed & Delivered (2020). Source: Check Point. Link: https://research.checkpoint.com/2020/bandook-signed-delivered/

BasBanke: Trend-setting Brazilian banking Trojan (2019). Source: Kaspersky Lab. Link: https://securelist.com/basbanke-trend-setting-brazilian-banking-trojan/90365/

BayWorld event, Cyber Attack Against Foreign Trade Industry (2020). Source: 360 SkyEye System. Link: https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/

BBSRAT Attacks Targeting Russian Organizations Linked to Roaming Tiger (2015). Source: Palo Alto Networks. Link: https://app.box.com/s/noqd4tec6z6nfv8w4z48vzvwfo3goegl

Be2 Custom Plugins, Router Abuse, And Target Profiles (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/0aem5xn8owa5hpsjxuqbyloielln6oyh

Bear Hunting Season: Tracking APT28 (2016). Source: tr1adx. Link: https://app.box.com/s/py4k1124p7hqacfb6dlkghvsh5xte2zw

Bear Spotting Vol. 1: Russian Nation State Targeting of Government and Military Interests (2017). Source: tr1adx. Link: https://app.box.com/s/7q3rd2vov9uhkxmbpqax8vsdjafxnebm

Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations (2020). Source: Booz Allen Hamilton. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/bearing-witness-uncovering-the-logic-behind-russian-military-cyber-operations-2020.pdf

Bears in the Midst: Intrusion into the Democratic National Committee (2016). Source: CrowdStrike. Link: https://app.box.com/s/x5sz7dw4as54b1rif3mdtqwzzj2aek68

Behind the Scenes with OilRig (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/

Behind The Syrian Conflict's Digital Front Lines (2015). Source: FireEye. Link: https://app.box.com/s/qriikjn5436zpiyazh8ta7gbzbd04onf

Belling the BEAR: russia-hacks-bellingcat-mh17-investigation (2016). Source: ThreatConnect. Link: https://app.box.com/s/xpj87wwmxjkl3cykpyjbekaqhb3v4py6

Bestsellers in the Underground Economy: Measuring Malware Polularity by Forum (2019). Source: Recorded Future. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/2_5308045752075814088.pdf

Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns (2016). Source: Citizen Lab. Link: https://app.box.com/s/goyec2m2zwl5fi4sv3ayzwhudcfly1lv

Beyond fake news: an investigation into the murky world of fake campaigns (2016). Source: Amnesty International. Link: https://medium.com/amnesty-insights/beyond-fake-news-an-investigation-into-the-murky-world-of-fake-campaigns-f4af8118844b

Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware (2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

Bisonal Malware Used in Attacks Against Russia and South Korea (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/

"BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0

(2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/"

BITTER APT: Not So Sweet (2019). Source: Meltx0r. Link: https://meltx0r.github.io/tech/2019/09/06/bitter-apt-not-so-sweet.html

BITTER APT: Not So Sweet pt. 2 (2019). Source: Meltx0r. Link: https://meltx0r.github.io/tech/2019/09/09/bitter-apt-not-so-sweet-pt2.html

Bitter CHM (2020). Source: Qianxin. Link: https://mp.weixin.qq.com/s/9O4nZV-LNHuBy2ihg2XeIw

Bitter Sweet: Supporters of Mexico’s Soda Tax Targeted With NSO Exploit Links (2017). Source: Citizen Lab. Link: https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/

BITTER: A Targeted attack against Pakistan (2016). Source: Forcepoint. Link: https://app.box.com/s/iegu4jz7v3q0vcvgrkzrnq3w28q3pyne

BlackBerry Uncovers Massive Hack-For-Hire Group Targeting Governments, Businesses, Human Rights Groups and Influential Individuals (2020). Source: Cylance. Link:

https://www.blackberry.com/us/en/company/newsroom/press-releases/2020/blackberry-uncovers-massive-hack-for-hire-group-targeting-governments-businesses-human-rights-groups-and-influential-individuals

BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks (2014). Source: F-Secure. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2014/blackenergy_whitepaper.pdf

Blackenergy & Quedagh: The Convergence Of Crimeware And Apt Attacks (2014). Source: F-Secure. Link: https://app.box.com/s/ccj81xcg1xunuyjmnb3kt3ug77r16z7q

BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents (2016). Source: Kaspersky Lab. Link: https://app.box.com/s/igygz8ihex1hok5r1dp215ui0gz1ghwr

BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry (2016). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/uo31npu9sese34f1ppggmrug48x7rlqp

Blackenergy Cyber Threat – The History of Attacks on Critical Infrastructure of Ukraine (2016). Source: CyS Centrum. Link: https://cys-centrum.com/ru/news/black_energy_2_3

BlackEnergy DDoS Bot Analysis (2007). Source: Arbor Networks. Link: http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

BlackEnergy Version 2 Threat Analysis (2010). Source: Dell Secureworks. Link: https://www.secureworks.com/research/blackenergy2

BLACKGEAR Espionage Campaign Evolves, Adds Japan To Target List (2016). Source: Trend Micro. Link: https://app.box.com/s/ws5vsndqqi7s17ysrfa39260wqy2ktyt

BlackOasis APT and new targeted attacks leveraging zero-day exploit (2017). Source: Kaspersky Lab. Link: https://app.box.com/s/8ydblix231swgmjochzrvchwxcedis8z

BlackWater Malware Leveraging Beirut Tragedy in New Targeted Campaign (2020). Source: Quointelligence. Link: https://quointelligence.eu/2020/08/blackwater-malware-leveraging-beirut-tragedy-in-new-targeted-campaign/

Blue Estimate, a blunt APT attack, appears as a quote for the Blue House event (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2645

Blue Termite (Internet Watch) (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/0qhbl4o5adpf8fhdun7kp6cfz4ql3rdj

Bookworm Trojan: A Model of Modular Architecture (2015). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2015/11/bookworm-trojan-a-model-of-modular-architecture/

Born This Way? Origins of LockerGoga (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/

Bots, Machines, And The Matrix (2014). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/91ckw3z2lh26ylhxbjbjirjuyv5oslul

Breaking the Rules: A Tough Outlook for Home Page Attacks (CVE-2017-11774) (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/12/breaking-the-rules-tough-outlook-for-home-page-attacks.html

Breaking The Weakest Link Of The Strongest Chain (2017). Source: Kaspersky Lab. Link: https://app.box.com/s/wlwdugbbup1g3kb0ol71eh74qo6e67pd

BRONZE BUTLER Targets Japanese Enterprises (2017). Source: Dell Secureworks. Link: https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Bronze Buttler (2017). Source: Dell Secureworks. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/SecureWorksBronzeButlerReport.pdf

BRONZE PRESIDENT Targets NGOs (2019). Source: Dell Secureworks. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.12.29_BRONZE_PRESIDENT_NGO/BRONZE%20PRESIDENT%20Targets%20NGOs.pdf

BRONZE UNION Cyberespionage Persists Despite Disclosures (2017). Source: Dell Secureworks. Link: https://www.secureworks.com/research/bronze-union

BRONZE VINEWOOD Targets Supply Chains (2020). Source: Dell Secureworks. Link: https://www.secureworks.com/research/bronze-vinewood-targets-supply-chains

Brute Force Attacks Conducted (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA18-086A

Buckeye cyberespionage group shifts gaze from US to Hong Kong (2016). Source: Symantec. Link: https://app.box.com/s/0rfkkv27x039vbqsblzdsm530ii2ymjl

Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers (2019). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit

Buhtrap group uses zero-day in latest espionage campaigns (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/

Building Out ProtonMail Spoofed Infrastructure with Creation Timestamp Pivoting (2019). Source: ThreatConnect. Link: https://threatconnect.com/blog/building-out-protonmail-spoofed-infrastructure/

Burned After Reading Endless Mayfly's Ephemeral Disinformation Campaign (2019). Source: Citizen Lab. Link: https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/

Burning Umbrella (2018). Source: ProtectWise. Link: https://github.com/401trg/detections/raw/master/pdfs/20180503_Burning_Umbrella.pdf

Butterfly: Corporate Spies Out For Financial Gain (2015). Source: Symantec. Link: https://app.box.com/s/e8hbsm0zsrjryz3suwvutn1zjfpugwak

Buyer beware: cyberthreats targeting e-commerce (2018). Source: Kaspersky Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/Kaspersky-Lab-e-commerce-threat-report_eng_final.pdf

Byebye Shell And The Targeting Of Pakistan (2013). Source: Rapid7. Link: https://app.box.com/s/a4a59w1go5opcj607ssoh11oqnhozv0h

CactusPete APT group's updated Bisonal backdoor (2020). Source: Kaspersky Lab. Link: https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/

Callisto Group (2017). Source: F-Secure. Link: https://www.f-secure.com/documents/996508/1030745/callisto-group

Calypso APT: new group attacking state institutions (2019). Source: Positive Technologies. Link: https://app.box.com/s/7vzrq3frrll02n1gx4ssbtljnbgl0h7w

Campaign Possibly Connected to “MuddyWater” Surfaces in the Middle East and Central Asia (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/

Campaign Targeting Syrian Activists Escalates with New Surveillance Malware (2012). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2012/04/campaign-targeting-syrian-activists-escalates-with-new-surveillance-malware

Can a BEAR Fit Down a Rabbit Hole? (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/state-board-election-rabbit-hole/

CannibalRAT targets Brazil (2018). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2018/02/cannibalrat-targets-brazil.html

Capability of the People\\92s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation (2009). Source: Arbor Networks. Link: https://github.com/fdiskyou/threat-INTel/raw/master/200x/Cyber-030-2009.pdf

Carbanak APT The Great Bank Robbery (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/p7qzcury97tuwk26694uutujwqmwqyhe

Carbanak Group (2017). Source: Forcepoint. Link: https://www.threatminer.org/_reports/2017/Carbanak Group uses Google for Malware Command-and-Control _ Forcepoint.pdf

Carbanak is packing new guns (2015). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/h1dn7d6ptcpwjbcfj468fy5201ev4bbz

Carbanak Oracle Breach (2016). Source: Krebs on Security. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/Visa_Oracle-Micros-Compromise.pdf

CARBANAK Week Part Four: The CARBANAK Desktop Video Player (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-four-desktop-video-player.html

CARBANAK Week Part One: A Rare Occurrence (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-one-a-rare-occurrence.html

CARBANAK Week Part Three: Behind the CARBANAK Backdoor (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-three-behind-the-backdoor.html

CARBANAK Week Part Two: Continuing the CARBANAK Source Code Analysis (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-two-continuing-source-code-analysis.html

Carbon Paper: Peering into Turlas second stage backdoor (2019). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/ESET_Carbon-Paper-Peering-into-Turlas-second-stage-backdoor.pdf

Card Fraud in a PSD2 World: A Few Examples (2020). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5249083500438488439.pdf

Cardinal RAT Sins Again, Targets Israeli Fin-Tech Firms (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

Case Study: Operation Aurora (2010). Source: Triumfant. Link: https://app.box.com/s/ni4xs2iuol4vskbc25vrxjih2w1ep7p6

Cat Scratch Fever: Crowdstrike Tracks Newly Reported Iranian Actor As Flying Kitten (2014). Source: CrowdStrike. Link: https://app.box.com/s/vr9chzv8t952gywbaom6r0p4bo4pub8r

Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/88504.pdf

CC Blog Malware Leveraging PowerSploit (2017). Source: JPCERT. Link: https://www.threatminer.org/_reports/2017/JPCERT_CC Blog_ Malware Leveraging PowerSploit.pdf

CCleaner Command and Control Causes Concern (2017). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

CCleanup: A Vast Number of Machines at Risk (2017). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

CeidPageLock: A Chinese RootKit (2018). Source: Check Point. Link: https://research.checkpoint.com/ceidpagelock-a-chinese-rootkit/

CERBERUS Banking Trojan Analysis (2020). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5368578325360937307.pdf

CERT Georgia: Georbot Botnet (2012). Source: Ministry of Foreign Affairs of Georgia. Link: http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf

Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

CHAES: Novel Malware Targeting Latin American E-Commerce (2020). Source: Cybereason. Link: https://www.cybereason.com/hubfs/dam/collateral/reports/11-2020-Chaes-e-commerce-malware-research.pdf

Chafer used Remexi malware to spy on Iran-based foreign diplomatic entities (2019). Source: Kaspersky Lab. Link: https://securelist.com/chafer-used-remexi-malware/89538/

Chafer: Latest Attacks Reveal Heightened Ambitions (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

Champing at the Cyberbit (2017). Source: Citizen Lab. Link: https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Charming Kitten: Iranian Cyber Espionage Against Human Rights Activists, Academic Researchers and Media Outlets – And the HBO Hacker Connection (2017). Source: ClearSky Cybersecurity . Link: http://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

Charming Kitten's Christmas Gift (2021). Source: Certfa. Link: https://blog.certfa.com/posts/charming-kitten-christmas-gift/

ChChes - Malware that Communicates with C&C Servers Using Cookie Headers (2017). Source: JPCERT. Link: https://app.box.com/s/ud9z8kc33scu3fwbon1at9lcul9h9hw3

ChessMaster Adds Updated Tools to Its Arsenal (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-adds-updated-tools-to-its-arsenal/

ChessMaster Makes its Move: A Look into the Campaign's Cyberespionage Arsenal (2017). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/

ChessMaster's New Strategy: Evolving Tools and Tactics (2017). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/chessmasters-new-strategy-evolving-tools-tactics/

Chilean RedBanc Instrusion (2019). Source: Flashpoint. Link: https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/

China Chopper still active 9 years later (2019). Source: Cisco Talos. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.27.China_Chopper/China%20Chopper%20still%20active%209%20years%20later.pdf

China Hacks The Peace Palace: All Your Eez's Are Belong To Us (2015). Source: ThreatConnect. Link: https://app.box.com/s/yso9235awisw1dmjh8dyqpi5r9nokzcx

China-Based APT Mustang Panda Targets Minority Groups, Public and Private Sector Organizations (2019). Source: Anomali. Link: https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations?utm_content=102682106&utm_medium=social&utm_source=twitter&hss_channel=tw-197216119

China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets (2015). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

China's Electronic Long-Range Reconnaissance (2008). Source: US Army. Link: http://fmso.leavenworth.army.mil/documents/chinas-electronic.pdf

China's Great Cannon (2015). Source: Citizen Lab. Link: https://citizenlab.ca/2015/04/chinas-great-cannon/

China's Espionage Dynasty (2016). Source: Institute for Critical Infrastructure Technology (ICIT). Link: http://icitech.org/wp-content/uploads/2016/07/ICIT-Brief-China-Espionage-Dynasty.pdf

Chinese Actor APT target Ministry of Justice Vietnamese (2019). Source: Sebastien Larinier. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.1

1.Chinese_APT_Vietnamese/Chineses%20Actor%20APT%20target%20Ministry%20of%20Justice%20Vietnamese.pdf

Chinese APT “Operation LagTime IT” Targets Government Information Technology Agencies in Eastern Asia (2019). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology

Chinese APT Hackers Attack Windows Users via FakeNarrator Malware to Implant PcShare Backdoor (2019). Source: GBHackers. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.09.26_China_APT_FakeNarrator_To_PcShare/Chinese%20APT%20Hackers%20Attack%20Windows%20Users%20via%20FakeNarrator%20Malware.pdf

Chinese APT TA413 Resumes Targeting of Tibet Following COVID-19 Themed Economic Espionage Campaign Delivering Sepulcher Malware Targeting Europe (2020). Source: Proofpoint. Link: https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

Chinese Cyberespionage Originating From Tsinghua University Infrastructure (2018). Source: Recorded Future. Link: https://go.recordedfuture.com/hubfs/reports/cta-2018-0816.pdf

Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests (2020). Source: Recorded Future. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/cta-2020-0429.pdf

Chinese Ministry of State Security Behind APT3 (2017). Source: Recorded Future. Link: https://app.box.com/s/rkactl8fr73y037u6fypz700i4e2dk2m

Chinese Spam Network Finally Starts to Gain Some Traction (2021). Source: Graphika. Link: https://graphika.com/reports/spamouflage-breakout/

Chinese state-sponsored group 'reddelta' targets the Vatican and Catholic organizations (2020). Source: Recorded Future. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_527857238941053941O.pdf

Chinese Threat Actor TEMP.Periscope Targets UK-Based Engineering Company Using Russian APT Techniques (2018). Source: Recorded Future. Link: https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/

Chrome 0-day exploit CVE-2019-13720 used in Operation WizardOpium (2019). Source: Kaspersky Lab. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.1.Operation_WizardOpium/Chrome%200-day%20exploit%20CVE-2019-13720%20used%20in%20Operation%20WizardOpium%20.pdf

CLAMBLING - A New Backdoor Base On Dropbox (EN) (2020). Source: Talent-Jump. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.02.17_CLAMBLING_Dropbox_Backdoor/CLAMBLING%20-%20A%20New%20Backdoor%20Base%20On%20Dropbox%20(EN).pdf

Clearing the MuddyWater - Analysis of new MuddyWater Samples (2018). Source: Security 0wnage. Link: https://sec0wn.blogspot.com/2018/05/clearing-muddywater-analysis-of-new.html?m=1

Cloud Atlas: Redoctober Apt Is Back In Style (2014). Source: Kaspersky Lab. Link: https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/

Cmstar Downloader: Lurid And Enfal's New Cousin (2015). Source: Palo Alto Networks. Link: https://app.box.com/s/67esnb1ppzsgyo3mm5es3zs8khtf3rpe

COBALT DICKENS Goes Back to School…Again (2019). Source: Dell Secureworks. Link: https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

Cobalt Gang APT: Recent infrastructure and CobInt/COOLPANTS malware analysis (2019). Source: Meltx0r. Link: https://meltx0r.github.io/tech/2019/10/15/cobalt-gang-apt.html

Cobalt Group 2.0 (2018). Source: Morphisec. Link: https://blog.morphisec.com/cobalt-gang-2.0

Cobalt Group Returns To Kazakhstan (2019). Source: Check Point. Link: https://research.checkpoint.com/cobalt-group-returns-to-kazakhstan/

Cobalt Logical Attacks on ATMs (2020). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/Group-IB_Cobalt.pdf

Cobalt Renaissance: new attacks and joint operations (2018). Source: Group-IB. Link: https://www.group-ib.com/blog/renaissance

Cobalt strikes back: an evolving multinational threat to finance (2017). Source: Positive Research. Link: http://blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html

Cobalt: tactics and tools update (2020). Source: Positive Technologies. Link: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/cobalt_upd_ttps/

Collaboration between FIN7 and the RYUK group, a Truesec Investigation (2020). Source: Truesec. Link: https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/

COM Object hijacking: the discreet way of persistence (2014). Source: G Data Software. Link: https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence

Combating Aurora (2010). Source: Intel Security-McAfee. Link: https://app.box.com/s/jhy5k76ox6z8sy6tdjnqqrlz5r2o29h8

Command And Control In The Fifth Domain (2013). Source: Command Five. Link: https://app.box.com/s/yfduvs6jw8w3ankhjkbi4ei5ykqho368

Comment Crew: Indicators Of Compromise (2013). Source: Symantec. Link: https://app.box.com/s/0leqi6xaid7v745y3kujcyi5vgvf73su

Commonly Known Tools Used by Lazarus (2021). Source: JPCERT. Link: https://blogs.jpcert.or.jp/en/2021/01/Lazarus_tools.html

COMMSEC: The Trails of WINDSHIFT APT (2018). Source: DarkMatter. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/D1_COMMSEC.pdf

Comnie Continues to Target Organizations in East Asia (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/01/unit42-comnie-continues-target-organizations-east-asia/

Comparing the Regin module 50251 and the 'Qwerty' keylogger (2015). Source: Kaspersky Lab. Link: http://securelist.com/blog/research/68525/comparing-the-regin-module-50251-and-the-qwerty-keylogger/

COMpfun authors spoof visa application with HTTP status-based Trojan (2020). Source: Kaspersky Lab. Link: https://securelist.com/compfun-http-status-based-trojan/96874/

"COMpfun successor Reductor infects files on the fly to compromise TLS traffic

(2019). Source: Kaspersky Lab. Link: https://securelist.com/compfun-successor-reductor/93633/"

Compromise at the State Department (2006). Source: Anomali. Link: http://www.cbsnews.com/news/state-department-computers-hacked/

Compromise at U.S. Naval War College (2006). Source: Accenture. Link: http://fcw.com/articles/2006/12/04/china-is-suspected-of-hacking-into-navy-site.aspx?sc_lang=en

Compromise of a Pentagon legacy system (2015). Source: Antiy Labs. Link: http://www.defense.gov/News/Transcripts/Transcript-View/Article/607043

Compromise of Canada's National Research Council (2014). Source: Open Source. Link: https://web.archive.org/web/20140729142533/http://news.gc.ca/web/article-en.do?nid=871449

Compromise of French Defense Ministry website (2007). Source: Financial Times. Link: https://web.archive.org/web/20080118141424/http://www.france24.com/france24Public/en/news/france/20070909-Internet-piracy-france-secuirty-china-hacker.html

Compromise of iCloud in China (2014). Source: Electronic Frontier Foundation. Link: https://en.greatfire.org/blog/2014/oct/china-collecting-apple-icloud-data-attack-coincides-launch-new-iphone

Compromise of Indian military computers (2008). Source: Cylance. Link: http://timesofindia.indiatimes.com/india/China-mounts-cyber-attacks-on-Indian-sites/articleshow/3010288.cms

Compromise of National Defense University (2007). Source: Electronic Frontier Foundation. Link: http://www.washingtontimes.com/news/2007/jan/12/20070112-123024-8199r/?page=1

Compromise of Saudi Aramco and RasGas (2012). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/57854/shamoon-the-wiper-copycats-at-work/

Compromise of the Finnish Ministry of Foreign Affairs (2013). Source: Avast. Link: http://www.mtv.fi/uutiset/kotimaa/artikkeli/mtv3-suomen-ulkoministerio-laajan-verkkovakoilun-kohteena-vuosia/2369718

Compromise of the Indian Prime Minister's Office (2010). Source: RSA Security. Link: http://indiatoday.intoday.in/story/Chinese+hackers+target+PMO/1/79215.html

Compromise of the office of Senator Ben Nelson (2009). Source: NATO. Link: http://web.archive.org/web/20090323095526/http://www.cqpolitics.com/wmspage.cfm?docid=news-000003080993

Compromise of the Permanent Court of Arbitration's website (2015). Source: ThreatConnect. Link: https://web.archive.org/web/20151031022526/https://threatconnect.com/china-hacks-the-peace-palace-all-your-eezs-are-belong-to-us/

Compromise of the Seoul subway system (2015). Source: Electronic Frontier Foundation. Link: http://www.koreaherald.com/view.php?ud=20151005001125

Compromise of U.S. Investigations Services (2014). Source: Electronic Frontier Foundation. Link: https://web.archive.org/web/20150223064255/http://usis.com/Media-Release-Detail.aspx?dpid=151

Compromise of U.S. Transportation Command Contractors (2014). Source: NATO. Link: https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors

Confucius APT deploys Warzone RAT (2021). Source: Uptycs. Link: https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat

Confucius Update: New Tools and Techniques, Further Connections with Patchwork (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/confucius-update-new-tools-and-techniques-further-connections-with-patchwork/

Connecting the dots Exposing the arsenal and methods of the Winnti Group (2019). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/ESET_Winnti.pdf

Connecting The Dots: Syrian Malware Team Uses Blackworm For Attacks (2014). Source: FireEye. Link: https://app.box.com/s/5sir2hjd6rhi9a03nb5e4ykkx3s4l7d6

Copy cat of APT Sidewinder ? (2020). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/copy-cat-of-apt-sidewinder-1893059ca68d

CopyKittens Attack Group (2015). Source: ClearSky Cybersecurity . Link: https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

Corporate IoT – a path to intrusion (2019). Source: Microsoft. Link: https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

Cosmic Banker campaign is still active revealing link with Banload malware (2019). Source: SCILabs. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.12.06.Cosmic_Banker_campaign/Cosmic%20Banker%20campaign%20is%20still%20active%20revealing%20link%20with%20Banload%20malware.pdf

Cosmic Lynx: The Rise of Russian BEC (2020). Source: AGARI. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/acid-agari-cosmic-lynx.pdf

Cosmicduke Cosmu With A Twist Of Miniduke (2014). Source: F-Secure. Link: https://app.box.com/s/b0mc62by5j96jg9l91t68mlq6roksbg2

Cozyduke (2015). Source: F-Secure. Link: https://app.box.com/s/wig4z9nwq6wjxf3i4aslu9qro14pgsbe

Craft for Resilence - APT Group Chimera - APT Operation Skeleton Key Targets Taiwan Semiconductor Vendors (2020). Source: Cycraft. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/20200415_Chimera_V4.1.pdf

CrashOverride (2017). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA17-163A

CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations (2017). Source: Dragos. Link: https://app.box.com/s/cl2m9xiifjoz0iajwthet2eaeyp26e13

CrashOverride: Analysis of the Threat to Electric Grid Operations (2017). Source: Dragos. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/CrashOverride-01.pdf

CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack (2019). Source: Dragos. Link: https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

CRAT wants to plunder your endpoints (2020). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2020/11/crat-and-plugins.html

CREDENTIALS GATHERING CAMPAIGN (2019). Source: Agence nationale de la sécurité des systèmes d'information. Link: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-009.pdf

Crime Without Punishment: In-depth analysis of js-sniffers (2020). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/Group-IB_js-sniffers.pdf

Cross-Platform Spam Network Targeted Hong Kong Protests (2019). Source: Graphika. Link: https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf

Crouching Tiger, Hidden Dragon, Stolen Data (2012). Source: Context IS. Link: https://app.box.com/s/vk0oacayqkgrk3tp492h3ja9jnlktk7t

Crouching Yeti: Appendixes (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/90zdh7pfbmon8mtea3okbc6s83ro28bx

Crowdstrike Global Threat Intel Report (2015). Source: CrowdStrike. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2015/GlobalThreatIntelReport.pdf

CrowdStrike’s January Adversary of the Month: VOODOO BEAR (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/

Crude Faux: An Analysis Of Cyber Conflict Within The Oil & Gas Industries (2013). Source: CERIAS. Link: https://app.box.com/s/9dpb6yyvb4yedosa75fo1ibuo46oy35a

Cryptocurrency businesses still being targeted by Lazarus (2019). Source: Kaspersky Lab. Link: https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/

Cutwail Spam Campaign Uses Steganography to Distribute URLZone (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/

CVE-2014-4114: Details on August BlackEnergy PowerPoint Campaigns (2014). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/

CVE-2015-2545: overview of current threats (2016). Source: Kaspersky Lab. Link: https://app.box.com/s/ztb6a52hkbenfurrecc3jifk9b67ie79

CVE-2017-8570 RTF and the Sisfader RAT (2018). Source: NCCGroup. Link: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8570-rtf-and-the-sisfader-rat/

CVE-2017-8759: Zero-Day Used in the Wild to Distribute FINSPY (2017). Source: FireEye. Link: https://app.box.com/s/mgz7lvnbg6bjhjognrlc7ovqdcqpbhgo

Cyber Actors Target Home and Office Routers and Networked Devices Worldwide (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA18-145A

Cyber Attack Impersonating Identity Of Indian Think Tank To Target Central Bureau Of Investigation (cbi) And Possibly Indian Army Officials (2017). Source: Cysinfo. Link: https://app.box.com/s/mmr87n5onrrqiz8gnt93vvifpwn1rvah

Cyber Attack Targeting Indian Navy's Submarine And Warship Manufacturer (2017). Source: Cysinfo. Link: https://app.box.com/s/zdwfwsi2pw1081j2reu3qotz577g7pt6

Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations (2017). Source: FireEye. Link: https://app.box.com/s/zutjtgdovy2dc32ktf5347y46eslqxq0

Cyber War and Iranian Cyber Army -In the name of Ashrar- An article by Ashrar team (2019). Source: Treadstone 71. Link: https://cybershafarat.com/2019/03/10/cyber-war-and-iranian-cyber-army-in-the-name-of-ashrar-an-article-by-ashrar-team/

Cyber war in perspective: Russian aggression against Ukraine (2015). Source: NATO. Link: https://app.box.com/s/tnk1sw3cv0k0semcc9o275tjm5iliz45

Cyber-Espionage Campaign Targeting the Naval Industry (“MartyMcFly”) (2018). Source: Yoroi. Link: https://blog.yoroi.company/?p=1829

CYBERATTACKS AGAINST UKRAINIAN ICS (2017). Source: NATO. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/EBOOK_CYBERATTACKS-AGAINST-UKRAINIAN-ICS.pdf

Cybercrime in West Africa Poised for an Underground Market (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5429601942257010394.pdf

Cybereason Threat Intel Report: Blurring the lines between nation-state and for profit (2017). Source: Cybereason. Link: https://www.cybereason.com/blog/blog-blurring-the-lines-between-nation-state-and-for-profit

Cybereason vs. MedusaLocker Ransomware (2020). Source: Cybereason. Link: https://www.cybereason.com/blog/medusalocker-ransomware

Cyberwarfare: A deep dive into the latest Gamaredon Espionage Campaign (2020). Source: Yoroi. Link: https://blog.yoroi.company/research/cyberwarfare-a-deep-dive-into-the-latest-gamaredon-espionage-campaign/

Cycldek: Bridging the (air) gap (2020). Source: Kaspersky Lab. Link: https://securelist.com/cycldek-bridging-the-air-gap/97157/

Cylance Spear Team: A Threat Actor Resurfaces (2015). Source: Cylance. Link: https://app.box.com/s/ma0qrrczbji4grvjbezpeugf3gru084x

Dacls, the Dual platform RAT (2019). Source: NetLab. Link: https://blog.netlab.360.com/dacls-the-dual-platform-rat-en/

Damballa discovers new toolset linked to Destover Attacker's arsenal helps them to broaden attack surface (2015). Source: Damballa/SecureAuth. Link: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/2015.11.18.Destover/amballa-discovers-new-toolset-linked-to-destover-attackers-arsenal-helps-them-to-broaden-attack-surface.pdf

Dark Basin: Uncovering a Massive Hack-For-Hire Operation (2020). Source: Citizen Lab. Link: https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

Dark Caracal: Cyber-espionage at a Global Scale (2018). Source: Lookout. Link: https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Dark Seoul Cyber Attack: Could It Be Worse? (2013). Source: Dongseo University. Link: https://app.box.com/s/qw0kvewoi3uxy4g3xkc31ammxttbft5z

Dark Tequila Añejo (2018). Source: Kaspersky Lab. Link: https://securelist.com/dark-tequila-anejo/87528/

Darkhotel Indicators of Compromise (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/r97cjt70ywsd7pnrstr7buqzxn5svfw1

Darkhotel's attacks in 2015 (2015). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/66779/the-darkhotel-apt/

DarkHydrus delivers new Trojan that can use Google Drive for C2 communications (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/

DarkHydrus Uses Phishery to Harvest Credentials in the Middle East (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/08/unit42-darkhydrus-uses-phishery-harvest-credentials-middle-east/

DarkPulsar (2018). Source: Kaspersky Lab. Link: https://securelist.com/darkpulsar/88199/

Darkseoul-Jokra Analysis And Recovery (2013). Source: Fidelis Cybersecurity. Link: http://www.fidelissecurity.com/sites/default/files/FTA%201008%20-%20Darkseoul-Jokra%20Analysis%20and%20Recovery.pdf

DarkUniverse – the mysterious APT framework #27 (2019). Source: Kaspersky Lab. Link: https://securelist.com/darkuniverse-the-mysterious-apt-framework-27/94897/

Darwin's Favorite Apt Group (2014). Source: FireEye. Link: https://app.box.com/s/aj0b81yqt1fe6ufuklxuirvh8hawnnjb

DEADLYKISS: HIT ONE TO RULE THEM ALL. TELSY DISCOVERED A PROBABLE STILL UNKNOWN AND UNTREATED APT MALWARE AIMED AT COMPROMISING INTERNET SERVICE PROVI (2019). Source: Telsy. Link: https://blog.telsy.com/deadlykiss-malware/

Dealing with the threats posed by Triton / Trisis destructive malware (2018). Source: Accenture. Link: https://www.accenture.com/t20180123T095554Z__w__/us-en/_acnmedia/PDF-46/Accenture-Security-Triton-Trisis-Threat-Analysis.pdf

Dear Joohn: The Sofacy Group's Global Campaign (2018). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/

Debugging the Pakistan Cyber Army: From Pakbugs to Bitterbugs (2014). Source: ThreatConnect. Link: https://threatconnect.com/blog/debugging-pca-from-pakbugs-to-bitterbugs/

Decade of the RATs: Novel APT Attacks Targeting Linux, Windows and Android (2020). Source: Cylance. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/Decade_of_the_Rats.pdf

Deciphering Confucius' Cyberespionage Operations (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/

DECLAWING THE DRAGON: WHY THE U.S. MUST COUNTER CHINESE CYBER-WARRIORS (2009). Source: US Army. Link: https://github.com/fdiskyou/threat-INTel/raw/master/200x/DECLAWING-THE-DRAGON-2009.pdf

Decrypting Strings in Emdivi (2015). Source: JPCERT. Link: http://blog.jpcert.or.jp/2015/11/decrypting-strings-in-emdivi.html

Deep Dive On The DragonOK Rambo Backdoor (2017). Source: Morphick. Link: http://www.morphick.com/resources/news/deep-dive-dragonok-rambo-backdoor

Deep Panda (2013). Source: CrowdStrike. Link: https://app.box.com/s/6po2pgedkjf4br5p7tm51go7p5g3z6g3

Deep Panda Uses Sakula Malware (2014). Source: CrowdStrike. Link: http://blog.crowdstrike.com/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/

Defeating Compiler Level Obfuscations Used in APT10 Malware (2019). Source: Carbon Black. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.02.25.APT10_Defeating_Compiler_Level/Defeating%20Compiler-Level%20Obfuscations%20Used%20in%20APT10%20Malware.pdf

DEFLECT LABS REPORT #6: PHISHING AND WEB ATTACKS TARGETING UZBEK HUMAN RIGHT ACTIVISTS AND INDEPENDENT MEDIA (2019). Source: eQualitie. Link: https://equalit.ie/en/deflect-labs-report-6/

Delivery (Key)Boy (2018). Source: AlienVault. Link: https://www.alienvault.com/blogs/labs-research/delivery-keyboy

Democracy In Hong Kong Under Attack (2014). Source: Volexity. Link: https://app.box.com/s/dvtxta3jtratjxlpr5rzwsqvqfetsn6z

Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability CVE-2015-5119 Following Hacking Team Leak (2015). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

Denial of service incident against South Korean and U.S. targets (2011). Source: Intel Security-McAfee. Link: https://web.archive.org/web/20140602010545/http://blogs.mcafee.com/mcafee-labs/10-days-of-rain-in-korea

Derusbi (Server Variant) Analysis (2014). Source: Novetta. Link: https://app.box.com/s/t3h83k7pfdyzoi3hrhfl7k5o33sk1fwk

Desktop, Mobile Phishing Campaign Targets South Korean Websites, Steals Credentials Via Watering Hole (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.28.Desktop_Mobile_Phishing_Campaign/Desktop%2C%20Mobile%20Phishing%20Campaign%20Targets%20South%20Korean%20Websites%2C%20Steals%20Credentials%20Via%20Watering%20Hole.pdf

Destructive Attack “DUSTMAN” (2019). Source: National CyberSecurity Authority. Link:

Detailed Analysis of Red Eyes Hacking Group (2018). Source: AhnLab. Link: https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5D%20Red_Eyes_Hacking_Group_Report%20(1).pdf

Detecting and Responding Pandas and Bears (2016). Source: SANS Institute. Link: http://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Detecting-and-Responding-to-Pandas-and-Bears-Christopher-Scott-CrowdStrike-and-Wendi-Whitmore-IBM.pdf

Detecting Lateral Movement through Tracking Event Logs (2017). Source: JPCERT. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/20170612ac-ir_research_en.1.pdf

Detecting threat actors in recent German industrial attacks (2017). Source: Microsoft. Link: https://www.threatminer.org/_reports/2017/Detecting threat actors in recent German industrial attacks with Windows Defender ATP - Microsoft.pdf

Development of the activity of the TA505 Cybercriminal Group (2020). Source: Agence nationale de la sécurité des systèmes d'information. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5350498639053588191.pdf

Digging up InvisiMole’s hidden arsenal (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs (2019). Source: Volexity. Link: https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

Dimnie: Hiding in Plain Sight (2017). Source: Palo Alto Networks. Link: https://app.box.com/s/scdmr7ekxhx4ktprct29ojxyllr41bjq

Dino: The Latest Spying Malware From An Allegedly French Espionage Group Analyzed (2015). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/wavmm2zrlt4n1jri8byn31b9fb1wo35i

Diplomats in Eastern Europe bitten by a Turla mosquito (2017). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/vmzqwqfrmtdjemtdaei60jqu5qrouwrt

Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware (2017). Source: Citizen Lab. Link: https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/

Dissecting Geost: Exposing the Anatomy of the Android Trojan Targeting Russian Banks (2020). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.05_Dissecting_Geost/Dissecting%20Geost_%20Exposing%20the%20Anatomy%20of%20the%20Android%20Trojan%20Targeting%20Russian%20Banks%20-%20TrendLabs%20Security%20Intelligence%20Blog.pdf

Dissecting Linux/Moose: The Analysis Of A Linux Router-Based Worm Hungry For Social Networks (2015). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/38tsu5p4cc9kevuiiaxrptw3wrgksguk

Dissecting One of APT29's Fileless WMI and PowerShell Backdoors (2017). Source: FireEye. Link: https://www.threatminer.org/_reports/2017/Dissecting One of APT29â€™s Fileless WMI and PowerShell Backdoors (POSHSPY) Â« Threat Research Blog _ FireEye Inc.pdf

Dissecting Operation Troy: Cyberespionage In South Korea (2013). Source: Intel Security-McAfee. Link: https://app.box.com/s/b91tgqhiw7zyivfnxe3sbrtzfgk6n08f

Dissecting the APT28 Mac OS X Payload (2017). Source: BitDefender. Link: https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf

Dissecting The Kraken (2015). Source: G Data Software. Link: https://app.box.com/s/r5vy0kolgdxwwby2wjo523devdbt5leg

Dissecting the Malware Involved in the INOCNATION Campaign (2016). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/dl6izicyky1x946ueo77nn2w8c5jxgm3

DNS Hijacking Abuses Trust In Core Internet Service (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/04/seaturtle.html

DNS Infrastructure Hijacking Campaign (2019). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/AA19-024A

DNS Manipulation in Venezuela in regards to the Humanitarian Aid Campaign (2019). Source: Kaspersky Lab. Link: https://securelist.com/dns-manipulation-in-venezuela/89592/

DNS Tunneling in the Wild: Overview of OilRig's DNS Tunneling (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/

DNSpionage Campaign Targets Middle East (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

Domestic Kitten – An Inside Look at the Iranian Surveillance Operations (2021). Source: Check Point. Link: https://research.checkpoint.com/2021/domestic-kitten-an-inside-look-at-the-iranian-surveillance-operations/

Domestic Kitten: An Iranian Surveillance Operation (2018). Source: Check Point. Link: https://research.checkpoint.com/domestic-kitten-an-iranian-surveillance-operation/

Donot (APT-C-35) Group Is Targeting Pakistani Businessman Working In China (2018). Source: 360 SkyEye System. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.12.12.Donot_Group/Donot_Group.pdf

Donot Team Leverages New Modular Malware Framework in South Asia (2018). Source: Arbor Networks. Link: https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/

Double DragonAPT41, a dual espionage and cyber crime operation (2019). Source: FireEye. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/apt41.pdf

Double the Infection, Double the Fun (2018). Source: Arbor Networks. Link: https://www.netscout.com/blog/asert/double-infection-double-fun

Double Trouble: RevengeRAT and WSHRAT (2019). Source: Fortinet. Link: https://www.fortinet.com/blog/threat-research/malware-analysis-revenge-rat-sample.html

Down the H-W0rm Hole with Houdini's RAT (2016). Source: Fidelis Cybersecurity. Link: https://www.fidelissecurity.com/threatgeek/2016/11/down-h-w0rm-hole-houdinis-rat

Downeks and Quasar RAT Used in Recent Targeted Attacks Against Governments (2017). Source: Palo Alto Networks. Link: https://www.threatminer.org/_reports/2017/Downeks and Quasar RAT Used in Recent Targeted Attacks Against Governments - Palo Alto Networks Blog.pdf

Dragonfish delivers new form of Elise malware targeting ASEAN Defense Ministers' meeting and associates (2018). Source: Accenture. Link: https://www.accenture.com/t20180127T003755Z__w__/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf

Dragonfly: Cyberespionage Attacks Against Energy Suppliers (2014). Source: Symantec. Link: https://app.box.com/s/edyb0yn2g8ozavlmxoh082l7z5o5v3yx

Dragonfly: Western energy sector targeted by sophisticated attack group (2017). Source: Symantec. Link: https://app.box.com/s/4kpnzlrdqdcg3cq02hz4zj8nmjd9iywi

DragonOK Updates Toolset and Targets Multiple Geographic Regions (2017). Source: Palo Alto Networks. Link: https://app.box.com/s/50tu7yfcrcj3ntj6b894rq6londdps34

Dridex's Cold War: Enter AtomBombing (2017). Source: IBM. Link: https://securityintelligence.com/dridexs-cold-war-enter-atombombing/

Drilling Deep: A Look at Cyberattacks on the Oil and Gas Industry (2020). Source: Trend Micro. Link: https://documents.trendmicro.com/assets/white_papers/wp-drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry.pdf

Drive-by as a service: BlackTDS (2018). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/drive-service-blacktds

DROPPING ANCHOR: FROM A TRICKBOT INFECTION TO THE DISCOVERY OF THE ANCHOR MALWARE (2019). Source: Cybereason. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.12.11_DROPPING_ANCHOR/Anchor%20IOCs.pdf

Duke APT Group's Latest Tools: Cloud Services And Linux Support (2015). Source: F-Secure. Link: https://app.box.com/s/4oehib8xu2boak3hd72sh1f9ka9gwwh7

Duqu 1.5: A Ghost in the Wires of a Diplomatic Venue (2019). Source: Chronicle. Link: https://storage.googleapis.com/chronicle-research/DuQu%201.5%20A%20Ghost%20in%20the%20Wires.pdf

Duqu 2.0: A Comparison To Duqu (2015). Source: Laboratory of Cryptography and System Security (CrySyS Lab). Link: https://app.box.com/s/yfoqrf6r0i0ih38pl0bmtud3ke0e6vhf

Duqu 2.0: Reemergence of an aggressive cyberespionage threat (2015). Source: Symantec. Link: https://www.symantec.com/connect/blogs/duqu-20-reemergence-aggressive-cyberespionage-threat

Duqu Trojan Questions And Answers (2011). Source: Dell Secureworks. Link: https://app.box.com/s/ygyqokm0cxq56lut0v1u0i4u5vts9idc

Earth Wendigo Injects JavaScript Backdoor to Service Worker for Mailbox Exfiltration (2021). Source: Trend Micro. Link: https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html

Ego Market When Greed for Fame Benefits Large-Scale Botnets (2016). Source: blackhat. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/eu-16-Paquet-Clouston-Ego-Market_When-Greed-for-Fame-Benefits-Large-Scale-Botnets-wp.pdf

EHDevel – The story of a continuously improving advanced threat creation toolkit (2017). Source: BitDefender. Link: https://labs.bitdefender.com/2017/09/ehdevel-the-story-of-a-continuously-improving-advanced-threat-creation-toolkit/

EKANS Ransomware and ICS Operations (2020). Source: Dragos. Link: https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

El Machete (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/badlir1w3z6fowjb0xj9too0mf11ls4e

El Machete's Malware Attacks Cut Through LATAM (2017). Source: Cylance. Link: https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html

Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S. (2019). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

Elimination of sample analysis and traceability using a variety of Office OLE features (2018). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/analysis-of-office-ole-sample/

ELISE: Security Through Obesity (2015). Source: PWC. Link: https://app.box.com/s/xjjieg8w489osjfp4jk7vgum37a6ibro

Emerging Threat Profile Shell_Crew (2014). Source: RSA Security. Link: https://app.box.com/s/xqldk5renv5ecihr7wyyazplrnezknmx

Emissary Panda APT: Recent infrastructure and RAT analysis (2019). Source: Meltx0r. Link: https://meltx0r.github.io/tech/2019/09/19/emissary-panda-apt.html

Emissary Panda Attacks Middle East Government Sharepoint Servers (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

Emissary Trojan Changelog: Did Operation Lotus Blossom Cause It to Evolve? (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/

EMOTET: A technical analysis of the destructive, polymorphic malware (2019). Source: CrowdStrike. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/Bromium-Emotet-Technical-Analysis-Report.pdf

En Route with Sednit Part 1: Approaching the Target (2016). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/c7oz0zci5gxsbgnucxwah82bfdj0boe0

En Route with Sednit Part 2: Observing the Comings and Goings (2016). Source: ESET WeLiveSecurity. Link: http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

En Route with Sednit Part 3: A Mysterious Downloader (2016). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/p4ywd9iqr5fr48nbz5o0nfwwgjkq5itk

Encrypted APT attack, Kimsuky organization's 'smoke screen' PART 2 (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2299

Energetic Bear _ Crouching Yeti (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/z0apbug9w1ztt8ex0pe99sq0d2u9r3nu

Energetic Bear/Crouching Yeti: attacks on servers (2018). Source: Kaspersky Lab. Link: https://securelist.com/energetic-bear-crouching-yeti/85345/

Energy At Risk: A Study Of It Security In The Energy And Natural Resources Industry (2013). Source: KPMG. Link: https://app.box.com/s/z7lwte5v91lz2rkfywd9s1grnqeuy1fk

Enhanced Analysis of GRIZZLY STEPPE Activity (2017). Source: US-CERT. Link: https://www.threatminer.org/_reports/2017/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf

Equation Group: Questions And Answers (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/reidof9i3qnjdq4t0k49o392g8r98tbt

ESET discovered an undocumented backdoor used by the infamous Stealth Falcon group (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/09/09/backdoor-stealth-falcon-group/

Espionage toolkit targeting Central and Eastern Europe uncovered (2016). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/kmb22xnoniwxfkhsw8r3tkpo5rko0w1a

Etso Apt Attacks Analysis (2013). Source: AhnLab. Link: https://app.box.com/s/n4vji662ern1bii9hhahvglujeobqmk0

Evasive Tactics: Terminator Rat (2013). Source: FireEye. Link: http://www.fireeye.com/blog/technical/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

Everything we know about GoldenEye (2017). Source: BitDefender. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Bitdefender-Whitepaper-GoldenEye.pdf

Evidence Aurora Operation Still Active: Supply Chain Attack Through CCleaner (2017). Source: Intezer. Link: https://app.box.com/s/o8rait7di3od2z60v8mj77x4a5jb2xun

Evidence Aurora Operation Still Active: Supply Chain Attack Through CCleaner part2 (2017). Source: Intezer. Link: https://app.box.com/s/pszqtsxza5quthzuz31pqwypaf6idzum

Evil Bunny: Suspect #4 (2014). Source: Marion Marschalek. Link: https://app.box.com/s/xvilsesi5qd2gh6so2g3tnric51ndv57

Evil Eye Threat Actor Resurfaces with iOS Exploit and Updated Implant (2020). Source: Volexity. Link: https://www.volexity.com/blog/2020/04/21/evil-eye-threat-actor-resurfaces-with-ios-exploit-and-updated-implant/

EvilBunny: Malware Instrumented By Lua (2015). Source: Cyphort. Link: https://www.cyphort.com/evilbunny-malware-instrumented-lua/

EvilGnome: Rare Malware Spying on Linux Desktop Users (2019). Source: Intezer. Link: https://www.intezer.com/blog-evilgnome-rare-malware-spying-on-linux-desktop-users/

Evilgrab Delivered by Watering Hole Attack on President of Myanmar's Website (2015). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/

Evolution of Agent.BTZ to ComRAT (2015). Source: G Data Software. Link: https://blog.gdatasoftware.com/blog/article/evolution-of-sophisticated-spyware-from-agentbtz-to-comrat.html

Evolution of Cyber Threats in the Corporate Sector (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/ql84nxbrheluzhi3bt7k48damnuz00u5

Evolution Of Sophisticated Spyware: From Agent.Btz To Comrat (2015). Source: G Data Software. Link: https://app.box.com/s/gqksdtk0gogqzzzbg2w6b4y7fej6f26t

Evolution of the GOLD EVERGREEN Threat Group (2017). Source: Dell Secureworks. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Evolution_of_the_GOLD_EVERGREEN_ThreatGroup_SecureWorks.pdf

Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa (2019). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/

Evolving Threats:dissection of a CyberEspionage attack (2015). Source: RSA Security. Link: http://www.rsaconference.com/writable/presentations/file_upload/cct-w08_evolving-threats-dissection-of-a-cyber-espionage-attack.pdf

Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families/

Exclusive disclosure worldwide: the information assassin "Golden Eagle" APT organization over Central Asia (2019). Source: 360 SkyEye System. Link: http://www.360.cn/n/11338.html

ExileRAT shares C2 with LuckyCat, targets Tibet (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/02/exilerat-shares-c2-with-luckycat.html

Exodus: New Android Spyware Made in Italy (2019). Source: Security Without Borders. Link: https://www.securitywithoutborders.org/blog/2019/03/29/exodus.html

ExPetr/Petya/NotPetya is a Wiper, Not Ransomware (2017). Source: Kaspersky Lab. Link: https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

Exploitation of Accellion File Transfer Appliance (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/alerts/aa21-055a

Exploring CVE-2015-2545 and its users (2016). Source: PWC. Link: https://app.box.com/s/g9pew9ajkp259c2t99mh4xspsev61hgm

Exposing Modular Adware: How DealPly, IsErIk, and ManageX Persist in Systems (2020). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/exposing-modular-adware-how-dealply-iserik-and-managex-persist-in-systems/

Fake or Fake: Keeping up with OceanLotus decoys (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/03/20/fake-or-fake-keeping-up-with-oceanlotus-decoys/

Fake YouTube Site Targets Syrian Activists With Malware (2012). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware

Fakem Rat: Malware Disguised As Windows Messenger And Yahoo! Messenger (2013). Source: Trend Micro. Link: https://app.box.com/s/otjh028wd3rfia4ysdtldj3whsd1i4y2

Falling on muddywater (2018). Source: Sekoia. Link: https://www.sekoia.fr/blog/falling-on-muddywater/

False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan (2017). Source: Amnesty International. Link: https://medium.com/amnesty-insights/false-friends-how-fake-accounts-and-crude-malware-targeted-dissidents-in-azerbaijan-9b6594cafe60

Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces (2018). Source: Citizen Lab. Link: https://citizenlab.ca/2018/08/familiar-feeling-a-malware-campaign-targeting-the-tibetan-diaspora-resurfaces/

FANCY BEAR Has an (IT) Itch that They Can't Scratch (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/fancy-bear-it-itch-they-cant-scratch/

Fancy Bears and Where to Find Them (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/tapping-into-democratic-national-committee/

Farewell to Kelihos and ZOMBIE SPIDER (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/farewell-to-kelihos-and-zombie-spider/

Farseer: Previously Unknown Malware Family bolsters the Chinese armoury (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/farseer-previously-unknown-malware-family-bolsters-the-chinese-armoury/

FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks (2020). Source: US-CERT. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5352750438867273316.pdf

FASTCash: How the Lazarus Group is Emptying Millions from ATMs (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware

FastPOS: Quick and Easy Credit Card Theft (2016). Source: Trend Micro. Link: http://documents.trendmicro.com/assets/fastPOS-quick-and-easy-credit-card-theft.pdf

Fictitious Profiles and WebRTCs Privacy Leaks Used to Identify Iranian Activists (2016). Source: Claudio Guarnieri e Collin Anderson. Link: https://iranthreats.github.io/resources/webrtc-deanonymization/

FIN10 Anatomy of a Cyber Extortion Operation (2017). Source: Positive Research. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/rpt-fin10.pdf

FIN6 Compromised E-commerce Platform via Magecart to Inject Credit Card Skimmers Into Thousands of Online Shops (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.10.09_FIN6_Magecart/FIN6%20Compromised%20E-commerce%20Platform%20via%20Magecart%20to%20Inject%20Credit%20Card%20Skimmers%20Into%20Thousands%20of%20Online%20Shops.pdf

FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings (2017). Source: FireEye. Link: https://www.threatminer.org/_reports/2017/FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings.pdf

FIN7.5: the infamous cybercrime rig “FIN7” continues its activities (2019). Source: Kaspersky Lab. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.08.Fin7.5/FIN7.5_%20the%20infamous%20cybercrime%20rig%20%E2%80%9CFIN7%E2%80%9D%20continues%20its%20activities.pdf

Financial Threat Group Targets Volume Boot Record (2015). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

Finding Holes Operation Emmental (2014). Source: Trend Micro. Link: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf

Findings from Analysis of DNC Intrusion Malware (2016). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/406jm438rm7s65du4d4qnj7iwj5bkphv

FinFisher surveillance campaigns: Internet providers involved? (2017). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

FINTEAM: Trojanized TeamViewer Against Government Targets (2019). Source: Check Point. Link: https://research.checkpoint.com/finteam-trojanized-teamviewer-against-government-targets/

First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group (2020). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.01.06.SideWinder_Google_Play/First%20Active%20Attack%20Exploiting%20CVE-2019-2215%20Found%20on%20Google%20Play%2C%20Linked%20to%20SideWinder%20APT%20Group.pdf

Flame 2.0: Risen from the Ashes (2019). Source: Chronicle. Link: https://storage.googleapis.com/chronicle-research/Flame%202.0%20Risen%20from%20the%20Ashes.pdf

Flash 0-Day In The Wild: Group 123 At The Controls (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/02/group-123-goes-wild.html

Flash zero-day exploit deployed by the ScarCruft APT Group (2016). Source: Kaspersky Lab. Link: https://app.box.com/s/0vp77yw58zhqmt9xoez6f7nmicbgkqrw

Flying Kitten to Rocket Kitten, a Case of Ambiguity and Shared Code (2017). Source: Claudio Guarnieri e Collin Anderson. Link: https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/

Flying Kitten: From Defacements to Industrial Espionage (2018). Source: Claudio Guarnieri e Collin Anderson. Link: https://iranthreats.github.io/resources/notes-flying-kitten/

Follow the money: Dissecting the operations of the cyber crime group FIN6 (2016). Source: FireEye. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/rpt-fin6.pdf

Following the Trail of BlackTech's Cyber Espionage Campaigns (2017). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/

FOLLOWING THE TURLA'S SKIPPER OVER THE OCEAN OF CYBER OPERATIONS (2019). Source: Telsy. Link: https://blog.telsy.com/following-the-turlas-skipper-over-the-ocean-of-cyber-operations/

For Their Eyes Only: The Commercialization of Digital Spying (2013). Source: Citizen Lab. Link: https://citizenlab.ca/2013/04/for-their-eyes-only-2/

Forced To Adapt: Xslcmd Backdoor Now On Os X (2014). Source: FireEye. Link: https://app.box.com/s/fc2gc8m4ospivuhzjmj2vfc1l3sxc17j

Foreign Cyber Threats to the United States (2017). Source: US Senate. Link: https://www.threatminer.org/_reports/2017/Clapper-Lettre-Rogers_01-05-16.pdf

Forkmeiamfamous: Seaduke, Latest Weapon In The Duke Armory (2015). Source: Symantec. Link: http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory

From AGENT.BTZ to COMRAT V4. A ten-year journey (2020). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5219890908375287908.pdf

From Bahrain With Love: Finfisher Spy Kit Exposed? (2012). Source: Citizen Lab. Link: https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

From BlackEnergy to ExPetr (2017). Source: Kaspersky Lab. Link: https://app.box.com/s/n13ohbzc6qkod8yqxay19pnltnecchev

From Cybercrime to Political Repression Shedding Light on the Iranian Cyber Army (2018). Source: Claudio Guarnieri e Collin Anderson. Link: https://blog.domaintools.com/2018/01/from-cybercrime-to-political-repression-shedding-light-on-the-iranian-cyber-army/

From Espionage to Cyber Propaganda: Pawn Storm's Activities over the Past Two Years (2017). Source: Trend Micro. Link: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm

From Georgia, with Love (2012). Source: ESET WeLiveSecurity. Link: http://blog.eset.com/2012/03/21/win32georbot-information-stealing-trojan-botnet-from-georgia-with-love

From HummingBad to Worse (2016). Source: Check Point. Link: http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf

From Seoul to Sony: The History of the Darkseoul group and the Sony intrusion malware Destover (2016). Source: Blue Coat Systems. Link: https://app.box.com/s/xyyord0b806e6or2nh92coxw2areyyx4

From Shamoon to StoneDrill (2017). Source: Kaspersky Lab. Link: https://www.threatminer.org/_reports/2017/Report_Shamoon_StoneDrill_final - Kaspersky Lab.pdf

From tweet to rootkit (2019). Source: Exatrack. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/winnti_EN.pdf

FrozenCell: Multi-platform surveillance campaign against Palestinians (2017). Source: Lookout. Link: https://blog.lookout.com/frozencell-mobile-threat

Full Discloser of Andariel,A Subgroup of Lazarus Threat Group (2020). Source: AhnLab. Link: https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus%20(3).pdf

Full Disclosure Of Havex Trojans (2014). Source: NETRESEC. Link: https://app.box.com/s/v76ozenghvxl8cnk7rcdw4dxsnsffz2g

Fully equipped Spying Android RAT from Brazil: BRATA (2019). Source: Kaspersky Lab. Link: https://securelist.com/spying-android-rat-from-brazil-brata/92775/

GALLIUM: Targeting global telecom (2019). Source: Microsoft. Link: https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

Gallmaker: New Attack Group Eschews Malware to Live off the Land (2018). Source: Symantec. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.10.11.Gallmaker/Gallmaker%20New%20Attack%20Group%20Eschews%20Malware%20to%20Live%20off%20the%20Land.pdf

Gamaredon Activity (2019). Source: Anomali. Link: https://www.anomali.com/files/white-papers/Anomali_Threat_Research-Gamaredon_TTPs_Target_Ukraine-WP.pdf

Gamaredon APT Group Use Covid-19 Lure in Campaigns (2020). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/gamaredon-apt-group-use-covid-19-lure-in-campaigns

GAME OVER: Detecting and Stopping an APT41 Operation (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html

Games Are Over: Winnti Is Now Targeting Pharmaceutical Companies (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/f090ea4pi40hoaxe6otzfw7yl65ylw6y

Gaming industry still in the scope of attackers in Asia (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/

GandCrab and Ursnif Campaign (2019). Source: Carbon Black. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.01.24.GandCrab_and_Ursnif/GandCrab%20and%20Ursnif%20Campaign.pdf

Gangnam Industrial Style: APT Campaign Targets Korean Industrial Companies (2019). Source: CyberX. Link: https://cyberx-labs.com/blog/gangnam-industrial-style-apt-campaign-targets-korean-industrial-companies/

Gathering In The Middle East, Operation Stteam (2014). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/ine4z2lyf8ryqao789oc0als335iip8c

Gauss: Abnormal Distribution (2012). Source: Kaspersky Lab. Link: https://app.box.com/s/y0wmp82qdqivrx4x21nfj5miod1tjuf1

Gaza Cybergang – updated activity in 2017 (2017). Source: Kaspersky Lab. Link: https://securelist.com/gaza-cybergang-updated-2017-activity/82765/

Gaza Cybergang Group1, operation SneakyPastes (2019). Source: Kaspersky Lab. Link: https://securelist.com/gaza-cybergang-group1-operation-sneakypastes/90068/

Gazing at Gazer (2017). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/sqiber6gp1q75h6r4eq89fjeeur2mz8h

GCHQ intercepted foreign politicians' communications at G20 summits (2013). Source: Open Source. Link: https://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

Geopolitical strategy of Iran and the cyberattacks of APT33 (2019). Source: S2 Grupo. Link: https://lab52.io/blog/geopolitical-strategy-of-iran-and-the-cyberattacks-of-apt33/

GEOST Botnet. The story of the discovery of a new Android Banking trojan from an OPSEC error (2019). Source: Virus Bulletin. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/VB2019-Garcia-etal.pdf

German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed (2020). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

Gholee Protective Edge Themed Spear Phishing Campaign (2014). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/krnvva7fu9o6ywa81uwbpsasj4sz3y2n

Giving Fraudsters the Cold Shoulder: Inside the Largest Connected TV Bot Attack (2020). Source: White Ops. Link: https://www.whiteops.com/blog/giving-fraudsters-the-cold-shoulder-inside-the-largest-connected-tv-bot-attack

GlitchPOS: New PoS malware for sale (2019). Source: Cisco Talos. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.13.GlitchPOS_POS_Malware/GlitchPOS_New_Pos_Malwre_for_sale.pdf

"Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

(2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html"

Global Energy Cyberattacks: Night Dragon (2011). Source: Intel Security-McAfee. Link: https://app.box.com/s/o2tc88oihh4c67a0s8ygok9fwd66zp71

Global Iranian Disinformation Operation (2018). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/global-iranian-disinformation-operation/

Global Oil and Gas Cyber Threat Perspective (2019). Source: Dragos. Link: https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf

Global Threat Intel Report (2015). Source: CrowdStrike. Link: https://app.box.com/s/xbbiyzpb3614bdaxuu3rs96n7f4ysppa

Global Threat Report: “Adversary Tradecraft and the Importance of Speed” (2019). Source: CrowdStrike. Link:

Glupteba Campaign Hits Network Routers and Updates C&C Servers with Data from Bitcoin Transactions (2019). Source: Trend Micro. Link: https://www.trendmicro.com/en_us/research/19/i/glupteba-campaign-hits-network-routers-and-updates-cc-servers-with-data-from-bitcoin-transactions.html

Goblin Panda against the Bears (2018). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/gobelin-panda-against-the-bears-1f462d00e3a4

Goblin Panda changes the dropper and reuses the old infrastructure (2018). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/goblin-panda-changes-the-dropper-and-reused-the-old-infrastructure-a35915f3e37a

Goblin Panda targets Cambodia sharing capacities with another Chinese group hackers Temp Periscope (2018). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/goblin-panda-targets-cambodia-sharing-capacities-with-another-chinese-group-hackers-temp-periscope-7871382ffcc0

Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victims’ Systems (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Golden Chickens: Uncovering A Malware-as-a-Service (MaaS) Provider and Two New Threat Actors Using It (2018). Source: QuoScient. Link: https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Golden Eagle (APT-C-34) (2019). Source: 360 SkyEye System. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.20.Golden_Eagle_APT-C-34/APT-C-34.cn.pdf

Golden Rat Organization - Targeted Attacks in Syria (2017). Source: 360 SkyEye System. Link: http://blogs.360.cn/post/%E9%BB%84%E9%87%91%E9%BC%A0%E7%BB%84%E7%BB%87-%E5%8F%99%E5%88%A9%E4%BA%9A%E5%9C%B0%E5%8C%BA%E7%9A%84%E5%AE%9A%E5%90%91%E6%94%BB%E5%87%BB%E6%B4%BB%E5%8A%A8.html

Goldfin Security Alert (2018). Source: Accenture. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.08.02.Goldfin_Security_Alert/Accenture-Goldfin-Security-Alert-1.pdf

Gorgon APT targeting MSME sector in India (2020). Source: Seqrite. Link: https://www.seqrite.com/blog/gorgon-apt-targeting-msme-sector-in-india/

GOZNYM MALWARE target US, AT, DE (2016). Source: Team Cymru. Link: https://blog.team-cymru.org/2016/05/goznym-malware/

GOZNYM MALWARE: CYBERCRIMINAL NETWORK DISMANTLED IN INTERNATIONAL OPERATION (2019). Source: Europol. Link: https://www.europol.europa.eu/article-types/press-release

Grabit And The Rats (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/x7jlktifxatv3oam1altle8km1xwju7b

Grandoreiro: How engorged can an EXE get? (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

GravityRAT - The Two-Year Evolution Of An APT (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

Greenbug cyberespionage Group (2017). Source: Symantec. Link: https://www.threatminer.org/_reports/2017/Greenbug cyberespionage group targeting Middle East, possible links to Shamoon - Symantec.pdf

GREYENERGY A successor to BlackEnergy (2018). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/ESET_GreyEnergy.pdf

GreyEnergy: Dissecting the Malware from Maldoc to Backdoor (2019). Source: Nozomi. Link:

GreyEnergy: Updated arsenal of one of the most dangerous threat actors (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

GreyEnergy’s overlap with Zebrocy (2019). Source: Kaspersky Lab. Link: https://securelist.com/greyenergys-overlap-with-zebrocy/89506/

GRIZZLY STEPPE - Russian Malicious Cyber Activity (2016). Source: US-CERT. Link: https://app.box.com/s/5q1827f6ig94an0buhsk9i8k7e0eju8w

Group 123 (2018). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

Group 123 (2017). Source: Cisco Talos. Link: https://www.threatminer.org/_reports/2017/Korean MalDoc Drops Evil New Years Presents - Talos.pdf

Group5: Syria and the Iranian Connection (2016). Source: Citizen Lab. Link: https://app.box.com/s/2475tuv4oigvtrdy1jx6p2lct9ebzlcb

Guccifer 2.0: All Roads Lead to Russia (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/guccifer-2-all-roads-lead-russia/

Guccifer 2.0: the Man, the Myth, the Legend? (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/reassesing-guccifer-2-0-recent-claims/

Guccifer Rising? Months-Long Phishing Campaign on ProtonMail Targets Dozens of Russia-Focused Journalists and NGOs (2019). Source: Bellingcat. Link: https://www.bellingcat.com/news/uk-and-europe/2019/08/10/guccifer-rising-months-long-phishing-campaign-on-protonmail-targets-dozens-of-russia-focused-journalists-and-ngos/

Guildma: The Devil drives electric (2020). Source: ESET WeLiveSecurity. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.05_Guildma/Guildma_%20The%20Devil%20drives%20electric%20_%20WeLiveSecurity.pdf

GuLoader? No, CloudEyE (2020). Source: Check Point. Link: https://research.checkpoint.com/2020/guloader-cloudeye/

Hack ATM with an anti-hacking feature and walk away with $1M in 2 minutes (2017). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Hack-ATM-with-an-anti-hacking-feature-and-walk-away-with-1M-in-2-minutes.pdf

Hacker Group Creates Network of Fake LinkedIn Profiles (2015). Source: Dell Secureworks. Link: https://app.box.com/s/w32vcrjpq3fj0fg0t8c5gwmy0olwnmnd

Hackers acting in Turkey's interests believed to be behind recent cyberattacks (2020). Source: Reuters. Link: https://www.reuters.com/article/us-cyber-attack-hijack-exclusive-idUSKBN1ZQ10X

Hacking Group Spies on Android Users in India Using PoriewSpy (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-group-spies-android-users-india-using-poriewspy/

Hacking Team and the Targeting of Ethiopian Journalists (2014). Source: Citizen Lab. Link: https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/

Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware (2015). Source: Citizen Lab. Link: https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/

Hacking Team's US Nexus (2014). Source: Citizen Lab. Link: https://citizenlab.org/2014/02/hacking-teams-us-nexus/

Hacking The Street? Fin4 Likely Playing The Market (2014). Source: FireEye. Link: https://app.box.com/s/56mtum85h5pznvw9r4x6yh5qivb7vgql

Hacktivism: India vs. Pakistan (2016). Source: Recorded Future. Link: https://www.recordedfuture.com/india-pakistan-cyber-rivalry/

Hagga of SectorH01 continues abusing Bitly, Blogger and Pastebin to deliver RevengeRAT and NanoCore (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/09/19/sectorh01-continues-abusing-web-services/

Hainan Xiandun Technology Company is APT40 (2020). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2020/01/15/hainan-xiandun-technology-company-is-apt40/

Hamas Android Malware On IDF Soldiers-This is How it Happened (2020). Source: Check Point. Link: https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/

Hammertoss: Stealthy Tactics Define A Russian Cyber Threat Group (2015). Source: FireEye. Link: https://app.box.com/s/xqp6s3fb8w65f6mkm1zc89ftrl8lyfw7

Hands in the MuddyWater – Playing with Iranian Cyber-Espionage Campaign (2018). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/muddywater-apt/

HatMan—Safety System Targeted Malware (2018). Source: US-CERT. Link: https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF

Have I Got Newsforyou: Analysis Of Flamer C&C Server (2012). Source: Symantec. Link: https://app.box.com/s/6ujt4gi1c962id9o4iviesurww2grbxi

Hello! My name is Dtrack (2019). Source: Kaspersky Lab. Link: https://securelist.com/my-name-is-dtrack/93338/

Hellsing Indicators Of Compromise (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/ralrn76f32axakdv2fdl4kwtxqxvwee8

HELO Winnti: Attack or Scan? (2019). Source: lastline. Link: https://www.lastline.com/labsblog/helo-winnti-attack-scan/

HenBox: Inside the Coop (2018). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/unit42-henbox-inside-coop/

HenBox: The Chickens Come Home to Roost (2018). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

HERE WE GO: CRIMEWARE VIRUS & APT JOURNEY FROM "ROBBINHOOD" TO APT28 (2019). Source: SentinelOne. Link: https://www.sentinelone.com/blog/here-we-go-crimeware-apt-journey-from-robbinhood-to-apt28/

Here's the Evidence That Links Russia's Most Brazen Cyberattacks (Sandworm) (2019). Source: Wired. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/Evidence_That_Links_Russias_Most_Brazen_Cyberattacks_112019.pdf

HIDDEN COBRA – FASTCash Campaign (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA18-275A

HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA18-149A

Hidden Cobra – North Korea's DDoS Botnet Infrastructure (2017). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA17-164A

HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL (2017). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA17-318A

"HIDDEN COBRA – North Korean Trojan: Volgmer

(2017). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA17-318B"

Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

Hidden Lynx: Professional Hackers For Hire (2013). Source: Symantec. Link: https://app.box.com/s/m7yxjl7nljw2iltpbasm7t2dswhya6iv

HiddenWasp Malware Stings Targeted Linux Systems (2019). Source: Intezer. Link: https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/

HIDE AND SEEK Tracking NSO Groups Pegasus Spyware to Operations in 45 Countries (2018). Source: Citizen Lab. Link: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Hide and Seek: How Threat Actors Respond in the Face of Public Exposure (2016). Source: RSA Security. Link: https://www.rsaconference.com/writable/presentations/file_upload/tta1-f04_hide-and-seek-how-threat-actors-respond-in-the-face-of-public-exposure.pdf

Hiding in plain sight: FireEye and Microsoft expose obfuscation tactic (2015). Source: FireEye. Link: https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf

Higaisa APT (2019). Source: Tencent. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.04.Higaisa_APT/(cn)_higaisa_apt_report.pdf

Higaisa or Winnti? APT41 backdoors, old and new (2021). Source: Positive Research. Link: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor (2020). Source: FireEye. Link: https://www.fireeye.com/blog/threat-

research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Hikit Analysis (2014). Source: Novetta. Link: https://app.box.com/s/k1zaybbj4ickaq5u0flu9bpmtp8a1e5k

HOGFISH REDLEAVES CAMPAIGN (2018). Source: Accenture. Link: https://www.accenture.com/t20180423T055005Z__w__/us-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf

Hong Kong SWC attack (2015). Source: Dragon Threat Labs. Link: http://blog.dragonthreatlabs.com/2015/01/dtl-12012015-01-hong-kong-swc-attack.html

Hostile state actors compromising UK organisations with focus on engineering and industrial control companies (2018). Source: National Cyber Security Centre. Link: https://www.ncsc.gov.uk/alerts/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control

Houdini's Magic Reappearance (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/y4zzbao34iv483op59h1dettrwgoe7li

How an Entire Nation Became Russia's Test Lab for Cyberwar (Sandworm) (2017). Source: Wired. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/How_an_Entire_Nation_Became_Russias_Test_Lab_for_Cyberwar_062017.pdf

How Can I Tell If I Was Infected By Aurora? (2010). Source: Intel Security-McAfee. Link: https://app.box.com/s/k0qidf9g1yfehi6pbdodmcxdqag5a9bv

How China Will Use Cyber Warfare (2008). Source: Jason Fritz. Link: https://app.box.com/s/696xnzy1an3jbm3b212y5n8xieirbemd

How North Korea Revolutionized the Internet as a Tool for Rogue Regimes (2020). Source: Recorded Future. Link: https://www.recordedfuture.com/north-korea-internet-tool/

How Tortoiseshell created a fake veteran hiring website to host malware (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html

How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet (2019). Source: CrowdStrike. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/huge-fan-of-your-work-intelligence-report.pdf

Htran And The Advanced Persistent Threat (2011). Source: Dell Secureworks. Link: https://app.box.com/s/aqhzvj2a5vo91dgqjflh7nk4pm8aowon

Huge Fan of Your Work: How TURBINE PANDA and China’s Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet — Part I (2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/huge-fan-of-your-work-part-1/

Hungry for data, ModPipe backdoor hits POS software used in hospitality sector (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/

Hunting Libyan Scorpions (2016). Source: Cyberkov Security. Link: https://app.box.com/s/pov6xl0nvac5iaq4kafyw7p8ylmx3p8d

Hunting The Shadows: In Depth Analysis Of Escalated Apt Attacks (2013). Source: Xecure Lab. Link: https://app.box.com/s/owi5dxkk3zx164lp90swu3weeyp805se

Hussarini – Targeted Cyber Attack in the Philippines (2018). Source: Fortinet. Link: https://www.fortinet.com/blog/threat-research/hussarini---targeted-cyber-attack-in-the-philippines.html

I Am Ironman: Deep Panda Uses Sakula Malware To Target Organizations In Multiple Sectors (2014). Source: CrowdStrike. Link: http://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/

I know what you did last summer, MuddyWater blending in the crowd (2019). Source: Kaspersky Lab. Link: https://securelist.com/muddywaters-arsenal/90659/

ICAO victim of a major cyberattack in 2016 (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/03/01/icao-victim-major-cyberattack-2016/

Iexpl0Re Rat (2012). Source: Citizen Lab. Link: https://app.box.com/s/tdgkyqg7o511v8a29mc8ec28yxzw118j

Ikittens: Iranian Actor Resurfaces with Malware For Mac (2017). Source: Claudio Guarnieri e Collin Anderson. Link: https://iranthreats.github.io/resources/macdownloader-macos-malware/

Illuminating The Etumbot Apt Backdoor (2014). Source: Arbor Networks. Link: https://app.box.com/s/h8c0ds5etxke111s38r7rs3ltmpf2mot

Imminent Monitor – a RAT Down Under (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

Impact Of Alleged Russian Cyber Attack (2009). Source: William C. Ashmore. Link: https://app.box.com/s/4q3ws8a3ymx6y4ygsp4k4zm8gx0imsy0

In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia (2015). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

In the Balkans, businesses are under fire from a double-barreled weapon (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+eset%2Fblog+%28ESET+Blog%3A+We+Live+Security%29

IN THE TRAILS OF WINDSHIFT APT (2018). Source: DarkMatter. Link: https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf

In-depth analysis of CVE-2018-5002 exploit technology (2018). Source: 360 SkyEye System. Link: http://blogs.360.cn/post/indepth_CVE-2018-5002.html

In-Depth Analysis Of Hydraq: The Face Of Cyberwar Enemies Unfolds (2010). Source: CA Technologies. Link: https://app.box.com/s/44e7rbs177n5inhpm9si6gu3lm7fw6bj

Inception Attackers Target Europe with Year-old Office Vulnerability (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/11/unit42-inception-attackers-target-europe-year-old-office-vulnerability/

Inception Framework: Alive and Well, and Hiding Behind Proxies (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies

Incident Response lessons from recent Maze ransomware attacks (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html

Increased Use of Malware Target Journalists (2016). Source: Claudio Guarnieri e Collin Anderson. Link: https://iranthreats.github.io/resources/android-malware/

India: Human Rights Defenders Targeted by a Coordinated Spyware Operation (2020). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/

Indian organizations targeted in Suckfly attacks (2016). Source: Symantec. Link: https://app.box.com/s/nekeu5y0v2yk4rdwpuq8y1ahyyuaduen

Indian Space Research Organization (ISRO) was attacked by North Korean APT (2019). Source: 360 SkyEye System. Link: http://www.360.cn/n/11286.html

Indictment of PLA officers (2014). Source: US Justice Department. Link: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Industrial Control System Threats (2018). Source: Dragos. Link: https://www.dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf

Industroyer: Biggest threat to industrial control systems since Stuxnet (2017). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Inexsmar: An unusual DarkHotel campaign (2017). Source: BitDefender. Link: https://app.box.com/s/mlbeyha2vu6a5b8ystgdk6fdew4f6r98

Information Controls during Thailand's 2014 Coup (2014). Source: Citizen Lab. Link: https://citizenlab.ca/2014/07/information-controls-thailand-2014-coup/

Information Controls Yemen (2015). Source: Citizen Lab. Link: https://citizenlab.ca/2015/10/information-controls-military-operations-yemen/

Infrastructure and Samples of Hamas' Android Malware Targeting Israeli Soldiers (2018). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/glancelove/

Inside Report _ Apt Attacks On Indian Cyber Space (2013). Source: Infosec Consortium. Link: https://app.box.com/s/a2zw9uye2hhofsc1me6yfj39u6gjalcq

Inside The Equationdrug Espionage Platform (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/vdy6lfmpvu6gzglsc3d7sade6tp9gi7e

Inside the Hacking Community Market – Reselling RIG EKServices (2019). Source: Check Point. Link: https://research.checkpoint.com/inside-the-hacking-community-market-reselling-rig-ek-services/

Inside the Spyware Campaign Against Argentine Troublemakers (2015). Source: The Intercept. Link: https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/

Inside the UAE's secret hacking team of U.S. mercenaries (2019). Source: Reuters. Link: https://www.reuters.com/article/us-usa-spying-raven-specialreport/special-report-inside-the-uaes-secret-hacking-team-of-u-s-mercenaries-idUSKCN1PO19O

Insight In To A Strategic Web Compromise And Attack Campaign Against Hong Kong Infrastructure (2015). Source: Dragon Threat Labs. Link: https://app.box.com/s/9bt05cgrk8vbmylm5odno0k85s39kny0

Insight in to advances of adversary tactics, techniques and procedures through analysis of an attack against an organisation in the Asia Pacific regio (2015). Source: Dragon Threat Labs. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2015/DTL-06282015-01.pdf

Insights from one year of tracking a polymorphic threat: Dexphot (2019). Source: Microsoft. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.26.Dexphot/Insights%20from%20one%20year%20of%20tracking%20a%20polymorphic%20threat.pdf

Intelligence Games in the Power Grid (2017). Source: Treadstone 71. Link: https://treadstone71llc.files.wordpress.com/2017/09/intelligence-games-in-the-power-grid-2016.pdf

Intelligence operation against targets in Indonesia (2020). Source: S2 Grupo. Link: https://lab52.io/blog/intelligence-operation-against-targets-in-indonesia/

Interference with NASA satellite Landsat 7 (2011). Source: Arbor Networks. Link: https://web.archive.org/web/20111124012100/http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf

International Security and Estonia (2020). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/raport-2020-en.pdf

Internet Explorer and Windows zero-day exploits used in Operation PowerFall (2020). Source: Kaspersky Lab. Link: https://securelist.com/ie-and-windows-zero-day-operation-powerfall/97976/

Into the Fog – The Return of ICEFOG APT (2018). Source: FireEye. Link: https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt

"Introducing BIOLOAD: FIN7 BOOSTWRITE's Lost Twin

(2019). Source: Fortinet. Link: https://www.fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin.html"

Introducing Blue Mockingbird (2020). Source: RedCanary. Link: https://redcanary.com/blog/blue-mockingbird-cryptominer/

Introducing ROKRAT (2017). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2017/04/introducing-rokrat.html

Introducing WhiteBear (2017). Source: Kaspersky Lab. Link: https://app.box.com/s/ck26ekr69wmhxk6hyii507o09p20eixs

Intruder File Report- Sneakernet Trojan (2014). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/yvbehxsn3tknzogt74z9ryn7r7elwpmf

Intrusions Affecting Multiple Victims Across Multiple Sectors (2017). Source: US-CERT. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/IR-ALERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf

Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware (2017). Source: Citizen Lab. Link: https://citizenlab.ca/2017/07/mexico-disappearances-nso/

Investigation with a twist: an accidental APT attack and averted data destruction (2020). Source: Positive Technologies. Link: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/

Investigation: WannaCry cyber attack and the NHS (2017). Source: National Cyber Security Centre. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

InvisiMole: Surprisingly equipped spyware, undercover since 2013 (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

Iran and the Soft War for Internet Dominance (2016). Source: Claudio Guarnieri e Collin Anderson. Link: https://iranthreats.github.io/resources/human-rights-impersonation-malware/

Iran-based attackers use back door threats to spy on Middle Eastern targets (2015). Source: Symantec. Link: https://app.box.com/s/oeix6b4jcwdkwyrzq35brtmq2ktoyxnw

Iran's Cyber Threat: Espionage Sabotage and Revenge (2018). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/Iran_Cyber_Final_Full_v2.pdf

Iran’s Hacker Hierarchy Exposed (2018). Source: Recorded Future. Link: https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf

Iranian APT group MuddyWater Adds Exploits to Their Arsenal Jun (2019). Source: ClearSky Cybersecurity . Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/Clearsky-Iranian-APT-group-MuddyWater-Adds-Exploits-to-Their-Arsenal.pdf

Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia (2020). Source: BitDefender. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5348093092295608246.pdf

Iranian Cyber Response to Death of IRGC Head Would Likely Use Reported TTPs and Previous Access (2020). Source: Recorded Future. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.01.07_Iranian_Cyber_Response/Iranian%20Cyber%20Response%20to%20Death%20of%20IRGC%20Head%20Would%20Likely%20Use%20Reported%20TTPs%20and%20Previous%20Access.pdf

IRANIAN EXPOSURE – OILRIG HACKERS OUTED (2019). Source: Treadstone 71. Link: https://cybershafarat.com/category/cyber-intelligence-common-body-of-knowledge/

Iranian Fileless Attack Infiltrates Israeli Organizations (2017). Source: Morphisec. Link: http://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability

Iranian Nation State Interdiction - OilRig (2017). Source: TrapX Security. Link: https://deceive.trapx.com/WPAOAOilRig_210LandingPage.html

Iranian Nation-State APT Groups - "Black Box" Leak (2019). Source: ClearSky Cybersecurity . Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf

Iranian PupyRAT Bites Middle Eastern Organizations (2017). Source: Dell Secureworks. Link: https://app.box.com/s/ztp64lp34bn9ax4vithevntn6pab6sxz

Iranian Threat Actor Amasses Large Cyber Operations Infrastructure Network to Target Saudi Organizations (2019). Source: Recorded Future. Link: https://www.recordedfuture.com/iranian-cyber-operations-infrastructure/

Iranian Threat Agent Greenbug Impersonates Israeli High-Tech and Cyber Security Companies (2017). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/fga01c36ebgqga5ic0a4o73j5jq9vdvr

Iranian Threat Agent OilRig Delivers Digitally Signed Malware (2017). Source: ClearSky Cybersecurity . Link: https://www.threatminer.org/_reports/2017/Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford _ ClearSky Cybersecurity.pdf

Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

Irans Hacker Hierarchy Exposed (2018). Source: Recorded Future. Link: https://www.recordedfuture.com/iran-hacker-hierarchy/

Iraq Information Controls Update: Analyzing Internet Filtering and Mobile Apps (2014). Source: Citizen Lab. Link: https://citizenlab.ca/2014/06/monitoring-information-controls-in-iraq/

Iron Cybercrime Group Under The Scope (2018). Source: Intezer. Link: https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

IRON TWILIGHT Supports Active Measures (2017). Source: Dell Secureworks. Link: https://www.threatminer.org/_reports/2017/IRON TWILIGHT Supports Active Measures - SecureWork.pdf

IRONGATE ICS Malware: Nothing to See Here...Masking Malicious Activity on SCADA Systems (2016). Source: FireEye. Link: https://app.box.com/s/6s871m2xa63x4ru8glto9crcv6kk8jor

IronPython, darkly: how we uncovered an attack on government entities in Europe (2019). Source: Positive Technologies. Link: http://blog.ptsecurity.com/2019/07/ironpython-darkly-how-we-uncovered.html

Is Babar a Bunny? (2015). Source: F-Secure. Link: https://www.f-secure.com/weblog/archives/00002794.html

Is Emotet gang targeting companies with external SOC? (2019). Source: Marco Ramilli. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.10.1

4.Emotet_external_SOC/Is%20Emotet%20gang%20targeting%20companies%20with%20external%20SOC.pdf

Is Lazarus/APT38 Targeting Critical Infrastructures (2019). Source: Marco Ramilli. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.04.Lazarus_APT38/Is%20Lazarus_APT38%20Targeting%20Critical%20Infrastructures%20_%20%E2%80%93%20Marco%20Ramilli%20Web%20Corner.pdf

IT IS IDENTIFIED ATTACKS OF THE CIBERCRIMINAL LAZARUS GROUP DIRECTED TO ORGANIZATIONS IN RUSSIA (2019). Source: Secure Soft. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.02.20.LAZARUS_to_RUSSIA/LAZARUS%20GROUP%20DIRECTED%20TO%20ORGANIZATIONS%20IN%20RUSSIA_google_translate.pdf

It's alive: Threat actors cobble together open-source pieces into monstrous Frankenstein campaign (2016). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

It'S Not The End Of The World: Darkcomet Misses By A Mile (2012). Source: Arbor Networks. Link: https://app.box.com/s/akmz317h8dkapm52ksycf187rw2ylp21

It's Parliamentary: KeyBoy and the targeting of the Tibetan Community (2016). Source: Citizen Lab. Link: https://app.box.com/s/q7rywbgt6s5c380vvjpk643ppcdtdl8v

ITSecTeam (2012). Source: Open Source. Link: http://pastebin.com/mCHia4W5

Ixeshe An Apt Campaign (2012). Source: Trend Micro. Link: https://app.box.com/s/t74crjmu21ee2gpnnx56182bj74facvi

IXESHE Derivative IHEATE Targets Users in America (2016). Source: Trend Micro. Link: https://app.box.com/s/8glps1qnq0glc2c2b2wsmeb4019f9wpd

Jaku: an on-going botnet campaign (2016). Source: Forcepoint. Link: https://www.forcepoint.com/sites/default/files/resources/files/report_jaku_analysis_of_botnet_campaign_en_0.pdf

Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign (2020). Source: Symantec. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.11.17.Cicada_Japan/Japan-Linked%20Organizations%20Targeted%20in%20Long-Running%20and%20Sophisticated%20Attack%20Campaign%20_%20Symantec%20Blogs.pdf

Jerusalem Post and other Israeli websites compromised by Iranian threat agent CopyKitten (2017). Source: ClearSky Cybersecurity . Link: https://www.threatminer.org/_reports/2017/Jerusalem Post and other Israeli websites compromised by Iranian threat agent CopyKitten _ ClearSky Cybersecurity.pdf

"JhoneRAT: Cloud based python RAT targeting Middle

Eastern countries (2020). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2020/01/jhonerat.html"

JOLLY ROGER'S PATRONS (2020). Source: Group-IB. Link: https://www.group-ib.com/resources/threat-research/black-jack.html

jRAT += Houdini: New Year 2019 (2019). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/jrat-again-with-the-magic-of-houdini/

JUPYTER INFOSTEALER (2020). Source: Morphisec. Link: https://blog.morphisec.com/jupyter-infostealer-backdoor-introduction

KASPERAGENT Malware Campaign resurfaces in May Election (2017). Source: ThreatConnect. Link: https://app.box.com/s/vye9qg0l3u5180jk03mwul4p7wlc3gvo

Kaspersky's report on The Regin Platform (2014). Source: Kaspersky Lab. Link: http://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/

Kazuar: Multiplatform Espionage Backdoor with API Access (2017). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-acces

Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents (2016). Source: Citizen Lab. Link: https://app.box.com/s/is08b06f6fj6a9z6wymf4u5y5xjm6opr

Keyboy, Targeted Attacks Against Vietnam And India (2013). Source: Rapid7. Link: https://app.box.com/s/f8p3dagvmdezcpgmnh04mgqz21viklpz

KHRAT Malware Used in Cambodia Attacks (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/

"Kim Soo Ki Organization, Korea Cryptographic Exchange Event Impersonation APT Attack

(2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2336"

Kimsuky Organization, Operation Stealth Power Silence Operation (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2234

Kimsuky unveils APT campaign 'Smoke Screen' aimed at Korea and America (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2243

KingSlayer A Supply chain attack (2017). Source: RSA Security. Link: https://www.threatminer.org/_reports/2017/kingslayer-a-supply-chain-attack(02-03-2017).pdf

Know Your Enemies 2.0: A Primer on Advanced Persistent Threat Groups (2016). Source: Institute for Critical Infrastructure Technology (ICIT). Link: https://app.box.com/s/kj9eyf73oh2hi8zum6a8lygzqb5jhsm7

KONNI: A Malware Under The Radar For Years (2017). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html

KopiLuwak: A New JavaScript Payload from Turla (2017). Source: Kaspersky Lab. Link: https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/

Korean MalDoc Drops Evil New Years Presents (2017). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2017/02/korean-maldoc.html

Korplug Military Targeted Attacks: Afghanistan & Tajikistan (2014). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/jih94kv82ucn12fdne8tsijvwn06cf4p

Kuwait Oil Themed Malware Targeting Industry (2019). Source: MalCrawler. Link: https://www.malcrawler.com/kuwait-oil-themed-malware-targeting-industry/

LATAM Financial Cybercrime: Competitors-in-crime sharing TTPs (2020). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5454144652401707099.pdf

Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.07.04.TA505_Gelup_FlowerPippi/Appendix-Latest-Spam-Campaigns-from-TA505-Now-Using-New-Malware-Tools-Gelup-and-FlowerPippi.pdf

Latest Target Attack of DarkHydruns Group Against Middle East (2019). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/

Latest Trickbot Campaign Delivered via Highly Obfuscated JS File (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.05.Trickbot_Obfuscated_JS/Latest%20Trickbot%20Campaign%20Delivered%20via%20Highly%20Obfuscated%20JS%20File%20.pdf

Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware (2017). Source: Citizen Lab. Link: https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/

Lazarus & Watering-Hole Attacks (2017). Source: BAE Systems Detica. Link: https://www.threatminer.org/_reports/2017/LAZARUS & WATERING-HOLE ATTACKS - BAE Systems.pdf

Lazarus Arisen - article (2017). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/LAZARUS_ARISEN.pdf

Lazarus Arisen: Architecture, Techniques and Attribution (2017). Source: Group-IB. Link: http://www.group-ib.com/lazarus.html

Lazarus Campaign Targeting Cryptocurrencies (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/

Lazarus Continues Heists, Mounts Attacks on Financial Organizations in Latin America (2018). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.11.20.lazarus-in-latin-america/blog.trendmicro.com-Lazarus%20Continues%20Heists%20Mounts%20Attacks%20on%20Financial%20Organizations%20in%20Latin%20America.pdf

Lazarus covets COVID-19-related intelligence (2020). Source: Kaspersky Lab. Link: https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/

Lazarus Group Targets More Cryptocurrency Exchanges and FinTech Companies (2018). Source: Intezer. Link: http://www.intezer.com/lazarus-group-targets-more-cryptocurrency-exchanges-and-fintech-companies/

LAZARUS GROUP: Campaign Targetting The Cryptocurrenct Vertical (2020). Source: F-Secure. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5343537399009904368.pdf

Lazarus supply chain attack in South Korea (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

Lazarus Under The Hood (2017). Source: Kaspersky Lab. Link: https://app.box.com/s/np8kzut76ruc8whb32v7jpexx4bils6z

Lazarus: History of mysterious group behind infamous cyber attacks (2017). Source: Symantec. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Lazarus.pdf

Lazarus' False Flag Malware (2017). Source: BAE Systems Detica. Link: https://www.threatminer.org/_reports/2017/LAZARUS FALSE FLAG MALWARE - BAE Systems.pdf

Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Leery Turtle Threat Report (2020). Source: CyberStruggle. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/LeeryTurtleThreatReport_05_20.pdf

LeetMX – a Yearlong Cyber-Attack Campaign Against Targets in Latin America (2017). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/leetmx/

Legit remote admin tools turn into threat actors tools (2019). Source: CyberInt. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/CyberInt_Legit.pdf

Leouncia And Orcarat (2014). Source: Airbus Defence and Space. Link: https://app.box.com/s/737gsokqbgsi9d6yenyob3kgafl8mrc4

LESSONS FROM OPERATION RUSSIANDOLL (2016). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2016/03/lessons-from-operation-russian-doll.html

Let It Ride: The Sofacy Group's DealersChoice Attacks Continue (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/7u92nzu48zg6kq0pmtlh9pj8p6jmjmrt

Leviathan: Espionage actor spearphishes maritime and defense targets (2017). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

Leviathan: Geostrategy and TTP (Tactics, Techniques and Procedures) (2019). Source: S2 Grupo. Link: https://lab52.io/blog/leviathan-geostrategy-and-ttp-technical-tactics-and-procedures/

Lifting the veil on DeathStalker, a mercenary triumvirate (2020). Source: Kaspersky Lab. Link: https://securelist.com/deathstalker-mercenary-triumvirate/98177/

Live off the Land? How About Bringing Your Own Island? An Overview of UNC1945 (2020). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2020/11/live-off-the-land-an-overview-of-unc1945.html

Living off the land and fileless attack techniques (2017). Source: Palo Alto Networks. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

Lock Like a Pro: How QAKBOT Fuels Enterprise Ransomware Campaigns (2020). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5406875492177413645.pdf

LoJax // First UEFI rootkit found in the wild, courtesy of the Sednit group (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

LOLSnif – Tracking Another Ursnif-Based Targeted Campaign (2020). Source: Telekom. Link: https://www.telekom.com/en/blog/group/article/lolsnif-tracking-another-ursnif-based-targeted-campaign-600062

London Blue (2019). Source: AGARI. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/london-blue-april-2019.pdf

London Calling: Two-Factor Authentication Phishing From Iran (2015). Source: Citizen Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2015/Two-Factor-Authentication-Phishing-From-Iran.pdf

Longhorn: Tools used by cyberespionage group linked to Vault 7 (2017). Source: Symantec. Link: https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7

LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards (2019). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

Looking Into a Cyber-Attack Facilitator in the Netherlands (2016). Source: Trend Micro. Link: https://app.box.com/s/ub5txv2ky12s7kuuv7d1vzqvkympepaq

Looking Into a Cyber-Attack Facilitator in the Netherlands (Appendix) (2016). Source: Trend Micro. Link: https://app.box.com/s/1vjcdqrpcvtb5fqfehk3ehxj6qh8eaf0

Lookout discovers new mobile surveillanceware developed by Russian defense contractor Special Technology Center (2019). Source: Lookout. Link: https://blog.lookout.com/monokle

Lookout Discovers Novel Confucius APT Android Spyware Linked to India-Pakistan Conflict (2021). Source: Lookout. Link: https://blog.lookout.com/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict

Lookout finds new surveillanceware in Google Play with ties to known threat actor targeting the Middle East (2018). Source: Lookout. Link: https://blog.lookout.com/desert-scorpion-google-play

Lookout Phishing AI provides an inside look into a phishing campaign targeting mobile banking users (2020). Source: Lookout. Link: https://blog.lookout.com/lookout-phishing-ai-reveals-mobile-banking-phishing-campaign

Lotus Blossom Continues ASEAN Targeting (2018). Source: RSA Security. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.02.13.Lotus-Blossom-Continues/Lotus%20Blossom%20Continues%20ASEAN%20Targeting.pdf

LOWKEY: Hunting for the Missing Volume Serial ID (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/10/lowkey-hunting-for-the-missing-volume-serial-id.html

Lucky Cat (2012). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/luckycat-redux-inside-an-apt-campaign/

LUCKY ELEPHANT CAMPAIGN MASQUERADING (2019). Source: Netscout. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.22.LUCKY_ELEPHANT/LUCKY%20ELEPHANT%20Campaign%20Masquerading.pdf

Luckycat Redux: Inside An Apt Campaign With Multiple Targets In India And Japan (2012). Source: Trend Micro. Link: https://app.box.com/s/vun0x0rrek5l51djb8igbojb7v85sg3q

LuckyMouse signs malicious NDISProxy driver with certificate of Chinese IT company (2018). Source: Kaspersky Lab. Link: https://securelist.com/luckymouse-ndisproxy-driver/87914

LYCEUM Takes Center Stage in Middle East Campaign (2019). Source: Dell Secureworks. Link: https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

M-TRENDS2018 (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/04/m-trends-2018.html

MA-774.022020: MyCERT Advisory - Espionage Campaign Based On Technical Indicators (2020). Source: MyCERT. Link: https://www.mycert.org.my/portal/advisory?id=MA-774.022020

Mac Backdoor Linked to Lazarus Targets Korean Users (2019). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/mac-backdoor-linked-to-lazarus-targets-korean-users/

Mac Spyware Found at Oslo Freedom Forum (2013). Source: F-Secure. Link: https://www.f-secure.com/weblog/archives/00002554.html

Magecart Skimming Attack Targets Mobile Users of Hotel Chain Booking Websites (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.09.18.Magecart_Hotel_Chain_Booking/Magecart%20Skimming%20Attack%20Targets%20Mobile%20Users%20of%20Hotel%20Chain%20Booking%20Websites.pdf

Magic Hound Campaign Attacks Saudi Targets (2017). Source: Palo Alto Networks. Link: https://app.box.com/s/qg2l481eu51ab9znszagv2ktlh4bh9z5

Mahalo FIN7: Responding to the Criminal Operators' New Tools and Techniques (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

MahaPlant Group (2016). Source: 360 SkyEye System. Link: http://zhuiri.360.cn/report/index.php/2016/08/04/mahaplant-group/?lang=en

Malicious Document Targets Pyeongchang Olympics (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/

Malicious document targets Vietnamese officials (2018). Source: Sebastien Larinier. Link: https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a

Malicious Office files dropping Kasidet and Dridex (2016). Source: Zscaler. Link: http://research.zscaler.com/2016/01/malicious-office-files-dropping-kasidet.html

Maliciously Repackaged Psiphon Found (2014). Source: Citizen Lab. Link: https://citizenlab.org/2014/03/maliciously-repackaged-psiphon/

Malware Actors Using Nic Cyber Security Themed Spear Phishing To Target Indian Government Organizations (2016). Source: Cysinfo. Link: https://app.box.com/s/zsm16yh2sffqr9caehmifmvw2jrrwiga

Malware analysis about sample of APT Patchwork (2019). Source: StrangerealIntel. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.27.Patchwork_Malware_Analysis/Malware%20analysis%20about%20sample%20of%20APT%20Patchwork.pdf

Malware analysis about unknown Chinese APT campaign (2019). Source: StrangerealIntel. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.20.unknown_Chinese_APT/CyberThreatIntel_Malware%20analysis%2020-08-19.md%20at%20master%20%C2%B7%20StrangerealIntel_CyberThreatIntel.pdf

Malware analysis about unknown Israel APT campaign (2019). Source: CyberThreatIntel. Link: https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Israel/APT/Unknown/26-08-19/Malware%20analysis%2026-08-19.md

Malware analysis on Bitter APT campaign (2019). Source: StrangerealIntel. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.31.Bitter_APT_Malware_analysis/Bitter_APT_Malware_analysis.pdf

Malware analysis on Gamaredon APT campaign (2019). Source: StrangerealIntel. Link: https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Russia/APT/Gamaredon/16-08-19/Malware%20analysis%2016-08-19.md

Malware analysis on Gorgon APT campaign (2019). Source: StrangerealIntel. Link: https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Pakistan/APT/Gorgon/23-08-19/Malware%20analysis%2025-08-19.md

Malware Analysis Report (AR18-221A) (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

Malware Analysis Report (AR19-129A) (2019). Source: US-CERT. Link: https://www.us-cert.gov/ncas/analysis-reports/AR19-129A

Malware Analysis Report (AR21-039A) (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039a

Malware Analysis Report (AR21-039B) (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b

Malware Attack Targeting Syrian Isis Critics (2014). Source: Citizen Lab. Link: https://app.box.com/s/bnq1jfzfmvflkui8zw06fkp9c0x5dgxq

Malware Attacks Targeting Syrian ISIS Critics (2014). Source: Citizen Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2014/Malware-Attack-Targeting-Syrian-ISIS-Critics.pdf

Malware targets Vietnamese users (2010). Source: Electronic Frontier Foundation. Link: https://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html

Malware that Communicates with C&C Servers Using Cookie Headers (2017). Source: JPCERT. Link: https://www.threatminer.org/_reports/2017/JPCERT_CC Blog_ ChChes â€“ Malware that Communicates with C&C Servers Using Cookie Headers.pdf

Malware Used by “Rocke” Group Evolves to Evade Detection by Cloud Security Products (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/

Malware Used by BlackTech after Network Intrusion (2019). Source: JPCERT. Link: https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html

Mapping Hacking Team’s “Untraceable” Spyware (2014). Source: Citizen Lab. Link: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

Mapping out AridViper Infrastructure Using Augury’s Malware Module (2020). Source: Team Cymru. Link: https://team-cymru.com/blog/2020/12/16/mapping-out-aridviper-infrastructure-using-augurys-malware-addon/

Mapping the connections inside Russia’s APT Ecosystem (2019). Source: Check Point. Link: https://research.checkpoint.com/russianaptecosystem/

MAR-10135536-10 – North Korean Trojan: BADCALL (2019). Source: US-CERT. Link: https://www.us-cert.gov/ncas/analysis-reports/ar19-252a

MAR-10135536-21 – North Korean Proxy Malware: ELECTRICFISH (2019). Source: US-CERT. Link: https://www.us-cert.gov/ncas/analysis-reports/ar19-252b

MAR-10135536-8 – North Korean Trojan: HOPLIGHT (2019). Source: US-CERT. Link: https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

MAR-10292089-1.v2 – Chinese Remote Access Trojan: TAIDOOR (2020). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a

MAR-10322463-1.v1 - AppleJeus: Celas Trade Pro (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048a

MAR-10322463-2.v1 - AppleJeus: JMT Trading (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048b

MAR-10322463-3.v1 - AppleJeus: Union Crypto (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048c

MAR-10322463-4.v1 - AppleJeus: Kupay Wallet (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048d

MAR-10322463-5.v1 - AppleJeus: CoinGoTrade (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048e

MAR-10322463-6.v1 - AppleJeus: Dorusio (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048f

MAR-10322463-7.v1 - AppleJeus: Ants2Whale (2021). Source: US-CERT. Link: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048g

MartyMcFly Malware: Targeting Naval Industry (2018). Source: Marco Ramilli. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.10.17_MartyMcFly_Targeting_Naval_Industry/MartyMcFly%20Malware_%20Targeting%20Naval%20Industry.pdf

Masha and these Bears 2018 Sofacy Activity (2018). Source: Kaspersky Lab. Link: https://securelist.com/masha-and-these-bears/84311/

Massive malicious campaign by FakeSecurity JS-sniffer (2019). Source: Group-IB. Link: https://www.group-ib.com/blog/fakesecurity

MATA: Multi-platform targeted malware framework (2020). Source: Kaspersky Lab. Link: https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/

McAfee Labs Threats Report (2017). Source: Intel Security-McAfee. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/rp-quarterly-threats-mar-2017.pdf

McAfee Uncovers Operation Honeybee, a Malicious Document Campaign Targeting Humanitarian Aid Groups (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/

MEDJACK.4 Medical Device Hijacking (2015). Source: TrapX Security. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2015/2_5402583565718259452.pdf

Meet CrowdStrike’s Adversary of the Month for April: STARDUST CHOLLIMA (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima/

Meet CrowdStrike’s Adversary of the Month for August: GOBLIN PANDA (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/

Meet CrowdStrike’s Adversary of the Month for February: MUMMY SPIDER (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/

Meet CrowdStrike’s Adversary of the Month for July: WICKED SPIDER (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/

Meet CrowdStrike’s Adversary of the Month for June: MUSTANG PANDA (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/

Meet CrowdStrike’s Adversary of the Month for March: VENOMOUS BEAR (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/

Meet CrowdStrike’s Adversary of the Month for May: MYTHIC LEOPARD (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/adversary-of-the-month-for-may/

Meet CrowdStrike’s Adversary of the Month for November: HELIX KITTEN (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

Meet CrowdStrike’s Adversary of the Month for October: DUNGEON SPIDER (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-october-dungeon-spider/

Meet CrowdStrike’s Adversary of the Month for September: COBALT SPIDER (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-september-cobalt-spider/

menuPass Playbook and IOCs (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/menupass-playbook-and-iocs/

menuPass Returns with New Malware and New Attacks (2017). Source: Palo Alto Networks. Link: https://www.threatminer.org/_reports/2017/menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations - Palo Alto Networks Blog.pdf

MESSAGETAP: Who’s Reading Your Text Messages? (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html

Metamorfo Campaigns Targeting Brazilian Users (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/04/metamorfo-campaign-targeting-brazilian-users.html

MFSocket: A Chinese surveillance tool (2019). Source: Elliot Alderson. Link: https://medium.com/@fs0c131y/mfsocket-a-chinese-surveillance-tool-58e8850c3de4

Micro-Targeted Malvertising Via Real-Time Ad Bidding (2014). Source: Invincea. Link: https://app.box.com/s/fy9ss400cv8irbkyrw7i72dc8xaf5xiv

Microsoft Security Intelligence Report (Volume 19) (2015). Source: Microsoft. Link: https://app.box.com/s/qjvx7sdbo7cufb5b8putfyqn8ku82xq2

Middle East Cyber-Espionage (2018). Source: Objective-See. Link: https://objective-see.com/blog/blog_0x3B.html

Middle East Cyber-Espionage (2019). Source: Objective-See. Link: https://objective-see.com/blog/blog_0x3D.html

Middle East Cyber-Espionage: analyzing WindShift's implant: OSX.WindTail (2018). Source: Objective-See. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.12.20.WindShift_Middle_East/analyzing%20WindShift%20implant%20OSX.WindTail.pdf

Mikroceen: Spying backdoor leveraged in high-profile networks in Central Asia (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/

MILE TEA: Cyber Espionage Campaign Targets Asia Pacific Businesses and Government Agencies (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

Military Financing Maldoc: analysis (2019). Source: S2 Grupo. Link: https://lab52.io/blog/military-financing-maldoc-analysis/

Miniduke Still Duking It Out (2014). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/dnn3hp5nlwuiwxcqjc9kmsfiodcimi64

Miniduke: Indicators (2013). Source: Laboratory of Cryptography and System Security (CrySyS Lab). Link: https://app.box.com/s/d5npu14e4471j5mmpkgt1xwdnu90t43e

MirageFox: APT15 Resurfaces With New Tools Based On Old Ones (2018). Source: Intezer. Link: https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

Mirrorthief Hits Campus Online Stores Using Magecart (2019). Source: Trend Micro. Link: https://www.trendmicro.com/en_us/research/19/e/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada.html

Missed 0day? - APT-C-06 organized another network arsenal analysis (2018). Source: 360 SkyEye System. Link: http://blogs.360.cn/post/VBScript_vul_CH.html

Mm Core In-Memory Backdoor Returns As Bigboss And Sillygoose (2017). Source: Forcepoint. Link: https://www.threatminer.org/_reports/2017/MM CORE IN-MEMORY BACKDOOR RETURNS AS BIGBOSS AND SILLYGOOSE - Forcepoint.pdf

Mo' Shells Mo' Problems - Deep Panda Web Shells (2014). Source: CrowdStrike. Link: https://app.box.com/s/pn1mtot3a2d2seuqx46unamdl7udlwq0

Mobile APT Surveillance Campaigns Targeting Uyghurs (2020). Source: Lookout. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5471880419202827949.pdf

Modified Binaries Tor (2014). Source: Leviathan Security Group. Link: https://app.box.com/s/nj7stspq3veln8iebra2f5u1203i86eg

Mofang: A politically motivated information stealing adversary (2016). Source: Fox-IT. Link: https://app.box.com/s/p2oftago51ohnku082ztx1kbvaa1lxps

MoneyTaker 1.5 Years of Silent Operations (2017). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Group-IB_MoneyTaker.pdf

MoneyTaker, revealed after 1.5 years of silent operations. (2017). Source: Group-IB. Link: https://www.group-ib.com/resources/reports/money-taker.html

Monitoring Information Controls in Iraq in Reaction to ISIS Insurgency (2014). Source: Citizen Lab. Link: https://citizenlab.ca/2014/06/monitoring-information-controls-in-iraq/

Monthly Threat Actor Group Intelligence Report, August 2019 (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/10/07/august-2019-intelligence-report/

Monthly Threat Actor Group Intelligence Report, December 2019 (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2020/02/13/december-2019-intelligence-report/

Monthly Threat Actor Group Intelligence Report, October 2019 (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/12/19/october-2019-intelligence-report/

Moonlight - Targeted attacks in the Middle East (2016). Source: Vectra Networks. Link: http://blog.vectranetworks.com/blog/moonlight-middle-east-targeted-attacks

Moonlight is Coming again - An analysis of the latest attack by the MoonLight organization against the Middle East (2019). Source: 360 SkyEye System. Link: https://ti.qianxin.com/blog/articles/anatomy-of-moonLight-attack-on-the-middle-east/

Moonsoon - Analysis of an APT Campaign (2016). Source: Forcepoint. Link: https://app.box.com/s/cdivyys0ej34bh9r151vybct5nlqy4l5

More Evidence of APT Hackers-for-Hire Used for Industrial Espionage (2020). Source: BitDefender. Link: https://labs.bitdefender.com/2020/08/apt-hackers-for-hire-used-for-industrial-espionage/

More evil: A deep look at Evilnum and its toolset (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

More on Huaying Haitai and Laoying Baichaun, the companies associated with APT10. Is there a state connection? (2018). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2018/08/09/was-apt10-the-work-of-individuals-a-company-or-the-state/

More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting (2019). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/#

More_eggs, Anyone? Threat Actor ITG08 Strikes Again (2019). Source: IBM. Link: https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/

Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools (2020). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/

Morocco: Human Rights Defenders Targeted with NSO Group’s Spyware (2019). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware/

Muddying the Water: Targeted Attacks in the Middle East (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

"MuddyWater expands operations

(2018). Source: Kaspersky Lab. Link: https://securelist.com/muddywater/88059/"

MuddyWater Operations in Lebanon and Oman (2018). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/

MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.06.10.MuddyWater_Resurfaces/blog_new_muddywater_findings_uncovered.pdf

Multi-stage APT attack drops Cobalt Strike using Malleable C2 feature (2020). Source: MalwareBytes. Link: https://blog.malwarebytes.com/threat-analysis/2020/06/multi-stage-apt-attack-drops-cobalt-strike-using-malleable-c2-feature/

Multiple ArtraDownloader Variants Used by BITTER to Target Pakistan (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/

Multiple Chinese Threat Groups Exploiting CVE-2018-0798 Equation Editor Vulnerability Since Late 2018 (2019). Source: Anomali. Link: https://www.anomali.com/blog/multiple-chinese-threat-groups-exploiting-cve-2018-0798-equation-editor-vulnerability-since-late-2018

Multiple Cobalt Personality Disorder (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html

Musical Chairs Playing Tetris (2018). Source: Arbor Networks. Link: https://www.arbornetworks.com/blog/asert/musical-chairs-playing-tetris/

Musical Chairs: Multi-Year Campaign Involving New Variant of Gh0st Malware (2015). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2015/09/musical-chairs-multi-year-campaign-involving-new-variant-of-gh0st-malware/

MyKings Botnet (2020). Source: AhnLab. Link: http://download.ahnlab.com/kr/site/library/%5BAhnLab%5DAnalysis%20Report_MyKings%20Botnet.pdf

MyKings: The Slow But Steady Growth of a Relentless Botnet (2020). Source: SophosLabs. Link: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-uncut-mykings-report.pdf

NanHaiShu: RATing the South China Sea (2016). Source: F-Secure. Link: https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf

NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/05/navrat.html

Nazar: Spirits of the Past (2020). Source: Check Point. Link: https://research.checkpoint.com/2020/nazar-spirits-of-the-past/

Nettraveler Apt Gets A Makeover For 10Th Birthday (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/5p59z0cnoul885qx2hj1f85h00mk2ec5

NetTraveler APT Targets Russian, European Interests (2016). Source: Proofpoint. Link: https://app.box.com/s/u16hs4trjkamdxkb8xth6e5ugckr3230

NetTraveler Spear-Phishing Email Targets Diplomat of Uzbekistan (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/01/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/

New activity of the Blue Termite APT (2015). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/71876/new-activity-of-the-blue-termite-apt/

New Adwind Campaign targets US Petroleum Industry (2019). Source: Netskope. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.10.01.Adwind_Campaign_US_Petroleum_Industry/New%20Adwind%20Campaign%20targets%20US%20Petroleum%20Industry.pdf

New Andariel Reconnaissance Tactics Hint At Next Targets (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/new-andariel-reconnaissance-tactics-hint-at-next-targets/

New Android Spyware ActionSpy Revealed via Phishing Attacks from Earth Empusa (2020). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/

New Approaches Utilized by OceanLotus to Target An Environmental Group in Vietnam (2019). Source: Qianxin. Link: https://ti.qianxin.com/blog/articles/english-version-of-new-approaches-utilized-by-oceanLotus-to-target-vietnamese-environmentalist/

New APT32 Malware Campaign Targets Cambodian Government (2020). Source: Recorded Future. Link: https://www.recordedfuture.com/apt32-malware-campaign/

"New BabyShark Malware Targets U.S. National Security Think Tanks

(2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/"

New Bank Attacks (2018). Source: Positive Technologies. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/New-Bank-Attacks-eng.pdf

NEW CAMPAIGN DELIVERS ORCUS RAT (2019). Source: Morphisec. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.01.30.ORCUS_RAT/New%20Campaign%20delivers%20orcus%20rat.pdf

New Carbanak / Anunak Attack Methodology (2016). Source: Trustwave. Link: https://app.box.com/s/cbclbgiu54ihivxe7bvblwsv1e8jq44h

New Cdto: A Sneakernet Trojan Solution (2014). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/63rg0wfr0ki2xvtt7ja1b7lmn7dspcdc

New Cyber Espionage Campaigns Targeting Palestinians - Part 1: The Spark Campaign (2020). Source: Cybereason. Link: https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one

New Cyber Espionage Campaigns Targeting Palestinians - Part 2: The Discovery of the New, Mysterious Pierogi Backdoor (2020). Source: Cybereason. Link: https://www.cybereason.com/blog/new-cyber-

espionage-campaigns-targeting-palestinians-part-2-the-discovery-of-the-new-mysterious-pierogi-backdoor

New cyberattacks targeting sporting and anti-doping organizations (2019). Source: Microsoft. Link: https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

New dark_nexus IoT Botnet Puts Others to Shame (2020). Source: BitDefender. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5222179159576413852.pdf

New Destructive Wiper “ZeroCleare” Targets Energy Sector in the Middle East (2019). Source: IBM. Link: https://www.ibm.com/downloads/cas/OAJ4VZNJ

New Espionage Operations Target Military and Government Organizations (2018). Source: Symantec. Link: https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

New Evidence Proves Ongoing WIZARD SPIDER / LUNAR SPIDER Collaboration (2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/

New Fileless Botnet Novter Distributed by KovCoreG Malvertising Campaign (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.10.01.kovcoreg-malvertising-campaign/Appendix-New-Fileless-Botnet-Novter-Distributed-by-KovCoreG-Malvertising-Campaign.pdf

"New FinSpy iOS and Android implants revealed ITW

(2019). Source: Kaspersky Lab. Link: https://securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/"

New HawkEye Reborn Variant Emerges Following Ownership Change (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/04/hawkeye-reborn.html

New Indicators Of Compromise For Apt Group Nitro Uncovered (2014). Source: Palo Alto Networks. Link: https://app.box.com/s/drb0p2idherjlxlwdqh0nharpt310s8u

New Insights into Energetic Bear’s Watering Hole Attacks on Turkish Critical Infrastructure (2017). Source: RISKIQ. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2017/2017.11.02.Energetic_Bear_on_Turkish_Critical_Infrastructure/New%20Insights%20into%20Energetic%20Bear's%20Attacks%20on%20Turkish%20Critical%20Infrastructure.pdf

New Internet Explorer zero-day exploited in Hong Kong attacks (2015). Source: Symantec. Link: http://www.symantec.com/connect/blogs/new-internet-explorer-zero-day-exploited-hong-kong-attacks

New Iranian Campaign Tailored to US Companies Utilizes an Updated Toolset (2020). Source: Intezer. Link: https://intezer.com/blog-new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/

New KillDisk Variant Hits Financial Organizations in Latin America (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

New LNK attack tied to Higaisa APT discovered (2020). Source: MalwareBytes. Link: https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/

New MacOS Backdoor Linked to OceanLotus Found (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/

New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan (2012). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2012/07/new-blackshades-malware

New Malware with Ties to SunOrcal Discovered (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

New modular downloaders fingerprint systems - Part 2: AdvisorsBot (2018). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-2-advisorsbot

New modular downloaders fingerprint systems - Part 3: CobInt (2018). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-3-cobint

New modular downloaders fingerprint systems, prepare for more - Part 1: Marap (2018). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-prepare-more-part-1-marap

New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

New PatchWork Spearphishing Attack (2019). Source: S2 Grupo. Link: https://lab52.io/blog/new-patchwork-campaign-against-pakistan/

New Perl Botnet (Tuyul) Found with Possible Indonesian Attribution (2020). Source: F5 Networks. Link: https://www.f5.com/labs/articles/threat-intelligence/new-perl-botnet--tuyul--found-with-possible-indonesian-attributi

New Poison Ivy Activity Targeting Myanmar, Asian Countries (2016). Source: Arbor Networks. Link: https://www.arbornetworks.com/blog/asert/recent-poison-iv/

New Poison Ivy RAT Variant Targets Hong Kong Pro-Democracy Activists (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/

New PowerShell-based Backdoor Found in Turkey, Strikingly Similar to MuddyWater Tools (2018). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.11.30.MuddyWater_Turkey/PowerShell-

based%20Backdoor%20Found%20in%20Turkey%20Strikingly%20Similar%20to%20MuddyWater%20Tools.pdf

New Python-based payload MechaFlounder used by Chafer (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/

New Ransomware Variant "Nyetya" Compromises Systems Worldwide (2017). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

New Sofacy Attacks Against US Government Agency (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/49rs6u4cyq43khamdah90y9zyacjzmbr

New Spear Phishing Campaign Pretends to be EFF (2016). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff

New Targeted Attack in the Middle East by APT34 (2017). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

New Targeted Attack On Taiwanese Government & Tibetan Activists Open Up a Can Of Worms (2013). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2013/04/new-targeted-attack-on-taiwanese-government-tibetan-activists-open-up-a-can-of-worms-graypigeon-hangame-shiqiang-gang.html

New Techniques to Uncover and Attribute Cobalt Gang Commodity Builders and Infrastructure Revealed (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/10/unit42-new-techniques-uncover-attribute-cobalt-gang-commodity-builders-infrastructure-revealed/

New TeleBots backdoor: First evidence linking Industroyer to NotPetya (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

New Threat Actor Group DarkHydrus Targets Middle East Government (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

New traces of Hacking Team in the wild (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/

New Trojan Spread Over Skype as Cat and Mouse Game Between Syrian Activists and Pro-Syrian-Government Hackers Continues (2012). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware

New Ursnif Campaign: A Shift from PowerShell to Mshta (2020). Source: Zscaler. Link: https://www.zscaler.com/blogs/research/new-ursnif-campaign-shift-powershell-mshta

New Version Of Osx.Sabpub & Confirmed Mac Apt Attacks (2012). Source: Kaspersky Lab. Link: https://app.box.com/s/ew3h0mve5lf5x69ydjd1sm1r380rqy4k

New VPNFilter malware targets at least 500K networking devices worldwide (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/05/VPNFilter.html

New wave of cyberattacks against Ukrainian power industry (2016). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/

New wave of PlugX targets Hong Kong (2020). Source: Avira. Link: https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/

New Wekby Attacks Use DNS Requests As Command and Control Mechanism (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/5dcx9g1lrt3m9y2wgmxpyiv4malmdnpp

New Wine in Old Bottle: New Azorult Variant Found in FindMyName Campaign using Fallout Exploit Kit (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/11/unit42-new-wine-old-bottle-new-azorult-variant-found-findmyname-campaign-using-fallout-exploit-kit/

New Zero-Day Exploit Targeting Internet Explorer Versions 9 Through 11 Identified In Targeted Attacks (2014). Source: FireEye. Link: https://app.box.com/s/5epjx7i7fc3q8jh8o4exabquoar1s3ii

Newcomers in the Derusbi family (2015). Source: Airbus Defence and Space. Link: http://blog.airbuscybersecurity.com/post/2015/11/Newcomers-in-the-Derusbi-family

Newly identified StrongPity operations (2019). Source: Alien Labs. Link: https://cybersecurity.att.com/blogs/labs-research/newly-identified-strongpity-operations

Newly identified StrongPity operations (2019). Source: AlienVault. Link: https://www.alienvault.com/blogs/labs-research/newly-identified-strongpity-operations

Nigerian Cybercriminals Target High-Impact Industries in India via Pony (2016). Source: Cylance. Link: https://blog.cylance.com/threat-update-nigerian-cybercriminals-target-high-impact-indian-industries-via-pony

Night Dragon: Specific Protection Measures For Consideration (2011). Source: North American Electric Reliability Corporation (NERC). Link: https://app.box.com/s/grv4y3nziuxbsv4g16nyf4u1i1g1w0nm

Night of the Devil: Ransomware or wiper? A look into targeted attacks in Japan using MBR-ONI (2017). Source: Cybereason. Link: https://www.cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan

Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society (2017). Source: Citizen Lab. Link: https://citizenlab.ca/2017/02/nilephish-report/

Njrat Uncovered (2013). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/vdg51zbfvap52w60zj0is3l1dmyya0n4

Njrat, The Saga Continues (2013). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/6blnvkflzcded9jlthm7yt1zzki6eakz

No need to hack when it's leaking: GITHUB HEALTHCARE LEAKS (2020). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5319106843346208325.pdf

NO REST FOR THE WICKED: EVILNUM UNLEASHES PYVIL RAT (2020). Source: Cybereason. Link: https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat

No summer vacations for Zebrocy (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

North American Electric Cyber Threat Perspective (2020). Source: Dragos. Link: https://dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf

North Korea Bitten by Bitcoin Bug: Financially motivated campaigns reveal new dimension of the Lazarus Group (2017). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new

North Korea Is Not Crazy (2017). Source: Recorded Future. Link: https://app.box.com/s/tb68b0jfrwg7ji1o01jw28def2lp86y7

North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign (2018). Source: Recorded Future. Link: https://go.recordedfuture.com/hubfs/reports/cta-2018-0116.pdf

North Korea Turns Against New Targets?! (2019). Source: Check Point. Link: https://research.checkpoint.com/north-korea-turns-against-russian-targets/

North Korean Defectors and Journalists Targeted Using Social Networks and KakaoTalk (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/north-korean-defectors-journalists-targeted-using-social-networks-kakaotalk/

North Korean hackers are skimming US and European shoppers (2020). Source: Sansec. Link: https://sansec.io/research/north-korea-magecart

Nortrom_Lion_APT (2020). Source: Qianxin. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.02.28_Nortrom_Lion_APT/Nortrom_Lion_APT_CN_version.pdf

Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign (2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html

Nothing Sacred Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware (2020). Source: Citizen Lab. Link: https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/

NSO Group / Q Cyber Technologies (2019). Source: Citizen Lab. Link: https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident (2018). Source: Citizen Lab. Link: https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/

Nueva campaña del grupo ruso TA505 dirigida a Chile y Argentina. #ServHelper #FlawedAmmy (2019). Source: Germán Fernández Bacian. Link: https://medium.com/@1ZRR4H/nueva-campa%C3%B1a-del-grupo-ruso-ta505-dirigida-a-chile-y-argentina-servhelper-1dc3bfbff0c7

Obfuscation Tools Found in the Capesand Exploit Kit Possibly Used in “KurdishCoder” Campaign (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.12.04.KurdishCoder_Campaign/Obfuscation%20Tools%20Found%20in%20the%20Capesand%20Exploit%20Kit%20Possibly%20Used%20in%20%E2%80%9CKurdishCoder%E2%80%9D%20Campaign.pdf

Observations gained from the front lines of Incident Response and Proactive Services in 2019 and insights that matter for 2020 (2020). Source: CrowdStrike. Link:

https://www.crowdstrike.com/resources/reports/crowdstrike-services-cyber-front-lines-2020https://www.crowdstrike.com/resources/reports/crowdstrike-services-cyber-front-lines-2020/

Observing the Havex RAT (2014). Source: NETRESEC. Link: https://www.netresec.com/?page=Blog&month=2014-11&post=Observing-the-Havex-RAT

Oceanlotus (2015). Source: 360 SkyEye System. Link: https://app.box.com/s/fapwtkrudntz5po7c4u34l54j0vys9po

Oceanlotus APT-C-00 (2017). Source: 360 SkyEye System. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2015/OceanLotusReport.pdf

OceanLotus Blossoms Mass Digital Surveillance and Attacks Targeting ASEAN (2017). Source: Volexity. Link: https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/

OCEANLOTUS ON ASEAN AFFAIRS (2019). Source: Telsy. Link: https://blog.telsy.com/oceanlotus-on-asean-affairs/

OceanLotus ships new backdoor using old tricks (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/

OceanLotus Steganography (2019). Source: Cylance. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.04.02.OceanLotus_Steganography/OceanLotus-Steganography-Malware-Analysis-White-Paper.pdf

OceanLotus: Extending Cyber Espionage Operations Through Fake Websites (2020). Source: Volexity. Link: https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

OceanLotus: Old techniques, new backdoor (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf

OceanLotus' Attacks to Indochinese Peninsula: Evolution of Targets, Techniques and Procedure (2019). Source: Qianxin. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.08.OceanLotus/OceanLotus%20Attacks%20to%20Indochinese%20Peninsula.pdf

Octopus-infested seas of Central Asia (2018). Source: Kaspersky Lab. Link: https://securelist.com/octopus-infested-seas-of-central-asia/88200/

OilRig Deploys ALMA Communicator - DNS TunnelingTrojan (2017). Source: Palo Alto Networks. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/PaloAlto_OilRig-Deploys-ALMA-DNS-Tunneling-Trojan.pdf

OilRig Targets a Middle Eastern Government and Adds Evasion Techniques to OopsIE (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-targets-middle-eastern-government-adds-evasion-techniques-oopsie/

OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory (2020). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

OilRig Targets Technology Service Provider and Government Agency with QUADAGENT (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/

OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/07/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/

OilRig uses RGDoor IIS Backdoor on Targets in the Middle East (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/

OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

Okrum and Ketrican: An overview of recent Ke3chang group activity (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

Olympic Destroyer is still alive (2018). Source: Kaspersky Lab. Link: https://securelist.com/olympic-destroyer-is-still-alive/86169/

Olympic Destroyer Takes Aim At Winter Olympics (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

OlympicDestroyer is here to trick the industry (2018). Source: Kaspersky Lab. Link: https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/

On the StrongPity Waterhole Attacks Targeting Italian and Belgian Encryption Users (2016). Source: Kaspersky Lab. Link: https://app.box.com/s/c9w0xp0mgndij268ku7ti5ee4lxu54bv

Ongoing Njrat campaign against Middle East (2019). Source: S2 Grupo. Link: https://lab52.io/blog/ongoing-njrat-campaign-against-middle-east/

Ongoing Sophisticated Malware Campaign Compromising ICS (2014). Source: US-CERT. Link: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

Onionduke: Apt Attacks Via The Tor Network - F-Secure Weblog : News From The Lab (2014). Source: F-Secure. Link: https://app.box.com/s/vpr6m62odv8f7tz59xisqrba9khg4rhi

Oops, they did it again: APT Targets Russia and Belarus with ZeroT and PlugX (2017). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

Opening “STEELCORGI”: A Sophisticated APT Swiss Army Knife (2021). Source: Yoroi. Link: https://yoroi.company/research/opening-steelcorgi-a-sophisticated-apt-swiss-army-knife/

Operation ‘Dream Job’ Widespread North Korean Espionage Campaign (2020). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/operation-dream-job/

Operation ‘Honey Trap’: APT36 Targets Defense Organizations in India (2020). Source: Seqrite. Link: https://www.seqrite.com/blog/operation-honey-trap-apt36-targets-defense-organizations-in-india/

Operation AppleJeus Sequel (2020). Source: Kaspersky Lab. Link: https://securelist.com/operation-applejeus-sequel/95596/

Operation AppleJeus: Lazarus hits cryptocurrency exchange with fake installer and macOS malware (2018). Source: Kaspersky Lab. Link: https://securelist.com/operation-applejeus/87553/

Operation Arachnophobia Caught In The Spider's Web (2014). Source: ThreatConnect. Link: https://app.box.com/s/d7pm2c1r4cx80tt1rctysd7452lo367v

Operation Arid Viper: Bypassing The Iron Dome (2015). Source: Trend Micro. Link: https://app.box.com/s/uqh30535vxopnp0achnlcemu2034aa26

Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare (2015). Source: LookingGlass. Link: https://info.lookingglasscyber.com/rs/842-NZZ-976/images/Operation_Armageddon_Final.pdf

Operation Aurora (2010). Source: HBGary. Link: https://app.box.com/s/fjb89qr1vnk2ox0vllj68ivadqgyz3an

Operation Aurora: Detect, Diagnose, Respond (2010). Source: HBGary. Link: https://app.box.com/s/j36zc0da9nz6q8wnv13slwxcnmiaykul

Operation Bachosens: A detailed look into a long-running cyber crime campaign (2017). Source: Symantec. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Operation_Bachosens.pdf

Operation Beebus (2013). Source: FireEye. Link: https://app.box.com/s/3bk8cfcjiwhh1gxlkmyslrmp85wm7ewd

Operation Black Atlas, Part 2: Tools and Malware Used and How to Detect Them (2015). Source: Trend Micro. Link: http://documents.trendmicro.com/assets/Operation_Black%20Atlas_Technical_Brief.pdf

Operation Blockbuster (2016). Source: Novetta. Link: https://app.box.com/s/rhn69xecfqe8k2abwmn43ilmd59y1we0

Operation Blockbuster (2016). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/11/unit42-operation-blockbuster-goes-mobile/

Operation Bugdrop: Cyberx Discovers Large-Scale Cyber-Reconnaissance Operation Targeting Ukrainian Organizations (2017). Source: CyberX. Link: https://cyberx-labs.com/en/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/

Operation C-Major Actors Also Used Android BlackBerry Mobile Spyware Against Targets (2016). Source: Trend Micro. Link: https://app.box.com/s/xua6557tccyx7h0ksmjnu8u5bra3z15n

Operation C-Major: Information Theft Campaign Targets Military Personnel in India (2016). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/indian-military-personnel-targeted-by-information-theft-campaign/

Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign (2015). Source: FireEye. Link: https://app.box.com/s/vxnua4o5c8u12xl4r7e5zkndpw65wz0m

Operation Cleaver (2014). Source: Cylance. Link: http://www.cylance.com/operation-cleaver/

Operation Cleaver: The Notepad Files (2014). Source: Cylance. Link: https://app.box.com/s/vsret8sjx5qd6xaxzv0rxdw4pocdmjll

Operation Cloud Hopper (2017). Source: PWC. Link: https://app.box.com/s/ifeoa5huug0aqdecsniw7jmrxym0k85i

Operation Cloudyomega: Ichitaro Zero-Day And Ongoing Cyberespionage Campaign Targeting Japan (2014). Source: Symantec. Link: https://app.box.com/s/61pv7a2qufqbm3dhargkrsqjjzgswxba

Operation Cobalt Kitty Threat Actor Profile & IOC (2017). Source: Cybereason. Link: https://www.cybereason.com/blog/operation-cobalt-kitty-apt

Operation Cobalt Kitty: A large-scale APT in Asia carried out by the OceanLotus Group (2017). Source: Cybereason. Link: https://app.box.com/s/0bfouh1vvqc8esyh7tdvw2ttpsqzu1kh

Operation Comando: How to Run a Cheap and Effective Credit Card Business (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/operation-comando-or-how-to-run-a-cheap-and-effective-credit-card-business/

Operation Daybreak (2016). Source: Kaspersky Lab. Link: https://securelist.com/operation-daybreak/75100/

Operation Deputydog: Zero-Day (Cve-2013-3893) Attack Against Japanese Targets (2013). Source: FireEye. Link: https://app.box.com/s/w4rzfbf0ziip0dt4smkwtraluv8o0z9g

Operation Desert Eagle (2017). Source: Malware Party. Link: http://mymalwareparty.blogspot.tw/2017/07/operation-desert-eagle.html

Operation Double Tap (2014). Source: FireEye. Link: https://app.box.com/s/30f8215m5iow438k6gpjuxyvlsid7oom

Operation Dragonfly Analysis Suggests Links to Earlier Attacks (2017). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/operation-dragonfly-analysis-suggests-links-to-earlier-attacks/

Operation Duststorm (2016). Source: Cylance. Link: https://app.box.com/s/dt9mscechq7heg83z7vgujp5ujjzd97c

Operation Dusty Sky (2016). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/cydpeasz6l8cv9oo99o4tpazd5tq4xkm

Operation Dusty Sky (indicators) (2016). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/5iym3huegu3ssaejl0rr268sr7qy6seb

Operation DustySky Part 2 (2016). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/ldd528ht55m4avot9b485mi6529f8c3r

Operation DustySky Part 2 Indicators (2016). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/q9amfvko7h3x9g4rgcno0vy25btsv1rw

Operation Electric Powder - Who is targeting Israel Electric Company? (2017). Source: ClearSky Cybersecurity . Link: https://www.threatminer.org/_reports/2017/Operation Electric Powder â€“ Who is targeting Israel Electric Company_ _ ClearSky Cybersecurity.pdf

Operation ENDTRADE: Finding Multi-Stage Backdoors that TICK (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.29.Operation_ENDTRADE/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

Operation Ephemeral Hydra: Ie Zero-Day Linked To Deputydog Uses Diskless Method (2013). Source: FireEye. Link: https://app.box.com/s/qm0qqb7bpc0ut2c5n76zr5i0rdfhy5ts

Operation Gamework: Infrastructure Overlaps Found Between BlueAlpha and Iranian APTs (2019). Source: Recorded Future. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/cta-2019-1212.pdf

Operation Ghost (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/

Operation Ghoul: targeted attacks on industrial and engineering organizations (2016). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/75718/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/

Operation Grand Mars: Defending Against Carbanak Cyber Attacks (2017). Source: Trustwave. Link: https://www.trustwave.com/Resources/Library/Documents/Operation-Grand-Mars--Defending-Against-Carbanak-Cyber-Attacks/

Operation Greedywonk: Multiple Economic And Foreign Policy Sites Compromised, Serving Up Flash Zero-Day Exploit (2014). Source: FireEye. Link: https://app.box.com/s/870bnpwyxqjqg9o0z4sl0e2mlkzar60q

Operation Groundbait: Analysis of a surveillance toolkit (2016). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/hq5t0xjxxbkeulf942ufeiyf3k4zq9b6

Operation Hangover - Unveiling An Indian Cyberattack Infrastructure (2013). Source: Norman Shark. Link: https://app.box.com/s/f5wyu7306nti3lbp58uesioijsl9zamm

Operation Hangover - Unveiling An Indian Cyberattack Infrastructure (Appendix) (2013). Source: Norman Shark. Link: https://app.box.com/s/2k6oduwj3aetbetxdjx6gjqcg7mrcvvj

Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors (2017). Source: Trend Micro. Link: http://newsroom.trendmicro.com/blog/operation-iron-tiger-attackers-shift-east-asia-united-states

Operation JOKAA(RR) (2018). Source: Malware Party. Link: https://mymalwareparty.blogspot.com/2018/11/operation-jokaarr.html

Operation Ke3chang Resurfaces With New TidePool Malware (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/vwuocstge7xud74xhnw9s98h2m812pyr

Operation Ke3Chang Targeted Attacks Against Ministries Of Foreign Affairs (2013). Source: FireEye. Link: https://app.box.com/s/8w1uu9e2l7jwq40gtea7xem6ezg79ffu

Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal (2017). Source: Claudio Guarnieri e Collin Anderson. Link: https://medium.com/amnesty-insights/operation-kingphish-uncovering-a-campaign-of-cyber-attacks-against-civil-society-in-qatar-and-aa40c9e08852#.cly4mg1g8

Operation Lotus Bloom (2015). Source: Palo Alto Networks. Link: https://app.box.com/s/xhn6ru62qqom1kuxoe3mxnqrtb1sqw2q

Operation Manul: I Got a Letter From the Government the Other Day...Unveiling a Campaign of Intimidation, Kidnapping, and Malware in Kazakhstan (2016). Source: Electronic Frontier Foundation. Link: https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf

Operation Mermaid (2016). Source: 360 SkyEye System. Link: http://zhuiri.360.cn/report/index.php/2016/05/30/operation-mermaid/?lang=en

Operation Molerats (2013). Source: FireEye. Link: https://app.box.com/s/96rwehp2pkoou5gnimrx3sfdymv0nkhv

Operation Moneyholic With HWP Document (2019). Source: AhnLab. Link: https://asec.ahnlab.com/1251

Operation North Star: A Job Offer That's Too Good to be True? (2020). Source: Intel Security-McAfee. Link: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/

Operation Oceansalt Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group (2018). Source: Intel Security-McAfee. Link: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

Operation Oceansalt Delivers Wave After Wave (2018). Source: Intel Security-McAfee. Link: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/

Operation Oil Tanker: The Phantom Menace (2015). Source: Panda Security. Link: https://app.box.com/s/xrwk7gqk44dp89fioubewttrw8a88im1

Operation OnionDog: A 3 Year Old APT Focused On the Energy and Transportation Industries in Korean-language Countries (2016). Source: 360 SkyEye System. Link: http://www.prnewswire.com/news-releases/onion-dog-a-3-year-old-apt-focused-on-the-energy-and-transportation-industries-in-korean-language-countries-is-exposed-by-360-300232441.html

Operation Overtrap Targets Japanese Online Banking Users Via Bottle Exploit Kit and Brand-New Cinobi Banking Trojan (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5424768398946993891.pdf

Operation Parliament, who is doing what? (2018). Source: Kaspersky Lab. Link: https://securelist.com/operation-parliament-who-is-doing-what/85237/

Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House (2015). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house

Operation Pawn Storm Using Decoys To Evade Detection (2014). Source: Trend Micro. Link: https://app.box.com/s/t2flymgu0ct5s3z487oedaq8dycsge77

Operation Pistacchietto (2019). Source: Yoroi. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.06.Operation_Pistacchietto/Operation_Pistacchietto.pdf

Operation Poisoned Handover: Unveiling Ties Between Apt Activity In Hong Kong's Pro-Democracy Movement (2014). Source: FireEye. Link: https://app.box.com/s/4ld2qhui8rs1slmh76mzj9vaum353mk8

Operation Poisoned Helmand (2014). Source: ThreatConnect. Link: https://app.box.com/s/emf5ke7j5q12sku7vvvb0c1hbk70fygb

Operation Poisoned Hurricane (2014). Source: FireEye. Link: https://app.box.com/s/f74irgo6g47gr37urjypwcnetjj2ymie

Operation Poisoned News: Hong Kong Users Targeted with Mobile Malware via Local News Links (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/Operation_Poisoned_News.pdf

Operation Potao Express | IOC (2015). Source: ESET WeLiveSecurity. Link: https://github.com/eset/malware-ioc/tree/master/potao

Operation Potao Express: Analysis Of A Cyber-Espionage Toolkit (2015). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/hji6y2fi3nwqbd8mtx6kiy6yckizwq2w

OPERATION PROWLI: MONETIZING 40,000 VICTIM MACHINES (2018). Source: GuardiCore. Link: https://www.guardicore.com/2018/06/operation-prowli-traffic-manipulation-cryptocurrency-mining/

Operation PZChao: a possible return of the Iron Tiger APT (2018). Source: BitDefender. Link: https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/

Operation Quantum Entanglement (2014). Source: FireEye. Link: https://app.box.com/s/qvuhc7j8tle0a83z3iivsz3yz6aok3tv

Operation RAT Cook: Chinese APT actors use fake Game of Thrones leaks as lures (2017). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures

Operation Red Gambler (2018). Source: AhnLab. Link: http://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.91.pdf

OPERATION RED KANGAROO: INDUSTRY'S FIRST DYNAMIC ANALYSIS OF 4M PUBLIC DOCKER CONTAINER IMAGES (2020). Source: Prevasio. Link: https://blog.prevasio.com/2020/12/operation-red-kangaroo-industrys-first.html

Operation Red October (2013). Source: Intel Security-McAfee. Link: https://app.box.com/s/yzybkh6neofhi2wonyn7abjyn2hlfa8f

Operation Roman Holiday Hunting the Russian APT28 group (2018). Source: Microsoft. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/20180713_CSE_APT28_X-Agent_Op-RomanHoliday-Report_v6_1.pdf

Operation Rubia cordifolia (2020). Source: Qianxin. Link: https://mp.weixin.qq.com/s/omacDXAdio88a_f0Xwu-kg

Operation Russiandoll: Adobe & Windows ZeroDay Exploits Likely leveraged By Russia's APT28 (2015). Source: FireEye. Link: https://app.box.com/s/oj4sr8vifeb03qe51newafin81tu8poy

Operation Saffron Rose (2014). Source: FireEye. Link: https://app.box.com/s/pnagcb7vgpqaxen71n2x557m05q7dazl

Operation ShadowHammer (2019). Source: Kaspersky Lab. Link: https://securelist.com/operation-shadowhammer/89992/

Operation Shady RAT (2011). Source: Intel Security-McAfee. Link: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Operation Shaheen (2018). Source: Cylance. Link: https://www.cylance.com/en-us/company/news-and-press/press-releases/cylance-discovers-new-middle-eastern-APT-actor-the-white-company.html

Operation Sharpshooter - Campaign Targets Global Defense, Critical Infrastructure (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/

Operation Sheep: Pilfer-Analytics SDK in Action (2019). Source: Check Point. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.13.Operation_Sheep/Operation_Sheep.pdf

Operation SideCopy (2020). Source: Seqrite. Link: https://www.seqrite.com/blog/operation-sidecopy/

Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

Operation SMN (2014). Source: Novetta. Link: https://www.novetta.com/product-technology/operation-smn/

Operation Snowman: Deputydog Actor Compromises Us Veterans Of Foreign Wars Website (2014). Source: FireEye. Link: https://app.box.com/s/6uv4v8hpnfpka971qk0gd3j4mnm5x7mt

Operation Soft Cell A Worldwide Campaign Against Telecommunications Providers (2019). Source: Cybereason. Link: https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

Operation Spalax: Targeted malware attacks in Colombia (2021). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/

Operation Sphinx (2016). Source: 360 SkyEye System. Link: http://zhuiri.360.cn/report/index.php/2016/07/01/sphinx-apt-c-15/?lang=en

Operation StealthyTrident: corporate software under attack (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

Operation TaskMasters: Cyberespionage in the digital economy age (2019). Source: Positive Technologies. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.22.Operation_TaskMasters/Operation-Taskmasters-2019-eng.pdf

Operation Toohash How Targeted Attacks Work (2014). Source: G Data Software. Link: https://app.box.com/s/11ozmt3fr8pucuo08gnotg6ab22ka7pp

Operation TradeSecret: Cyber Espionage at the Heart of Global Trade (2017). Source: Fidelis Cybersecurity. Link: https://www.fidelissecurity.com/threatgeek/cyberdefense

Operation Transparent Tribe (2016). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/Operation-Transparent-Tribe

Operation Tripoli (2019). Source: Check Point. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.07.01.Operation_Tripoli/Operation%20Tripoli%20.pdf

Operation Tropic Trooper: Relying On Tried-And-Tested Flaws To Infiltrate Secret Keepers (2015). Source: Trend Micro. Link: https://app.box.com/s/h3xtomk798hufzzqxnhn2kjmvt6yrcxh

Operation Wilted Tulip (2017). Source: ClearSky Cybersecurity . Link: https://app.box.com/s/s0c9085u0otvi6slu121mqikt5h5dzvn

Operation Wocao Shining a light on one of China's hidden hacking groups (2019). Source: Fox-IT. Link: https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wacao.pdf

Operation Wocao: Shining a light on one of China's hidden hacking groups (2019). Source: Fox-IT. Link: https://www.fox-it.com/en/news/whitepapers/operation-wocao-shining-a-light-on-one-of-chinas-hidden-hacking-groups/

Operation Woolen-Goldfish When Kittens Go Phishing (2015). Source: Trend Micro. Link: https://app.box.com/s/pqe4y802utfswg27g3jeyaup46zje5b0

Operation_BlackLion (2019). Source: VenusTech. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.18.Operation_BlackLion/Operation_BlackLion_CN_Version.pdf

ORANGEWORM GROUP – KWAMPIRS ANALYSIS UPDATE (2019). Source: S2 Grupo. Link: https://lab52.io/blog/orangeworm-group-kwampirs-analysis-update/

Orcarat - A Whale Of A Tale (2014). Source: PWC. Link: https://app.box.com/s/r3qo159trv793oeqdgsv99swjsxzq8pw

Organized Cybercrime Big in Japan: URLZone Now on the Scene (2016). Source: IBM. Link: https://securityintelligence.com/organized-cybercrime-big-in-japan-urlzone-now-on-the-scene/

OSX Malware Linked to Operation Emmental Hijacks User Network Traffic (2017). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/osx_dok-mac-malware-emmental-hijacks-user-network-traffic/

Outlaw group: Perl-Based Shellbot Looks to Target Organizations via C&C (2018). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.11.01_Outlaw_group/Perl-Based%20Shellbot%20Looks%20to%20Target%20Organizations%20via%20C%26C%20-%20TrendLabs%20Security%20Intelligence%20Blog.pdf

Outlaw is Back, a New Crypto-Botnet Targets European Organizations (2020). Source: Yoroi. Link: https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/

Outlaw Updates Kit to Kill Older Miner Versions, Targets More Systems (2020). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.02.10_Outlaw_Updates/Outlaw%20Updates%20Kit%20to%20Kill%20Older%20Miner%20Versions%2C%20Targets%20More%20Systems.pdf

Pacifier APT (2016). Source: BitDefender. Link: https://app.box.com/s/xcu346jhiokohlj9300q6hif06swac57

Packrat: Seven Years of a South American Threat Actor (2015). Source: Citizen Lab. Link: https://citizenlab.org/2015/12/packrat-report/

Pakistan Sidewinder APT Attack (2020). Source: Qianxin. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.01.01.SideWinder_APT/%5BCN%5D_SideWinder_APT.pdf

PAKISTAN: HUMAN RIGHTS UNDER SURVEILLANCE (2018). Source: Amnesty International. Link: https://www.amnesty.org/en/documents/asa33/8366/2018/en/

Palebot Trojan Harvests Palestinian Online Credentials (2011). Source: Norman Shark. Link: https://app.box.com/s/73rhctcs0kj6s52eeqn509p44a368kuv

Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors (2020). Source: Symantec. Link: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt

Panda Banker Zeros in on Japanese Targets (2018). Source: Arbor Networks. Link: https://www.arbornetworks.com/blog/asert/panda-banker-zeros-in-on-japanese-targets/

Panda's New Arsenal: Part 1 Tmanger (2020). Source: Nippon Telegraph and Telephone Corporation. Link: https://insight-jp.nttsecurity.com/post/102gi9b/pandas-new-arsenal-part-1-tmanger

Panda's New Arsenal: Part 2 Albaniiutas (2020). Source: Nippon Telegraph and Telephone Corporation. Link: https://insight-jp.nttsecurity.com/post/102gkfp/pandas-new-arsenal-part-2-albaniiutas

Panda's New Arsenal: Part 3 Smanager (2020). Source: Nippon Telegraph and Telephone Corporation. Link: https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager

Parlez-vous Fancy? (2017). Source: ThreatConnect. Link: https://threatconnect.com/blog/activity-targeting-french-election/

Partners in crime: North Koreans and elite Russian-speaking cybercriminals (2020). Source: Intel471. Link: https://public.intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals/

Pass the AppleJeus (2019). Source: Objective-See. Link: https://objective-see.com/blog/blog_0x49.html

Pat Bear (APT-C-37) (2019). Source: 360 SkyEye System. Link: https://app.box.com/s/gv5ug3d8shq5d6uuj6vb8nfgemtpznil

Patchwork APT Group Targets US Think Tanks (2018). Source: Volexity. Link: https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/

Patchwork cyberespionage group expands targets from governments to wide range of industries (2016). Source: Symantec. Link: https://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

Pawn Storm Update: Ios Espionage App Found (2015). Source: Trend Micro. Link: https://app.box.com/s/9b7dfetwel6ywbcfai2wa0ja20cym721

Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation (2015). Source: Citizen Lab. Link: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

PEERING INTO GLASSRAT: A Zero Detection Trojan from China (2015). Source: RSA Security. Link: https://app.box.com/s/3jg797vagekvf1xjyz1j49esdhm4fmjs

Permission to Spy: An Analysis of Android Malware Targeting Tibetans (2013). Source: Citizen Lab. Link: https://citizenlab.ca/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/

Pest Control: Taming The Rats (2012). Source: Matasano Security. Link: https://app.box.com/s/k6kyhjnok9n5vqtchm4u1luoluth0j1i

Petya Ransomware (2017). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA17-181A

Phantom in the Command Shell (2020). Source: Prevailion. Link: https://blog.prevailion.com/2020/05/phantom-in-command-shell5.html

Phishing and Web Attacks Targeting Uzbek Human Right Activists and Independent Media (2019). Source: eQualitie. Link: https://equalit.ie/deflect-labs-report-6/

Phishing attack targeting United Nations and humanitarian organizations (2019). Source: Lookout. Link: https://blog.lookout.com/lookout-phishing-ai-discovers-phishing-attack-targeting-humanitarian-organizations

Phishing attacks using third-party applications against Egyptian civil society organizations (2019). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

Phishing Campaign Impersonates Mexico, Peru, Uruguay Government’s e-Procurement Systems (2019). Source: Anomali. Link: https://www.anomali.com/blog/phishing-campaign-impersonates-mexico-peru-uruguay-governments-e-procurement-systems

Phishing Campaign Spoofs United Nations and Multiple Other Organizations (2019). Source: Anomali. Link: https://www.anomali.com/blog/phishing-campaign-spoofs-united-nations-and-multiple-other-organizations

Phishing Campaign targeting French Industry (2018). Source: F-Secure. Link: https://labsblog.f-secure.com/2018/11/26/phishing-campaign-targeting-french-industry/

Phishing Scam Lures Australian Government Contractors Into Disclosing Account Credentials (2019). Source: Anomali. Link: https://www.anomali.com/blog/phishing-scam-lures-australian-government-contractors-into-disclosing-account-credentials

"Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk

and LockerGoga Ransomware (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html"

Piercing the HawkEye: Nigerian Cybercriminals Use a Simple Keylogger to Prey on SMBs Worldwide (2016). Source: Trend Micro. Link: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-piercing-hawkeye.pdf

Pillars of Russia's Desinformation and Propaganda Ecosystem (2020). Source: US Justice Department. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5310207632454191381.pdf

PINCHY SPIDER Affiliates Adopt “Big Game Hunting” Tactics to Distribute GandCrab Ransomware (2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/

Pirates of Brazil: Integrating the Strengths of Russian and Chinese Hacking Communities (2019). Source: Recorded Future. Link: https://www.recordedfuture.com/brazilian-hacking-communities/

PKPLUG: Chinese Cyber Espionage Group Attacking Asia (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/

PLA Unit 61398 (2013). Source: Mandiant. Link: https://web.archive.org/web/20130219155150/http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Planetary Reef: Cybercriminal Hosting and Phishing-as-a-Service Threat Actor (2020). Source: PhishLabs. Link: https://info.phishlabs.com/blog/planetary-reef-cybercriminal-hosting-and-phishing-as-a-service-threat-actor

PLATINUM continues to evolve, find ways to maintain invisibility (2017). Source: Microsoft. Link: https://app.box.com/s/iryvk6gcqx4qyzfn245ruoo7syyex2yv

Platinum is back (2019). Source: Kaspersky Lab. Link: https://securelist.com/platinum-is-back/91135/

PLATINUM Targeted attacks in South and Southeast Asia (2016). Source: Microsoft. Link: http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

Playing defense against Gamaredon Group (2020). Source: Elastic. Link: https://www.elastic.co/pt/blog/playing-defense-against-gamaredon-group

PLEAD downloader used by BlackTech (2018). Source: JPCERT. Link: https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

Plugx Goes To The Registry (And India) (2015). Source: SophosLabs. Link: https://app.box.com/s/jfuf6eo3az72qrvh6ueke42ft9f23ztz

PlugX Threat Activity in Myanmar (2015). Source: Arbor Networks. Link: http://pages.arbornetworks.com/rs/082-KNA-087/images/ASERT%20Threat%20Intelligence%20Brief%202015-05%20PlugX%20Threat%20Activity%20in%20Myanmar.pdf

PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors (2020). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html

Poison Ivy Group (APT-C-01) (2018). Source: 360 SkyEye System. Link: http://blogs.360.cn/post/APT_C_01_en.html

Poison Ivy: Assessing Damage And Extracting Intelligence (2013). Source: FireEye. Link: https://app.box.com/s/7gw9d1cbuvygb3qamjytpgh9nbmk7cbw

"PoisonIvy adapts to communicate through Authentication

Proxies (2015). Source: JPCERT. Link: http://blog.jpcert.or.jp/2015/07/poisonivy-adapts-to-communicate-through-authentication-proxies.html"

Poking the Bear: Three-Year Campaign Targets Russian Critical Infrastructure (2018). Source: Cylance. Link: https://threatvector.cylance.com/en_us/home/poking-the-bear-three-year-campaign-targets-russian-critical-infrastructure.html

Police Story: Hacking Team Government Surveillance Malware (2014). Source: Citizen Lab. Link: https://citizenlab.ca/wp-content/uploads/2015/03/Police-Story-Hacking-Team%E2%80%99s-Government-Surveillance-Malware.pdf

Ponmocup A giant hiding in the shadows (2015). Source: Fox-IT. Link: https://foxitsecurity.files.wordpress.com/2015/12/foxit-whitepaper_ponmocup_1_1.pdf

Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage (2016). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/

PoshC2 (2020). Source: LAC JP. Link: https://www.lac.co.jp/lacwatch/people/20200424_002177.html

Post Soviet Bank Heists (2017). Source: Trustwave. Link: https://www.trustwave.com/Resources/Library/Documents/Post-Soviet-Bank-Heists/

PowDesk: Targeted APT34 Campaign Against LANDesk Users (2020). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/powdesk-apt34/

Power-Shell-based malware linked to Iranian group APT34 (OilRig and HelixKitten) (2020). Source: Volon. Link: https://volon.io/2020/01/14/power-shell-based-malware-linked-to-iranian-group-apt34-oilrig-and-helixkitten/

PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs (2016). Source: Volexity. Link: https://app.box.com/s/wd73vlkdiry8hibkbqvmtsn0bhmzkhgk

PRIMITIVE BEAR USES A NATO-THEMED LURE DOCUMENT TO TARGET UKRAINIAN GOVERNMENT AND DEFENSE AGENCIES (2019). Source: Telsy. Link: https://blog.telsy.com/primitive-bear-operation-uses-nato-themed-lure-documents-to-target-ukrainian-gov-and-defense-agencies/

Prince of Persia Game Over (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/

Prince of Persia: Infy Malware Active In Decade of Targeted Attacks (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/zkjmru7uknf1p90mqn81ycf867le78tn

Privileges and Credentials: Phished at the Request of Counsel (2017). Source: FireEye. Link: https://app.box.com/s/sj821a63jgyif6xv2yz4gnut8kxgg7lo

Pro-Chinese Inauthentic Network Debuts English-Language Videos (2020). Source: Graphika. Link: https://graphika.com/reports/spamouflage-dragon-goes-to-america/

Pro-Chinese Spam Network Tries Again (2020). Source: Graphika. Link: https://graphika.com/reports/return-of-the-spamouflage-dragon-1/

Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting (2020). Source: SentinelOne. Link: https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/

Proactive Threat Identification Neutralizes Remote Access Trojan Efficacy (2015). Source: Recorded Future. Link: http://go.recordedfuture.com/hubfs/reports/threat-identification.pdf

Probing Pawn Storm : Cyberespionage Campaign Through Scanning, Credential Phishing and More (2020). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.19_Probing_Pawn_Storm/wp-pawn-storm-in-2019.pdf

Profiling An Enigma: The Mystery Of North Korea's Cyber Threat Landscape (2014). Source: Hewlett Packard. Link: http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf

Profiling of TA505 Threat Group That Continues to Attack the Financial Sector (2020). Source: AhnLab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/Profiling_of_TA505_Threat_Group.pdf

Project Camerashy: Closing The Aperture On China's Unit 78020 (2015). Source: ThreatConnect. Link: https://www.threatconnect.com/camerashy/

Project DREAD (2019). Source: Reuters. Link: https://www.reuters.com/investigates/special-report/usa-raven-whitehouse/

Project TajMahal – a sophisticated new APT framework (2019). Source: Kaspersky Lab. Link: https://securelist.com/project-tajmahal/90240/

ProjectM: Link Found Between Pakistani Actor and Operation Transparent Tribe (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/03/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe/?utm_medium=email&utm_source=Adobe%20Campaign&utm_campaign=Unit%2042%20Blog%20Updates%2031Mar16

PROMETHIUM and NEODYMIUM: Parallel zero-day attacks targeting individuals in Europe (2016). Source: Microsoft. Link: http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf

PROMETHIUM extends global reach with StrongPity3 APT (2020). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html

Prototype Nation: The Chinese Cybercriminal Underground in 2015 (2015). Source: Trend Micro. Link: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/prototype-nation-the-chinese-cybercriminal-underground-in-2015/?utm_source=siblog&utm_medium=referral&utm_campaign=2015-cn-ug

"Publicly Available Tools Seen in Cyber Incidents Worldwide

(2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/AA18-284A"

Putter Panda (2014). Source: CrowdStrike. Link: https://app.box.com/s/ugahgfd07evh7q0h8lnb00brew4ixvdk

Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns (2014). Source: Electronic Frontier Foundation. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2013/quantum_of_surveillance4d.pdf

Quasar Open-Source Remote Administration Tool (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/analysis-reports/AR18-352A

Quick and dirty over APT37 (aka Group123, aka ScarCruft) Android spying backdoor (2019). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/group123-apt37-quick-and-dirty-over-their-malicious-jpge-viewer-mobile-app/

Ramsay: A cyber-espionage toolkit tailored for air-gapped networks (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

RANCOR APT: Suspected targeted attacks against South East Asia (2019). Source: Meltx0r. Link: https://meltx0r.github.io/tech/2019/09/11/rancor-apt.html

Rancor: Cyber Espionage Group Uses New Custom Malware to Attack Southeast Asia (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/

RANCOR: Targeted Attacks in South East Asia Using PLAINTEE and DDKONG Malware Families (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

Rancor: The Year of The Phish (2019). Source: Check Point. Link: https://research.checkpoint.com/rancor-the-year-of-the-phish/

Ransomware Impacting Pipeline Operations (2020). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/aa20-049a

Ransomware, Trojan and Miner together against “PIK-Group” (2019). Source: Marco Ramilli. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.02.28_RIK_Group/Ransomware%2C%20Trojan%20and%20Miner%20together%20against%20%E2%80%9CPIK-Group%E2%80%9D.pdf

Rat In A Jar: A Phishing Campaign Using Unrecom (2014). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/hhfmfv9itrx2mabe5m441a381zvc5jul

RATicate: an attacker's waves of information-stealing malware (2020). Source: SophosLabs. Link: https://news.sophos.com/en-us/2020/05/14/raticate/

Read The Manual A guide to the RTM Banking Trojan (2017). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Read-The-Manual.pdf

Recent Cloud Atlas activity (2019). Source: Kaspersky Lab. Link: https://securelist.com/recent-cloud-atlas-activity/92016/

Recent InPage Exploits Lead to Multiple Malware Families (2017). Source: Palo Alto Networks. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2017/2017.11.02.InPage_Exploits/Recent%20InPage%20Exploits%20Lead%20to%20Multiple%20Malware%20Families.pdf

Recent MuddyWater-associated BlackWater campaign shows signs of new anti-detection techniques (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html

Recent Observations in Tibet-Related Information Operations: Advanced social engineering for the distribution of LURK malware (2012). Source: Citizen Lab. Link: https://citizenlab.org/2012/07/recent-observations/

Recent Watering Hole Attacks Attributed To Apt Group Th3Bug Using Poison Ivy (2014). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/

Recent Winnti Infrastructure and Samples (2017). Source: ClearSky Cybersecurity . Link: http://www.clearskysec.com/winnti/

Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware (2017). Source: Citizen Lab. Link: https://citizenlab.org/2017/06/reckless-exploit-mexico-nso/

Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware (2017). Source: Citizen Lab. Link: https://citizenlab.org/2017/06/more-mexican-nso-targets/

Reckless VI Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague (2018). Source: Citizen Lab. Link: https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

RECKLESS VII - Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware (2019). Source: Citizen Lab. Link: https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/

ReconHellcat Uses NIST Theme as Lure To Deliver New BlackSoul Malware (2021). Source: Quointelligence. Link: https://quointelligence.eu/2021/01/reconhellcat-uses-nist-theme-as-lure-to-deliver-new-blacksoul-malware/

Recovering From Shamoon (2012). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/fjucrojt5ldxio2sbvsql7syv46l6p4g

Red Line Drawn: China Recalculates Its Use Of Cyber Espionage (2016). Source: FireEye. Link: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

RedAlpha: New Campaigns Discovered Targeting the Tibetan Community (2018). Source: Recorded Future. Link: https://www.recordedfuture.com/redalpha-cyber-campaigns/

REDCURL The pentest you didn't know about (2020). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5370732951539550297.pdf

Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance (2014). Source: Symantec. Link: https://app.box.com/s/at56dm7anwlk35y4cp4ung9qwgiz6bn1

Regional Conflict and Cyber Blowback (2013). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/regional-conflict-and-cyber-blowback/

Registers as “Default Print Monitor”, but is a malicious downloader. Meet DePriMon (2019). Source: ESET WeLiveSecurity. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.21.DePriMon/Registers%20as%20%E2%80%9CDefault%20Print%20Monitor%E2%80%9D%2C%20but%20is%20a%20malicious%20downloader.%20Meet%20DePriMon.pdf

Rehashed RAT Used in APT Campaign Against Vietnamese Organizations (2017). Source: Fortinet. Link: https://www.fortinet.com/blog/threat-research/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations.html

Release the Kraken: Fileless APT attack abuses Windows Error Reporting service (2020). Source: MalwareBytes. Link: https://blog.malwarebytes.com/malwarebytes-news/2020/10/kraken-attack-abuses-wer-service/

Remcos RAT Revisited: A Colombian Coronavirus-Themed Campaign (2021). Source: BitDefender. Link: https://labs.bitdefender.com/2021/01/remcos-rat-revisited-a-colombian-coronavirus-themed-campaign/

Remote Control Interloper: Analyzing New Chinese htpRAT Malware Attacks Against ASEAN (2017). Source: RISKIQ. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/RiskIQ-htpRAT-Malware-Attacks.pdf

Repackaging Open Source BeEF for Tracking and More (2016). Source: Kaspersky Lab. Link: https://securelist.com/blog/software/74503/freezer-paper-around-free-meat/

Report: OceanLotus APT Group Leveraging Steganography (2019). Source: Cylance. Link: https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html

RESEARCH SPOTLIGHT: NEEDLES IN A HAYSTACK (2016). Source: Cisco Talos. Link: https://app.box.com/s/6tlgwpp0u2lzahlrhtymkp2nnbtd421f

Resurgent Iron Liberty Targeting Energy Sector (2019). Source: Dell Secureworks. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.07.24.Resurgent_Iron_Liberty/Resurgent%20Iron%20Liberty%20Targeting%20Energy%20Sector.pdf

Retrohunting APT37: North Korean APT used VBA self decode technique to inject RokRat (2021). Source: MalwareBytes. Link: https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-self-decode-technique-to-inject-rokrat/

Revealing Targets of the Iranian MuddyWater Group, Extracted from their C2 (2020). Source: ClearSky Cybersecurity . Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/107607.pdf

Revenge is a Dish Best Served… Obfuscated? (2019). Source: Binary Defense. Link: https://www.binarydefense.com/revenge-is-a-dish-best-served-obfuscated/

Revenge RAT targeting users in South America (2020). Source: Uptycs. Link: https://www.uptycs.com/blog/revenge-rat-targeting-users-in-south-america

RevengeHotels: cybercrime targeting hotel front desks worldwide (2019). Source: Kaspersky Lab. Link: https://securelist.com/revengehotels/95229/

Reverse-engineering DUBNIUM (2016). Source: Microsoft. Link: https://app.box.com/s/f0xelxxs6ey9nms9fox1uugy8nuof40t

Reverse-engineering DUBNIUM's Flash-targeting exploit (2016). Source: Microsoft. Link: https://app.box.com/s/rsvvnrm7ct991olqsvbqrie614xt9f3b

Reversing malware in a custom format: Hidden Bee elements (2018). Source: MalwareBytes. Link: https://blog.malwarebytes.com/threat-analysis/2018/08/reversing-malware-in-a-custom-format-hidden-bee-elements/

Reversing The Inception APT Malware (2015). Source: Blue Coat Systems. Link: https://app.box.com/s/sctzfr6aoagpzb9aoajcodvn6we7e055

Reviving MuddyC3 Used by MuddyWater (IRAN) APT (2020). Source: ShellsSystems. Link: https://shells.systems/reviving-leaked-muddyc3-used-by-muddywater-apt/

RIGGING COMPROMISE - RIG EXPLOIT KIT (2016). Source: Cisco Talos. Link: http://blog.talosintel.com/2016/01/rigging-compromise.html

Roaming Tiger (2014). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/1q4787ruef22tvkgc7h82j6ib6qpc8v0

Rocket Kitten: A Campaign With 9 Lives (2015). Source: Check Point. Link: https://app.box.com/s/vhe51fr5m6kqqzbkkcuukta6nucn9p6a

Rocketman APT Campaign Returned to Operation Holiday Wiper (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2089

ROKRAT Reloaded (2017). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html

Rootkit analysis Use case on HideDRV (2016). Source: Sekoia. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf

Royal Road! Re:Dive (2021). Source: Nao-Sec. Link: https://nao-sec.org/2021/01/royal-road-redive.html

RSA Incident Response: An APT Case Study (2015). Source: RSA Security. Link: https://app.box.com/s/tjoi82cp4iq6xx561qcu3xjr2rmfgmo1

RSA Research Terracotta VPN: Enabler Of Advanced Threat Anonymity (2015). Source: RSA Security. Link: https://app.box.com/s/cx1sjzb1q7slnjho5n1n0iuc7y9om2ll

Running for Office: Russian APT Toolkits Revealed (2016). Source: Recorded Future. Link: https://www.recordedfuture.com/russian-apt-toolkits/

Russia and nation-state hacking tactics: A report from Cybereason Intelligence Group (2017). Source: Cybereason. Link: https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity

Russian Army Exhibition Decoy Leads to New BISKVIT Malware (2018). Source: Fortinet. Link: https://www.fortinet.com/blog/threat-research/russian-army-exhibition-decoy-leads-to-new-biskvit-malware.html

Russian Bank Offices Hit with Broad Phishing Wave (2017). Source: RSA Security. Link: https://app.box.com/s/xgtoqdnl8tdviws0jgvxnj8oniia4qqr

Russian Cyber Attack Campaigns and Actors (2020). Source: IronNet. Link: https://ironnet.com/blog/russian-cyber-attack-campaigns-and-actors/

Russian Cyber Espionage Campaign - Sandworm Team (2014). Source: iSIGHT Partners. Link: https://app.box.com/s/k0vbq8vx0z8qg3s4ycit1kc99cg5ay27

Russian Cyber Operations on Steroids (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/

Russian Cyberwar On Georgia (2008). Source: Ministry of Foreign Affairs of Georgia. Link: https://app.box.com/s/ce4fr8p0mxv2pjcvh4pmma1q7oqc4vnc

Russian financial cybercrime: how it works (2015). Source: Kaspersky Lab. Link: https://securelist.com/analysis/publications/72782/russian-financial-cybercrime-how-it-works/

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA18-074A

Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware (2020). Source: US Justice Department. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/TA18-106A

Ryuk Ransomware Attack: Rush to Attribution Misses (2019). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/

Ryuk ransomware targeting organisations globally (2019). Source: National Cyber Security Centre. Link: https://www.ncsc.gov.uk/news/ryuk-advisory

Safe A Targeted Threat (2013). Source: Trend Micro. Link: https://app.box.com/s/0yh8mn02v2wrehl9yaddrb8rjdzieeqb

SAIGON, the Mysterious Ursnif Fork (2020). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html

Sakula Reloaded (2015). Source: CrowdStrike. Link: http://www.crowdstrike.com/blog/sakula-reloaded/

SamSam Ransomware (2018). Source: US-CERT. Link: https://www.us-cert.gov/ncas/alerts/AA18-337A

Sandvine’s PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads? (2018). Source: Citizen Lab. Link: https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Sandworm intrusion set campaign targeting Centreon systems (2021). Source: Agence nationale de la sécurité des systèmes d'information. Link: https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-005/

Satellite Turla: APT Command and Control in the Sky (2015). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

Sayad (Flying Kitten) Infostealer: Is This The Work Of The Iranian Ajax Security Team? (2014). Source: Vinsula. Link: https://app.box.com/s/hjjb0aysslxse1ehpyt5ny68lf8tyctg

Scanbox Framework: Who's Affected, And Who's Using It? (2014). Source: PWC. Link: https://app.box.com/s/u273q9utje6wds8mtv17efskdu5oj8la

ScanBox II (2015). Source: PWC. Link: https://app.box.com/s/o83u5pekus9251w0cl5lo2m1k5u0u2vn

Scanbox: A Reconnaissance Framework Used With Watering Hole Attacks (2014). Source: AlienVault. Link: https://app.box.com/s/vlbe0y40djeaadl2l4iqdm13cju3v3n6

Scarab Attackers Took Aim At Select Russian Targets Since 2012 (2015). Source: Symantec. Link: https://app.box.com/s/pkoancu0b09aifvm2qfu6tdl8w0l5dqz

ScarCruft continues to evolve, introduces Bluetooth harvester (2019). Source: Kaspersky Lab. Link: https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/

Scarlet Mimic (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/zhour42vz6sxf7aws3oj70i1rd5ib8kx

Scattered Canary The Evolution and Inner Workings of a West African Cybercriminal Startup Turned BEC Enterprise (2019). Source: AGARI. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/scattered-canary.pdf

Schrodinger's Cat Video and the Death of Clear-Text (2014). Source: Citizen Lab. Link: https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/

Schroedinger’s Pet(ya) (2017). Source: Kaspersky Lab. Link: https://securelist.com/schroedingers-petya/78870/

"Sea Turtle keeps on swimming, finds new victims, DNS hijacking techniques

(2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html?m=1"

Second Wave of Shamoon 2 Attacks Identified (2017). Source: Palo Alto Networks. Link: https://www.threatminer.org/_reports/2017/Second Wave of Shamoon 2 Attacks Identified - Palo Alto Networks.pdf

Secret Malware In European Union Attack Linked To U.S. And British Intelligence (2014). Source: Symantec. Link: http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance

Secrets Of The Comfoo Masters (2013). Source: Dell Secureworks. Link: https://app.box.com/s/70bcgwlwqpp43spjxnyk2f7h96lg0718

SectorB06 using Mongolian language in lure document (2019). Source: Threat Recon Team. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.04.30.SectorB06_Mongolian/SectorB06%20using%20Mongolian%20language%20in%20lure%20document.pdf

SectorD01: When anime goes cyber (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/10/24/sectord01-when-anime-goes-cyber/

SectorJ04 Group's Increased Activity in 2019 (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/08/29/sectorj04-groups-increased-activity-in-2019/

Security Phishing Diplomacy (2018). Source: Area 1. Link: https://cdn.area1security.com/reports/Area-1-Security-PhishingDiplomacy.pdf

Sednit (2017). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Sednit adds two zero-day exploits using Trumps attack on Syria as a decoy (2017). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/Sednit.eset.2017.pdf

Sednit update: Analysis of Zebrocy (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/

Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group

Senior Mexican Legislators and Politicians Targeted with NSO Spyware (2017). Source: Citizen Lab. Link: https://citizenlab.ca/2017/06/more-mexican-nso-targets/

Several Polish banks hacked, information stolen by unknown attackers (2017). Source: Badcyber. Link: https://app.box.com/s/7s2s43nlaqxllf4ugef1vyvkm3mr0ryt

Shade Ransomware Hits High-Tech, Wholesale, Education Sectors in U.S, Japan, India, Thailand, Canada (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/shade-ransomware-hits-high-tech-wholesale-education-sectors-in-u-s-japan-india-thailand-canada/

ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.06.27.ShadowGate_Returns/ShadowGate%20Returns%20to%20Worldwide%20Operations%20With%20Evolved%20Greenflash%20Sundown%20Exploit%20Kit.pdf

ShadowPad: new activity from the Winnti group (2020). Source: Positive Technologies. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5454144652401707044.pdf

Shadows From the Past Threaten Italian Enterprises (2020). Source: Yoroi. Link: https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

Shadows In The Cloud: Investigating Cyber Espionage 2.0 (2010). Source: Shadowserver Foundation. Link: https://app.box.com/s/mxffbrs4ju2yeoa47sbeym6n5zm1hnf3

Shamoon / DiskTrack Malware IoC for recent Oil & Gas Energy sector attack (2018). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/shamoon-disktrack-ioc-oil-gas-energy-attack/

Shamoon 2 Delivering Disttrack (2017). Source: Palo Alto Networks. Link: https://www.threatminer.org/_reports/2017/Shamoon 2_ Delivering Disttrack - Palo Alto Networks Blog.pdf

Shamoon 2012 Complete Analysis (2019). Source: MalwareInDepth. Link: https://malwareindepth.com/shamoon-2012/

Shamoon 3 Targets Oil and Gas Organization (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/12/shamoon-3-targets-oil-gas-organization/

Shamoon 3: Modified Open-Source Wiper Contains Verse from the Quran (2018). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/shamoon-3-modified-open-source-wiper-contains-verse-from-the-quran/

Shamoon PowerShell Indicate Open Source RAT (2017). Source: Booz Allen Hamilton. Link: https://www.threatminer.org/_reports/2017/Shamoon PowerShell Indicate Open-Source RAT _ Cyber4Sight.pdf

Shamoon Returns to Wipe Systems in Middle East, Europe (2018). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-returns-to-wipe-systems-in-middle-east-europe

Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

Sharpening the Machete (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/08/05/sharpening-machete-cyberespionage/

Shedding Light on BlackEnergy With Open Source Intelligence (2016). Source: Recorded Future. Link: https://www.recordedfuture.com/blackenergy-malware-analysis/

Shedding Skin – Turla's Fresh Faces (2018). Source: Kaspersky Lab. Link: https://securelist.com/shedding-skin-turlas-fresh-faces/88069/

Shell Crew Variants Continue to Fly Under Big AV Radar (2017). Source: Cylance. Link: https://www.threatminer.org/_reports/2017/Shell Crew Variants Continue to Fly Under Big AVâ€™s Radar - Cylance.pdf

Shell_Crew (Deep Panda) (2015). Source: RSA Security. Link: http://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf

SHELLTEA + POSLURP MALWARE: memory resident point-of-sale malware attacks industry (2017). Source: root9b. Link: https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp_0.pdf

Shifting in the Wind: WINDSHIFT Attacks Target Middle Eastern Governments (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/shifting-in-the-wind-windshift-attacks-target-middle-eastern-governments/

Shifting Tactics Tracking Changes In Years Long Espionage Campaign Against Tibetans (2016). Source: Citizen Lab. Link: https://citizenlab.org/2016/03/shifting-tactics/

Shifts in Underground Markets (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5371064119287874977.pdf

Shiny Object? Guccifer 2.0 and the DNC Breach (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/guccifer-2-0-dnc-breach/

Shooting Elephants (2015). Source: Netzpolitik.org. Link: https://app.box.com/s/qog0dtpldhebhlasl12z3j82e0uv8t26

SideCopy An insight into Transparent Tribe's sub-division which has been incorrectly attributed for years (2020). Source: Seqrite. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5447658130798282764.pdf

SideWinder 2020 H1 (2020). Source: Qianxin. Link: https://mp.weixin.qq.com/s/5mBqxf_v6G006EnjECoTHw

Sidewinder Targeted Attack Against Android In The Golden Age Of Ad Libraries (2014). Source: FireEye. Link: https://app.box.com/s/qwg36lcvf9iaz3alks4w24btqcxmzlkq

SideWinder Uses South Asian Issues for Spear Phishing, Mobile Attacks (2020). Source: Trend Micro. Link: https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html

Silence 2.0 (2020). Source: Group-IB. Link: https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf

Silence 2.0 Going Global (2019). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/34941.pdf

Silence group targeting Russian Banks via Malicious CHM (2019). Source: REAQTA. Link: https://reaqta.com/2019/01/silence-group-targeting-russian-banks/

Silence: Moving into the darkside (2018). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/silence_moving-into-the-darkside.pdf

Silent Librarian APT right on schedule for 20/21 academic year (2020). Source: MalwareBytes. Link: https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/

SilverTerrier – 2018 Nigerian Business Email Compromise (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/silverterrier-2018-nigerian-business-email-compromise/

SILVERTERRIER: The Next Evolution in Nigerian Cybercrime (2016). Source: Palo Alto Networks. Link: https://www.paloaltonetworks.com/resources/research/silverterrier-next-evolution-nigerian-cybercrime

SilverTerrier: the rise of Nigerian business email compromise (2018). Source: Palo Alto Networks. Link: https://www.paloaltonetworks.com/resources/research/silverterrier-next-evolution-nigerian-cybercrime

Simjacker Technical Report (2019). Source: blackhat. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/AdaptiveMobile_Security_Simjacker_Technical_Paper_v1.01.pdf

Sinkholing Volatile Cedar DGA Infrastructure (2015). Source: Kaspersky Lab. Link: https://securelist.com/sinkholing-volatile-cedar-dga-infrastructure/69421/

Sk Hack By An Advanced Persistent Threat (2011). Source: Command Five. Link: https://app.box.com/s/c911g2eqxck6va9cdn9vync5628zrreb

Skeleton Key Malware Analysis (2015). Source: Dell Secureworks. Link: https://app.box.com/s/elb9hgj4rvcajilnlh67kpgoskjqjra0

Skygofree (2018). Source: Kaspersky Lab. Link: https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

Skygofree: Following in the footsteps of HackingTeam (2018). Source: Kaspersky Lab. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.01.16.skygofree/Skygofree_%20Following%20in%20the%20footsteps%20of%20HackingTeam%20-%20Securelist.pdf

Skywiper (A.K.A. Flame A.K.A. Flamer): A Complex Malware For Targeted Attacks (2012). Source: Laboratory of Cryptography and System Security (CrySyS Lab). Link: https://app.box.com/s/ebeqddqmxdjqttnqjr1xzi7agiqusrac

Slicing and Dicing CVE-2018-5002 Payloads: New CHAINSHOT Malware (2018). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/unit42-slicing-dicing-cve-2018-5002-payloads-new-chainshot-malware/

SLUB Gets Rid of GitHub, Intensifies Slack Use (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.07.16.SLUB/SLUB%20Gets%20Rid%20of%20GitHub%2C%20Intensifies%20Slack%20Use.pdf

Snake Campaign & Cyber Espionage Toolkit (2014). Source: BAE Systems Detica. Link: https://app.box.com/s/xmeq5ajvmzux1appt1qvd8wme7k13o63

Snake In The Grass: Python-based Malware Used For Targeted Attacks (2014). Source: Blue Coat Systems. Link: https://www.bluecoat.com/security-blog/2014-06-10/snake-grass-python-based-malware-used-targeted-attacks

Social Engineering and Malware in Syria: EFF and Citizen Lab's Latest Report on the Digital Battlefield (2013). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2013/12/social-engineering-and-malware-syria-eff-and-citizen-labs-latest-report-digital

Sofacy Activity (2018). Source: Kaspersky Lab. Link: https://securelist.com/a-slice-of-2017-sofacy-activity/83930/

Sofacy APT hits high profile targets with updated toolset (2015). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/

Sofacy Attacks Multiple Government Entities (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/02/unit42-sofacy-attacks-multiple-government-entities/

Sofacy Continues Global Attacks and Wheels Out New 'Cannon' Trojan (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/

Sofacy Creates New 'Go' Variant of Zebrocy Tool (2018). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/

Sofacy Group's Parallel Attacks (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

Sofacy II_ Same Sofacy, Different Day (2015). Source: PWC. Link: https://app.box.com/s/dm3fbeb7hl95ilno014ftskoc1vi7n1r

Sofacy Uses DealersChoice to Target European Government Agency (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/

Sofacy's Komplex OS X Trojan (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/w1qrcz1z9bx2dwt4gegv0h940ex35hlt

South Sudan: "These walls have ears": The chilling effect of surveillance in South Sudan (2021). Source: Amnesty International. Link: https://www.amnesty.org/en/documents/afr65/3577/2021/en/

Southeast Asia: An Evolving Cyber Threat Landscape (2015). Source: FireEye. Link: https://app.box.com/s/h8kx7u7euolv1d6kjup0bxoujjikcbil

Sowbug: Cyber espionage group targets South American and Southeast Asian governments (2017). Source: Symantec. Link: https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Spam Campaign Targets Colombian Entities with Custom-made 'Proyecto RAT,' Uses Email Service YOPmail for C&C (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.07.18.Proyecto_RAT_Colombian/Appendix_Spam_Campaign_Targets_Colombian_Entities_with_Custom_made_Proyecto_RAT_Uses_Email_Service_YOPmail_for_C%26C.pdf

Spear Phishing Campaign Targets Ukraine Government and Military; Infrastructure Reveals Potential Link to So-Called Luhansk People's Republic (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html

Spear Phishing Techniques Used in Attacks Targeting the Mongolian Government (2017). Source: FireEye. Link: https://www.threatminer.org/_reports/2017/Spear Phishing Techniques Used in Attacks Targeting the Mongolian Government - FireEye.pdf

Spear-phishing campaign targeting Qatar and Turkey (2018). Source: REAQTA. Link: https://reaqta.com/2018/12/spear-phishing-targeting-qatar-turkey/

Sphinx (APT-C-15) Targeted cyber-attack in the Middle East (2016). Source: 360 SkyEye System. Link: https://ti.360.com/upload/report/file/rmsxden20160721.pdf

Spoofing the European Parliament: Analysis of the Repurposing of Legitimate Content in Targeted Malware Attacks (2012). Source: Citizen Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2012/Spoofing-The-European-Parliament.pdf

Spying on a budget (2018). Source: Citizen Lab. Link: https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/

Spyware. HackingTeam (2013). Source: Kaspersky Lab. Link: https://securelist.com/analysis/publications/37064/spyware-hackingteam/

State of Cybersecurity in Asia-Pacific (2017). Source: Palo Alto Networks. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/the-state-of-cybersecurity-in-asia-pacific.pdf

State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack (2019). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

State-Sponsored SCADA Malware targeting European Energy Companies (2016). Source: SentinelOne. Link: https://sentinelone.com/blogs/sfg-furtims-parent/

Stealth Mango and Tangelo (2018). Source: Lookout. Link: https://blog.lookout.com/stealth-mango

STOLEN PENCIL Campaign Targets Academia (2018). Source: Arbor Networks. Link: https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia

Stopping Serial Killer: Catching the Next Strike: Dridex (2021). Source: Check Point. Link: https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/amp/

Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator (2020). Source: Citizen Lab. Link: https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/

Strider: Cyberespionage group turns eye of Sauron on targets (2016). Source: Symantec. Link: http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets

StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure (2020). Source: BitDefender. Link: https://labs.bitdefender.com/2020/06/strongpity-apt-revealing-trojanized-tools-working-hours-and-infrastructure/

StrongPity2 spyware replaces FinFisher in MitM campaign – ISP involved? (2017). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/

Study of the APT attacks on state institutions in Kazakhstan and Kyrgyzstan (2020). Source: DrWeb. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5246831700624803765.pdf

Study of the ShadowPad APT backdoor and its relation to PlugX (2020). Source: DrWeb. Link: https://news.drweb.com/show/?i=14048&lng=en

Studying Donot Team (2019). Source: Positive Research. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.25_Donot_Team/Studying%20Donot%20Team.pdf

Stuxnet 0.5: The Missing Link (2013). Source: Symantec. Link: https://app.box.com/s/jzbxpm7m7kakhubocrrerq0myig6befb

"Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments

(2019). Source: Dragos. Link: https://dragos.com/resource/stuxnet-to-crashoverride-to-trisis-evaluating-the-history-and-future-of-integrity-based-attacks-on-industrial-environments/"

Stuxnet Under The Microscope (2011). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/2mmdr5vhhrjt2prszn167a0v58az9put

Stuxnet/Duqu: The Evolution Of Drivers (2011). Source: Kaspersky Lab. Link: https://app.box.com/s/shakkou3wcgwfq5u83jncdit7cmmw151

Suckfly: Revealing the secret life of your code signing certificates (2016). Source: Symantec. Link: https://app.box.com/s/p3tmorslyk9q1s3s6eul4xa4148o6fp2

Summary of Iranian Advanced Persistent Threat (APT) 34 (2019). Source: Michael Lortz. Link: https://medium.com/@HybridAnalyst/summary-of-iranian-advanced-persistent-team-apt-34-7624d213d20e

Sunburst backdoor – code overlaps with Kazuar (2021). Source: Kaspersky Lab. Link: https://securelist.com/sunburst-backdoor-kazuar/99981/

Supply Chain – The Major Target of Cyberespionage Groups (2019). Source: Resecurity. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.08.Supply_Chain_Groups/Supply%20Chain%20%E2%80%93%20The%20Major%20Target%20of%20Cyberespionage%20Groups.pdf

Supply Chain Analysis: From Quartermaster To Sunshopfireeye (2013). Source: FireEye. Link: https://app.box.com/s/cpnh3qzju92xffn9qtlw45vceuleqh6d

Supply Chain Attack Operation Red Signature Targets South Korean Organizations (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations

Supply chain attacks: threats targeting service providers and design offices (2019). Source: Agence nationale de la sécurité des systèmes d'information. Link: https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-005/

Supply Chain Attacks. Threats targeting service providers and design offices (2019). Source: Agence nationale de la sécurité des systèmes d'information. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/CERTFR-2019-CTI-005.pdf

Sure, I'll take that! New ComboJack Malware Alters Clipboards to Steal Cryptocurrency (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/03/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/

Surtr: Malware Family Targeting The Tibetan Community (2013). Source: Citizen Lab. Link: https://app.box.com/s/m57wv4yn4wsa0j2bj6yuj23bzyrq5rg8

Survival Of The Fittest: New York Times Attackers Evolve Quickly (2013). Source: FireEye. Link: https://app.box.com/s/fkg2mxeqpb2ivx9neyz6bseopy1dfg5p

Suspected analysis and traceability of recent attack samples of an organization in Pakistan (2018). Source: Xiaohe. Link: https://paper.tuisec.win/detail/eaff0936fcdaaa6

Suspected BITTER APT Continues Targeting Government of China and Chinese Organizations (2019). Source: Anomali. Link: https://www.anomali.com/blog/suspected-bitter-apt-continues-targeting-government-of-china-and-chinese-organizations

Suspected BITTER organization's recent analysis of targeted attacks against China and Pakistan (2019). Source: 360 SkyEye System. Link: https://cert.360.cn/report/detail?id=137867e159331b7a968aa45050502d13

Suspected Molerats' New Attack in the Middle East (2019). Source: 360 SkyEye System. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.02.14.Molerats_APT/suspected-molerats-new-attack-in-the-middle-east-cn.pdf

Suspected North Korean Cyber Espionage Campaign Targets Multiple Foreign Ministries and Think Tanks (2019). Source: Anomali. Link: https://www.anomali.com/blog/suspected-north-korean-cyber-espionage-campaign-targets-multiple-foreign-ministries-and-think-tanks

Suspected Sapphire Mushroom (APT-C-12) malicious LNK files (2020). Source: Bitofhex. Link: https://bitofhex.com/2020/02/10/sapphire-mushroom-lnk-files/

SWEED Targeting Precision Engineering Companies in Italy (2019). Source: Marco Ramilli. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.10.28_SWEED_Italy/SWEED%20Targeting%20Precision%20Engineering%20Companies%20in%20Italy.pdf

SWEED: Exposing years of Agent Tesla campaigns (2019). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html

SWIFT attackers' malware linked to more financial attacks (2016). Source: Symantec. Link: https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

Sykipot (2013). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/

Syrian Activists Targeted with BlackShades Spy Software (2012). Source: Citizen Lab. Link: https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/

Syrian Activists Targeted With Facebook Phishing Attack (2012). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack

Syrian Malware, The Ever-Evolving Threat (2014). Source: Kaspersky Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2014/KL_report_syrian_malware.pdf

Systematic Cyber Attacks Against Israeli And Palestinian Targets Going On For A Year (2012). Source: Norman Shark. Link: https://app.box.com/s/83uopvit3i46wmy3hxvw4g3rjhv8ax1s

T9000: Advanced Modular Backdoor Uses Complex Anti Analysis Techniques (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

TA-505 Cybercrime on System Integrator Companies (2020). Source: Marco Ramilli. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.11.12_TA-505_On_SI/TA-505%20Cybercrime%20on%20System%20Integrator%20Companies.pdf

TA2101 plays government imposter to distribute malware to German, Italian, and US organizations (2019). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us

TA410: The Group Behind LookBack Attacks Against U.S. Utilities Sector Returns with New Malware (2020). Source: Proofpoint. Link: https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

TA428 Group abusing recent conflict between Iran and USA (2020). Source: S2 Grupo. Link: https://lab52.io/blog/icefog-apt-group-abusing-recent-conflict-between-iran-and-eeuu/

TA505 At It Again: Variety is the Spice of ServHelper and FlawedAmmyy (2019). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/

TA505 evolves ServHelper, uses Predator The Thief and Team Viewer Hijacking (2019). Source: Blueliv. Link: https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/servhelper-evolution-and-new-ta505-campaigns/

TA505 intensifica ciberataques a Chile y Latinoamérica con #FlawedAmmy (2019). Source: Germán Fernández Bacian. Link: https://medium.com/@1ZRR4H/ta505-intensifica-ciberataques-a-chile-y-latinoam%C3%A9rica-con-flawedammy-9fb92c2f0552

TA505 is Expanding its Operations (2019). Source: Yoroi. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.05.29.TA505/TA505%20is%20Expanding%20its%20Operations.pdf

TA505 organization uses Excel 4.0 macro to analyze the latest attack activities of banking institutions (2019). Source: 360 SkyEye System. Link: https://ti.360.net/blog/articles/excel-4.0-macro-utilized-by-ta505-to-target-financial-institutions-recently/

TA505: A Brief History Of Their Time (2020). Source: Fox-IT. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.11.16.TA505_History/TA505_%20A%20Brief%20History%20Of%20Their%20Time%20%E2%80%93%20Fox-IT%20International%20blog.pdf

Tactical Intelligence Bulletin Sofacy Phishing (2014). Source: PWC. Link: https://app.box.com/s/th78b3w9bhr1cpdtn9gmmm9v7j2vuq47

Tactics, Techniques and Procedures Used to Target Australian Networks (2020). Source: Australian Cyber Security Centre. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5352634118267995637.pdf

Tainted Leaks: Disinformation and Phishing With a Russian Nexus (2017). Source: Citizen Lab. Link: https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/

Taiwan Heist: Lazarus Tools And Ransomware (2017). Source: BAE Systems Detica. Link: https://app.box.com/s/t3sys73oilmytcsz38e6ihnjbp4ymxyo

Taiwan Presidential Election: A Case Study on Thematic Targeting (2016). Source: PWC. Link: https://app.box.com/s/lyradpx3h7eic3dyiz33ufiia0wj7otn

Taiwan targeted with new cyberespionage back door Trojan (2016). Source: Symantec. Link: https://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

Target Attacks Against Tibetan And Hong Kong Groups Exploiting CVE-2014-4114 (2015). Source: Citizen Lab. Link: https://citizenlab.org/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114/

Targeted attack analysis of suspected "Group 123" APT gangs using unpublished vulnerabilities in HWP software (2018). Source: 360 SkyEye System. Link: https://mp.weixin.qq.com/s/X8Iz26L1k5ibdqv3lKFHKg

Targeted Attack Leverages India-China Border Dispute to Lure Victims (2020). Source: Zscaler. Link: https://www.zscaler.com/blogs/research/targeted-attack-leverages-india-china-border-dispute-lure-victims

Targeted Attack on France's TV5Monde (2015). Source: AhnLab. Link: https://app.box.com/s/ightjgw5rkaldfpfel7q9v6p3pcqhqat

Targeted Attack on Indian Defense officials using SocketPlayer Malware (2018). Source: Volon. Link: https://volon.io/2018/06/19/targeted-attack-on-indian-defense-officials-using-socketplayer-malware/

Targeted Attack on Indian Ministry of External Affairs using Crimson RAT (2018). Source: Volon. Link: https://volon.io/2018/09/07/targeted-attack-on-indian-ministry-of-external-affairs-using-crimson-rat/

Targeted attack using Taidoor Analysis report (2019). Source: Nippon Telegraph and Telephone Corporation. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.06_Taidoor_Analysis/taidoor_analysis_jp.pdf

Targeted Attacks against Banks in the Middle East (2016). Source: FireEye. Link: https://app.box.com/s/43ovij7jz7isl93tow4s3f89yhuiwu4e

Targeted Attacks Against The Energy Sector (2014). Source: Symantec. Link: https://app.box.com/s/blcobivhvh1gwqh7qjtkrdpaggz2lmlr

Targeted Attacks In The Middle East (2018). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2018/02/targeted-attacks-in-middle-east.html

Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA (2017). Source: ClearSky Cybersecurity . Link: https://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

Targeted Attacks on Indian Government and Financial Institutions Using the JsOutProx RAT (2020). Source: Zscaler. Link: https://www.zscaler.com/blogs/research/targeted-attacks-indian-government-and-financial-institutions-using-jsoutprox-rat

Targeted Attacks on South Korean Organizations (2018). Source: AhnLab. Link: http://global.ahnlab.com/global/upload/download/techreport/Tech_Report_Malicious_Hancom.pdf

Targeted Cyber Attacks: Examples And Challenges Ahead (2013). Source: Laboratory of Cryptography and System Security (CrySyS Lab). Link: https://app.box.com/s/vsy0oa0n3l2m2lx5oxpzj71zhbqkkgxq

Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites (2015). Source: Citizen Lab. Link: https://citizenlab.ca/2015/10/targeted-attacks-ngo-burma/

Targeted Surveillance Attacks in Uzbekistan: An Old Threat with New Techniques (2020). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2020/03/targeted-surveillance-attacks-in-uzbekistan-an-old-threat-with-new-techniques/

Targeted Threat Index: Characterizing And Quantifying Politically-Motivated Targeted Malware (2014). Source: USENIX. Link: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/hardy

Targeted Threats Index (2013). Source: Citizen Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2013/Targeted-Threats-Index_website.pdf

Targeting of the government of Thailand (2015). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2015/11/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/

Targeting Portugal: A new trojan ‘Lampion’ has spread using template emails from the Portuguese Government Finance & Tax (2019). Source: Pedro Tavares. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.12.26.Trojan-Lampion/Targeting%20Portugal_%20A%20new%20trojan%20'Lampion'%20has%20spread%20using%20template%20emails%20from%20the%20Portuguese%20Government%20Finance%20%26%20Tax.pdf

TDrop2 Attacks Suggest Dark Seoul Attackers Return (2015). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2015/11/tdrop2-attacks-suggest-dark-seoul-attackers-return/

Teaching an old RAT new tricks (2016). Source: SentinelOne. Link: https://www.sentinelone.com/blogs/teaching-an-old-rat-new-tricks/

Technical Analysis of Pegasus Spyware (2016). Source: Lookout. Link: https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

Technical analysis of recent attacks against Polish banks (2017). Source: Badcyber. Link: https://badcyber.com/technical-analysis-of-recent-attacks-against-polish-banks/

TeleBots are back: supply-chain attacks against Ukraine (2017). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/740pmk3f6nrhfbj9nmcvovc64oah2ibi

Ten Days of Rain (2011). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf

Terminator RAT (2013). Source: FireEye. Link: http://www.fireeye.com/blog/technical/malware-research/2013/10/evasive-tactics-terminator-rat.html

Territorial Dispute – NSA's perspective on APT landscape (2018). Source: Laboratory of Cryptography and System Security (CrySyS Lab). Link: https://www.crysys.hu/files/tedi/ukatemicrysys_territorialdispute.pdf

The 'Madi' Infostealers - A Detailed Analysis (2012). Source: Kaspersky Lab. Link: https://app.box.com/s/h2rowevapfawgbkdpcinjgbci6iy71ml

The 'Penquin' Turla (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/5gfajyyz8firhnttdo72j0iz6uo4eo6q

The 'Spy Cloud' Operation: Geumseong121 group carries out the APT attack disguising the evidence of North Korean defection (2020). Source: ESTsecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/Operation_Spy_Cloud_eng.pdf

The "Silent Night" Zloader/Zbot (2020). Source: MalwareBytes. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5348507608179279471.pdf

The "EyePyramid" attacks (2017). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/77098/the-eyepyramid-attacks/

The Anthem Hack: All Roads Lead To China (2015). Source: ThreatConnect. Link: https://app.box.com/s/7rzfjpwud8blv668j1kxa7qmhcadn6pr

The Arsenal Behind the Australian Parliament Hack (2019). Source: Yoroi. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.02.26.Australian_Parliament_Hack/The%20Arsenal%20Behind%20the%20Australian%20Parliament%20Hack.pdf

The art and science of detecting Cobalt Strike (2020). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2020/09/coverage-strikes-back-cobalt-strike-paper.html

The Black Vine Cyberespionage Group (2015). Source: Symantec. Link: https://app.box.com/s/0ahidgtzecyx94hgvxoai9kmu5r6yw49

The Blockbuster Sequel (2017). Source: Palo Alto Networks. Link: https://app.box.com/s/lmzdurawuli1a65uvx4g6e8b9jvede3f

The British government infected Belgacom with among the most advanced malware ever seen (2014). Source: The Intercept. Link: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

The CARBANAK/FIN7 Syndicate a historical overview of an evolving threat (2017). Source: RSA Security. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/the-carbanak-fin7-syndicate.pdf

The Chinese Malware Complexes: The Maudi Surveillance Operation (2013). Source: Norman Shark. Link: https://app.box.com/s/v04cs4pueqq78rh8uasr39tsh36gtqra

The Chronicles Of The Hellsing APT: The Empire Strikes Back (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/ob16ltqxv6urff6z1ore9i6t4308cxy6

The Command Structure Of The Aurora Botnet (2010). Source: Damballa/SecureAuth. Link: https://app.box.com/s/6jeekvxflthmub9v26nybp5kqw9tjopj

The CostaRicto Campaign: Cyber-Espionage Outsourced (2020). Source: Cylance. Link: https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

The Cozyduke APT (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/8vksggruwwqzg7a4y7xrsrysrje56pqn

The Curious Case of an Unknown Trojan Targeting German-Speaking Users (2016). Source: Fortinet. Link: https://blog.fortinet.com/2016/06/21/the-curious-case-of-an-unknown-trojan-targeting-german-speaking-users

The Curious Case of Notepad and Chthonic: Exposing a Malicious Infrastructure (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/08/unit42-the-curious-case-of-notepad-and-chthonic-exposing-a-malicious-infrastructure/

The Dances of White Elephant – A Cyber Attack from South Asian Subcontinent (2016). Source: Antiy Labs. Link: http://www.antiy.net/p/the-dances-of-white-elephant-a-cyber-attack-from-south-asian-subcontinent/

The Dark Overlord Cyber Investigation Report (2020). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5235887904911263740.pdf

The Darkhotel Apt A Story Of Unusual Hospitality (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/rqk4up23y49pe1zalfmstkj4zb1dxbja

The Darkhotel Apt A Story Of Unusual Hospitality v1.0 (2014). Source: Kaspersky Lab. Link: https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

The Darkhotel APT A Story of Unusual Hospitality v1.1 (2014). Source: Kaspersky Lab. Link: https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT (2019). Source: SentinelOne. Link: https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/

The Deception Project: A New Japanese-Centric Threat (2017). Source: Cylance. Link: https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html

The Desert Falcons Targeted Attacks (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/y45wyjrr4tnz2jlt93pk6giurxpg7ue7

The destruction of APT3 (2018). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2018/05/22/the-destruction-of-apt3/

The Digital Plagiarist Campaign: TelePorting the Carbanak Crew to a New Dimension (2017). Source: tr1adx. Link: https://app.box.com/s/7pr8b7cy9liv1bi88ha7frtzgrjycex3

The Discovery of Fishwrap: A New Social Media Information Operation Methodology (2019). Source: Recorded Future. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.06.11.Fishwrap_Group/The%20Discovery%20of%20Fishwrap_%20A%20New%20Social%20Media%20Information%20Operation%20Methodology.pdf

The Double Life of SectorA05 Nesting in Agora (Operation Kitty Phishing) (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/01/30/operation-kitty-phishing/

The Dropping Elephant - aggressive cyber-espionage in the Asian region (2016). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/75328/the-dropping-elephant-actor/

THE DUKES: 7 years of Russian cyberespionage (2015). Source: F-Secure. Link: https://app.box.com/s/ipsg0t3krs811gesknvxrdsqhsknbydj

The Duqu 2.0 Technical Details (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/9bejel60h3doxinwxdfyhig5nsqz05ga

The Duqu Saga Continues (2011). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/31442/the-duqu-saga-continues-enter-mr-b-jason-and-tvs-dexter-22/

The Elderwood Project (2012). Source: Symantec. Link: https://app.box.com/s/kbhzz24wt2t7kd92c2409uyqawj1jl0t

The Enigmatic “Roma225” Campaign (2018). Source: Yoroi. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.12.27.Roma225_Campaign/The%20Enigmatic%20Roma225%20Campaign.pdf

The Epic Turla Operation: Solving Some Of The Mysteries Of Snake/Uroboros (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/9rsegtgvnwe9n2lrk6ezxfv8mnpfhpk3

The EPS Awakens (2015). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html

The EPS Awakens - Part 2 (2015). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

The Evolution of APT15’s Codebase 2020 (2020). Source: Intezer. Link: https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/

The Eye Of The Tiger (Pitty Tiger) (2014). Source: Airbus Defence and Space. Link: https://app.box.com/s/54porxs30re847wc7ca1jk1hzbtvt0hv

The Eye on the Nile (2019). Source: Check Point. Link: https://research.checkpoint.com/the-eye-on-the-nile/

THE FAKE CISCO: Hunting for backdoors in Counterfeit Cisco devices (2020). Source: F-Secure. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2020-07-the-fake-cisco.pdf

The footprints of Raccoon: a story about operators of JS-sniffer FakeSecurity distributing Raccoon stealer (2020). Source: Group-IB. Link: https://www.group-ib.com/blog/fakesecurity_raccoon

The forgotten domain: Exploring a link between Magecart Group 5 and the Carbanak APT (2019). Source: MalwareBytes. Link: https://blog.malwarebytes.com/threat-analysis/2019/10/the-forgotten-domain-exploring-a-link-between-magecart-group-5-and-the-carbanak-apt/

The Four Element Sword Engagement (2016). Source: Arbor Networks. Link: https://app.box.com/s/19ghms2qz9raaquoxu2bh3paoqyx545r

The Fractured Block Campaign: CARROTBAT Used to Deliver Malware Targeting Southeast Asia (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/11/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/

The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity (2014). Source: CrowdStrike. Link: http://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

The French Underground Under a Shroud of Extreme Caution (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5429601942257010393.pdf

The Full Shamoon: How the Devastating Malware Was Inserted Into Networks (2017). Source: IBM. Link: https://app.box.com/s/jymqnbm1hyqxboljaq7rv4p3mzizqd0c

The Gamaredon Group Toolset Evolution (2017). Source: Palo Alto Networks. Link: https://app.box.com/s/9wb59m0q2nw315jshwr3launllnnqtht

The Gamaredon Group: A TTP Profile Analysis (2019). Source: Fortinet. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.08.21.Gamaredon_Group/The%20Gamaredon%20Group_%20A%20TTP%20Profile%20Analysis.pdf

The geopolitical and potential cyber influence of Russia in Africa (2019). Source: S2 Grupo. Link: https://lab52.io/blog/the-geopolitical-and-potential-cyber-influence-of-russia-in-africa/

The Ghost Dragon (2016). Source: Cylance. Link: https://app.box.com/s/xr1ykgout1c9ho5rotpop09smkawg5me

The Gorgon Group: Slithering Between Nation State and Cybercrime (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

The GozNym criminal network: How it worked (2019). Source: Europol. Link: https://www.europol.europa.eu/article-types/press-release

The Growth of SectorF01 Group's Cyber Espionage Activities (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/07/25/growth-of-sectorf01-groups-cyber-espionage-activities/

The Hacker Infrastructure and Underground Hosting. An overview of the cybercriminal market (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5249083500438488411.pdf

The Heartbeat Apt Campaign (2012). Source: Trend Micro. Link: https://app.box.com/s/4qfg9m8wrdgsdf7k3fwrz7zmg2tkfxno

The Hunt for 3ve (2018). Source: Chronicle. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/3ve_google_whiteops_whitepaper_final_nov_2018.pdf

The Icefog Apt: A Tale Of Cloak And Three Daggers (2013). Source: Kaspersky Lab. Link: https://app.box.com/s/ebjeefvfx58arny58fb9vv6up39f293w

The Inception Framework: Cloud-Hosted Apt (2014). Source: Blue Coat Systems. Link: https://app.box.com/s/vny8b4ubmxo421amxtk8tvk4b9x1vz52

The Internet is Back in Syria and So is Malware Targeting Syrian Activists (2012). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2012/12/iinternet-back-in-syria-so-is-malware

The Iranian-Saudi Conflict and Its Cyber Outlet (2015). Source: Recorded Future. Link: https://www.recordedfuture.com/iranian-saudi-cyber-conflict/

The Italian Connection: An analysis of exploit supply chains and digital quartermasters (2015). Source: Shadowserver Foundation. Link: http://blog.shadowserver.org/2015/08/10/the-italian-connection-an-analysis-of-exploit-supply-chains-and-digital-quartermasters/

The KeyBoys are back in town (2017). Source: PWC. Link: http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html

The Kimsuky Operation: A North Korean Apt? (2013). Source: Kaspersky Lab. Link: https://app.box.com/s/bel4s8xubunn5gxjvorgm7qg2v0e9kgt

The Kingdom Came to Canada How Saudi-Linked Digital Espionage Reached Canadian Soil (2018). Source: Citizen Lab. Link: https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

The Kittens Are Back in Town 2 – Charming Kitten Campaign Keeps Going on, Using New Impersonation Methods (2019). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/the-kittens-are-back-in-town-2/

The Kittens Are Back in Town 3 (2020). Source: ClearSky Cybersecurity . Link: https://www.clearskysec.com/the-kittens-are-back-in-town-3/

The Kittens are back in town: Charming Kitten Campaign against Academic Researchers (2019). Source: ClearSky Cybersecurity . Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/The-Kittens-Are-Back-in-Town-Charming-Kitten-2019.pdf

The latest APT campaign of the Venus 121 Group - 'Operation Rocket Man' (2018). Source: ESTsecurity. Link: https://blog.alyac.co.kr/1853

The Lazarus Constellation (2020). Source: lexfo. Link: https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf

THE LAZARUS' GAZE TO THE WORLD: WHAT IS BEHIND THE FIRST STONE ? (2020). Source: Telsy. Link: https://www.telsy.com/lazarus-gaze/

The Legend of Adwind: A Commodity RAT Saga in Eight Parts (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/the-legend-of-adwind-a-commodity-rat-saga-in-eight-parts/

The Little Malware That Could: Detecting And Defeating The China Chopper Web Shell (2013). Source: FireEye. Link: https://app.box.com/s/yvk5tr8poletupw82biic0ucpvynvoyj

"The Luckycat Hackers (2012). Source: Symantec. Link: https://app.box.com/s/oiblu3lk6fsqnjqv6bx4ygkv7e14tcb8 "

The Lurid Downloader (2011). Source: Trend Micro. Link: https://app.box.com/s/7s9bvquu64vafpi14t8p6w2t6hwls1zi

The Many Faces Of Gh0St Rat: Plotting The Connections Between Malware Attacks (2012). Source: Norman Shark. Link: https://app.box.com/s/aj7ebr1v0x9mf3psmxeififqijwmmacy

The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender (2016). Source: Citizen Lab. Link: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

The Miniduke Mystery: Pdf 0-Day Government Spy Assembler 0X29A Micro Backdoor (2013). Source: Kaspersky Lab. Link: https://app.box.com/s/w3b1yh6agvwmocx8ftzjg8kyds0jodmk

The Mirage Campaign (2012). Source: Dell Secureworks. Link: https://app.box.com/s/h9vlkkgq0yaat56muq6nei95nchysbay

The mistakes of the Iranian APT organization: the self-built VPN (2019). Source: 360 SkyEye System. Link: http://www.360.cn/n/11315.html

The Monju Incident (2014). Source: Context IS. Link: https://app.box.com/s/l6n25enqom0uydgxogybp82294nkf4dt

The Msnmm Campaigns: The Earliest Naikon APT Campaigns (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/nbtyzfb5j5x9d2qznmj3bzcpa2e8kezj

The Msupdater Trojan And Ongoing Targeted Attacks (2010). Source: Seculert. Link: https://app.box.com/s/gh8m5os2jewj2adleu2xqivj9qzf9ok8

The Muddy Waters of APT Attacks (2019). Source: Check Point. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.04.10.Muddy_Waters/The%20Muddy%20Waters%20of%20APT%20Attacks.pdf

The Mutter Backdoor: Operation Beebus with New Targets (2013). Source: FireEye. Link: https://app.box.com/s/zg8cx9of6h9kdol7wwvgz8lxkqlvyr2p

The mystery of Duqu Framework solved (2012). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/32354/the-mystery-of-duqu-framework-solved-7/

The Mystery of Duqu: Part Five (2011). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/31208/the-mystery-of-duqu-part-five-6/

The Mystery of Duqu: Part One (2011). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/31177/the-mystery-of-duqu-part-one-5/

The Mystery of Duqu: Part Six (The Command and Control servers) (2011). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/31863/the-mystery-of-duqu-part-six-the-command-and-control-servers-36/

The Mystery of Duqu: Part Three (2011). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/31486/the-mystery-of-duqu-part-three-9/

The Mystery of Duqu: Part Two (2011). Source: Kaspersky Lab. Link: https://securelist.com/blog/incidents/31445/the-mystery-of-duqu-part-two-23/

The Naikon APT: Tracking Down Geo-Political Intelligence Across APAC, One Nation At A Time (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/zuyuhxayshyuaypjoxfm0nu8d5tivqih

The Nettraveler (Aka Travnet) (2013). Source: Kaspersky Lab. Link: https://app.box.com/s/1qx5mkzkcvwq3eazh2ygxowfbbadofby

The New and Improved macOS Backdoor from OceanLotus (2017). Source: Palo Alto Networks. Link: https://www.secureworks.com/research/threat-group-4127-targets-google-accounts

The Nitro Attacks: Stealing Secrets From The Chemical Industry (2011). Source: Symantec. Link: https://app.box.com/s/sp5gpgu0xpf0dsfxj269ptxyyzm0ohkf

The North Korean Kimsuky APT keeps threatening South Korea evolving its TTPs (2020). Source: Yoroi. Link: https://blog.yoroi.company/research/the-north-korean-kimsuky-apt-keeps-threatening-south-korea-evolving-its-ttps/

The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

The Oldest Stuxnet Component Dials Up (2019). Source: Chronicle. Link: https://storage.googleapis.com/chronicle-research/STUXSHOP%20Stuxnet%20Dials%20In%20.pdf

The Plugx Malware Revisited: Introducing Smoaler (2013). Source: SophosLabs. Link: https://app.box.com/s/dfdg420iygjtz1rmou2ps14zi25l7tfb

The Predator in your Pocket (2019). Source: Citizen Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/stalkerware-holistic.pdf

The ProjectSauron APT (2016). Source: Kaspersky Lab. Link: https://app.box.com/s/3n10k8gbwt7pfebhqjg8n2mwpo6m3u7j

The Red October Campaign - An Advanced Cyber Espionage Network (2013). Source: Kaspersky Lab. Link: https://app.box.com/s/ymcjx37fp0zyyjybcl80czcrpzctjfp9

The Regin Platform Nation-State Ownership Of Gsm Networks (2014). Source: Kaspersky Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2014/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

The Return of The Charming Kitten (2018). Source: Certfa. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.12.13.Charming_Kitten_Return/The%20Return%20of%20The%20Charming%20Kitten.pdf

The rise of TeleBots: Analyzing disruptive KillDisk attacks (2016). Source: ESET WeLiveSecurity. Link: http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

The Rocketman APT campaign, 'Operation Golden Bird' (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2205

The Rotten Tomato Campaign (2014). Source: SophosLabs. Link: https://app.box.com/s/ngqr8jevmhlypff49eju70nhxzfy26bh

The shadow knows: Malvertising campaigns use domain shadowing to pull in Angler EK (2015). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/The-Shadow-Knows

The Shadows of Ghosts Inside the Response of a Unique CARBANAK Intrusion (2017). Source: RSA Security. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/the-shadows-of-ghosts-carbanak-report.pdf

The Shadows of Ghosts: Inside the Response of a Unique Carbanak Intrusion (2017). Source: RSA Security. Link: https://community.rsa.com/community/products/netwitness/blog/2017/12/04/anatomy-of-an-attack-carbanak

The Siesta Campaign: A New Cybercrime Operation Awakens (2014). Source: Trend Micro. Link: https://app.box.com/s/0rcadhypkl7fod418nv58uicnnljvnrh

The Sin Digoo Affair (2012). Source: Dell Secureworks. Link: https://app.box.com/s/qj9849r6n72ktrc9q3n9107xduauffss

The Slingshot APT (2018). Source: Kaspersky Lab. Link: https://s3-eu-west-1.amazonaws.com/khub-media/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf

The SmartPhone Who Loved Me: FinFisher Goes Mobile? (2012). Source: Citizen Lab. Link: https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/

The Spy Kittens Are Back: Rocket Kitten 2 | PDF (2015). Source: ClearSky Cybersecurity . Link: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf

The SpyRATs of OceanLotus (2018). Source: Cylance. Link: https://threatvector.cylance.com/en_us/home/report-the-spyrats-of-oceanlotus.html

The State of the ESILE/Lotus Blossom Campaign (2016). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/the-state-of-the-esilelotus-blossom-campaign/

The Stealthy Email Stealer in the TA505 Arsenal (2019). Source: Yoroi. Link: https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/

The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability (2010). Source: US Senate. Link: http://www.fas.org/sgp/crs/natsec/R41524.pdf

The Syrian Malware House of Cards (2014). Source: Kaspersky Lab. Link: https://securelist.com/blog/research/66051/the-syrian-malware-house-of-cards/

The Teamspy Story - Abusing Teamviewer In Cyberespionage Campaigns (2013). Source: Kaspersky Lab. Link: https://app.box.com/s/742gtrl1fedxy8iqwjuqsiru1m8i0l2g

The TopHat Campaign: Attacks Within The Middle East Region Using Popular Third-Party Services (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/01/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/

The Turbo Campaign, Featuring Derusbi for 64-bit Linux (2016). Source: Fidelis Cybersecurity. Link: https://www.fidelissecurity.com/sites/default/files/TA_Fidelis_Turbo_1602_0.pdf

The Untold Story of NotPetya, the Most Devastating Cyberattack in History (Sandworm) (2018). Source: Wired. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2018/The_Untold_Story_of_NotPetya_the_Most_Devastating_Cyberattack_in_History_082018.pdf

The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Attack in History (Sandworm) (2019). Source: Wired. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/The_Untold_Story_of_the_2018_Olympics_Cyberattack_the_Most_Deceptive_Hack_in_History_102019.pdf

The Uroburos Case: New Sophisticated Rat Identified (2014). Source: G Data Software. Link: https://app.box.com/s/sg4cyodukt7edmmba6bfikuiu1jgzv59

The Urpage Connection to Bahamut, Confucius and Patchwork (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/

The Voho Campaign: An In Depth Analysis (2012). Source: RSA Security. Link: https://app.box.com/s/g1nx7q1o451m0o8hmhbeg82igcflk6q5

The Waterbug Attack Group (2016). Source: Symantec. Link: https://app.box.com/s/nrf432kfdk6kadkvbclgykekocn4pzzu

The zero-day exploits of Operation WizardOpium (2020). Source: Kaspersky Lab. Link: https://securelist.com/the-zero-day-exploits-of-operation-wizardopium/97086/

TheIntercept's report on The Regin Platform (2014). Source: The Intercept. Link: https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

Thieves and Geeks: Russian and Chinese Hacking Communities (2019). Source: Recorded Future. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/2_5308045752075814093.pdf

Threat Actor Group using UAC Bypass Module to run BAT File (2019). Source: Threat Recon Team. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.03.28.UAC_Bypass_BAT_APT/Threat%20Actor%20Group%20using%20UAC%20Bypass%20Module%20to%20run%20BAT%20File.pdf

Threat Actor Profile: KovCoreG, The Kovter Saga (2017). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-kovcoreg-kovter-saga

Threat Actor Profile: TA407, the Silent Librarian (2019). Source: Proofpoint. Link: https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian

Threat Actor Targeting Hong Kong Pro-Democracy Figures (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/12/03/threat-actor-targeting-hong-kong-activists/

Threat Actors Target Government of Belarus Using CMSTAR Trojan (2017). Source: Palo Alto Networks. Link: https://app.box.com/s/d8vup5qyc8poenl8e760pzau9mt0kdih

Threat Analysis: Poison Ivy and Links to an Extended PlugX Campaign (2015). Source: CYINT Analysis. Link: http://www.cyintanalysis.com/threat-analysis-poison-ivy-and-links-to-an-extended-plugx-campaign/

Threat Group APT28 Slips Office Malware into Doc Citing NYC Terror Attack (2017). Source: Intel Security-McAfee. Link: https://securingtomorrow.mcafee.com/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/#sf151634298

Threat Group Cards: A Threat Actor Encyclopedia (2019). Source: Open Source. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/Threat_Group_Cards.pdf

Threat Group-3390 Targets Organizations For Cyberespionage (2015). Source: Dell Secureworks. Link: https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Threat Group-4127 Targets Google Accounts (2016). Source: Dell Secureworks. Link: https://app.box.com/s/2y2p7im0bp3o5myvi5s9cxfchddn2zbd

Threat Group-4127 Targets Hillary Clinton Presidential Campaign (2016). Source: Dell Secureworks. Link: https://app.box.com/s/jfku9mhjnf150uokw2owfxy0isj3pi28

Threat landscape for industrial automation systems (2020). Source: Kaspersky Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/KASPERSKY_H22019_ICS_REPORT_FINAL_EN.pdf

Threat Spotlight: Follow the Bad Rabbit (2017). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2017/10/bad-rabbit.html

Threat Spotlight: Group 72 (2014). Source: Cisco Talos. Link: https://app.box.com/s/mtk3zeae1823kz2hv3f7z6pgjgwxlkyl

Threat Spotlight: Group 72, Opening The Zxshell (2014). Source: Cisco Talos. Link: https://app.box.com/s/89uahki8m2ksfgc8pysjw6utcqjp4q9u

Threat Spotlight: MenuPass/QuasarRAT Backdoor (2019). Source: Cylance. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.06.10.MenuPass_QuasarRAT_Backdoor/Threat%20Spotlight_%20MenuPass_QuasarRAT%20Backdoor.pdf

Threat Spotlight: Ratsnif - New Network Vermin from OceanLotus (2019). Source: Cylance. Link: https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html

ThreatConnect identifies Chinese targeting of two companies. Economic espionage or military intelligence? (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/

ThreatConnect Identifies DCLeaks As Another Russian-backed Influence Outlet (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/

Threats in the Netherlands (2018). Source: Kaspersky Lab. Link: https://securelist.com/threats-in-the-netherlands/88185/

Thrip: Ambitious Attacks Against High Level Targets Continue (2019). Source: Symantec. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.09.09.Thrip/Thrip_%20Ambitious%20Attacks%20Against%20High%20Level%20Targets%20Continue.pdf

Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies (2018). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Tibetan Groups Targeted with 1-Click Mobile Exploits (2019). Source: Citizen Lab. Link: https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/

Tibetan Uprising Day Malware Attacks (2015). Source: Citizen Lab. Link: https://app.box.com/s/43vz10qmcubl6d3cCVEzh2ahb9rbmyyj

Tick Group Weaponized Secure USB Drives to Target Air-Gapped Critical Systems (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/06/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/?utm_source=marketo&utm_medium=email&utm_campaign=unit42&mkt_tok=eyJpIjoiTkRrMlpHWXlPV1ptTlRrMiIsInQiOiJqVDQwNUhjUEdRekdwY2YxSUQ5XC9EdUVKSEdKNUhYUDNsMXM0YkZkK3BOVmNPV

Tick Tock - Activities of the Tick Cyber Espionage Group in East Asia Over the Last 10 Years (2019). Source: Open Source. Link: https://gsec.hitb.org/materials/sg2019/D1%20COMMSEC%20-%20Tick%20Group%20-%20Activities%20Of%20The%20Tick%20Cyber%20Espionage%20Group%20In%20East%20Asia%20Over%20The%20Last%2010%20Years%20-%20Cha%20Minseok.pdf

Tildeb: Analyzing the 18-year-old Implant from the Shadow Brokers' Leak (2018). Source: Trend Micro. Link: https://documents.trendmicro.com/assets/tech-brief-tildeb-analyzing-the-18-year-old-implant-from-the-shadow-brokers-leak.pdf

Time of death? A therapeutic postmortem of connected medicine (2018). Source: Kaspersky Lab. Link: https://securelist.com/time-of-death-connected-medicine/84315/

Tinbapore: Millions of Dollars at Risk (2016). Source: F5 Networks. Link: https://devcentral.f5.com/d/tinbapore-millions-of-dollars-at-risk?download=true

Titanium: the Platinum group strikes again (2019). Source: Kaspersky Lab. Link: https://securelist.com/titanium-the-platinum-group-strikes-again/94961/

Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks (2019). Source: Symantec. Link: https://app.box.com/s/ovf9il8mblb3szopr9q6gw2en6k61e4p

Tr-25 Analysis - Turla / PNet / Snake/ Uroburos (2014). Source: Computer Incident Response Center Luxembourg (CIRCL). Link: https://app.box.com/s/54kvbxp9nc0xtme1omd1xpxcckwm945g

Tracking Elirks Variants in Japan: Similarities to Previous Attacks (2016). Source: Palo Alto Networks. Link: https://app.box.com/s/ki60vxvdi2wzqrsrqik0yvg4sdwsbbal

Tracking Ghostnet: Investigating A Cyber Espionage Network (2009). Source: Information Warfare Monitor (IWM). Link: https://app.box.com/s/8dq0gur02w8oh0z7ljjz5mh8l11cmrhh

Tracking MiniDionis: CozyCar's New Ride Is Related to Seaduke (2015). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2015/07/tracking-minidionis-cozycars-new-ride-is-related-to-seaduke/

Tracking OceanLotus' new Downloader, KerrDown (2019). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/

Tracking Subaat: Targeted Phishing Attack Leads to Threat Actor's Repository (2017). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/

Tracking Tick Through Recent Campaigns Targeting East Asia (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/10/tracking-tick-through-recent-campaigns.html

Tracking Turla: New backdoor delivered via Armenian watering holes (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes

Transparent Tribe: Evolution analysis, part 1 (2020). Source: Kaspersky Lab. Link: https://securelist.com/transparent-tribe-part-1/98127/

Transparent Tribe: Evolution analysis, part 2 (2020). Source: Kaspersky Lab. Link: https://securelist.com/transparent-tribe-part-2/98233/

Trends in Android Ransomware (2017). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/ESET_Trends_2017_in_Android_Ransomware.pdf

Triout – Spyware Framework for Android with Extensive Surveillance Capabilities (2018). Source: BitDefender. Link: https://labs.bitdefender.com/2018/08/triout-spyware-framework-for-android-with-extensive-surveillance-capabilities/

TRISIS Malware Analysis of Safety System Targeted Malware (2017). Source: Dragos. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/TRISIS-01.pdf

TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping (2019). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html

"TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers

(2018). Source: FireEye. Link: https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html"

TRITON: The First ICS Cyber Attack on Safety Instrument Systems (2018). Source: Nozomi. Link: https://www.nozominetworks.com/downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf

Trochilus and New MoonWind RATs Used In Attack Against Thai Organizations (2017). Source: Palo Alto Networks. Link: https://www.threatminer.org/_reports/2017/Trochilus and New MoonWind RATs Used In Attack Against Thai Organizations - Palo Alto Networks.pdf

Trojan Hidden in Fake Revolutionary Documents Targets Syrian Activists (2012). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2012/05/trojan-hidden-fake-revolutionary-documents-targets-syrian-activists

Trojan.Apt.Banechant: In-Memory Trojan That Observes For Multiple Mouse Clicks (2013). Source: FireEye. Link: https://app.box.com/s/5ycaruh0zf07h2jy9mpasgm1crninjwp

Trojan.Apt.Seinup Hitting Asean (2013). Source: FireEye. Link: https://app.box.com/s/iap35ypb6u03wrzpmemy2z2ntf4k8wm0

Trojan.Taidoor: Targeting Think Tanks (2012). Source: Symantec. Link: https://app.box.com/s/td8bl14go6icl9lhi9c4idkk82e83t2c

Trojanized Adobe Installer Used To Install DragonOK's New Custom Backdoor (2017). Source: Forcepoint. Link: https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor

Tropic Trooper Targets Taiwanese Government and Fossil Fuel Provider With Poison Ivy (2016). Source: Palo Alto Networks. Link: http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Tropic Trooper's Back: USBferry Attack Targets Air-gapped Environments (2020). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments/

Tropic Trooper's New Strategy (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/

Turbo Twist: Two 64-bit Derusbi Strains Converge (2016). Source: Fidelis Cybersecurity. Link: https://app.box.com/s/ex6wh2qsg1c29sob6f70x1q6eoe3v64w

TURLA / VENOMOUS BEAR UPDATES ITS ARSENAL: "NEWPASS" APPEARS ON THE APT THREAT SCENE (2020). Source: Tesly. Link: https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/

Turla Crutch: Keeping the "back door" open (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

Turla group exploits Iranian APT to expand coverage of victims (2019). Source: National Cyber Security Centre. Link: https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims

Turla group update Neuron malware (2018). Source: National Cyber Security Centre. Link: https://www.ncsc.gov.uk/content/files/protected_files/article_files/Turla%20Neuron%20Malware%20Update.pdf

Turla group using Neuron and Nautilus tools alongside Snake malware (2017). Source: National Cyber Security Centre. Link: https://github.com/fdiskyou/threat-

INTel/raw/master/2017/Turla_group_using_Neuron_and_Nautilus_tools_alongside_Snake_malware_1.pdf

Turla LightNeuron: An email too far (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/05/07/turla-lightneuron-email-too-far/

Turla Mosquito: A shift towards more generic tools (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/

Turla Outlook Backdoor (2018). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

Turla renews its arsenal with Topinambour (2019). Source: Kaspersky Lab. Link: https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/

Twas the night before (2019). Source: Kaspersky Lab. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.07.04.NewsBeef_APT/Twas%20the%20night%20before.pdf

Twitterbots: Anatomy of a Propaganda Campaign (2019). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation

Two Birds, One STONE PANDA (2018). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

Two Bytes to $951M (2016). Source: BAE Systems Detica. Link: https://app.box.com/s/49t6zpzjln2vvm2npdnzwtr0hkrxq37v

Two Tailed Scorpion (2017). Source: 360 SkyEye System. Link: http://zhuiri.360.cn/report/index.php/2017/03/09/twotailedscorpion/

Two Years of Pawn Storm Examining an Increasingly Relevant Threat (2017). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2017/wp-two-years-of-pawn-storm.pdf

Two-tailed scorpion APT-C-23 (2020). Source: SecPulse. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.12_Two-tailed_scorpion/Two-tailed_scorpion_CN_version.pdf

UAE used cyber super-weapon to spy on iPhones of foes (2019). Source: Reuters. Link: https://www.reuters.com/article/us-usa-spying-karma-exclusive/exclusive-uae-used-cyber-super-weapon-to-spy-on-iphones-of-foes-idUSKCN1PO1AN

Ukraine election 2019 polls Maldoc: analysis (2019). Source: S2 Grupo. Link: https://lab52.io/blog/ukraine-election-2019-polls-maldoc-analysis/

ULTRARANK The unexpected twist of a JS-sniffer triple threat (2020). Source: Group-IB. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5361980413780691010.pdf

Uncovering New Activity By APT10 (2019). Source: Ensilo. Link: https://blog.ensilo.com/uncovering-new-activity-by-apt10

Uncovering the Seven Pointed Dagger (2016). Source: Arbor Networks. Link: https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn

Underlying Dimensions of Yemen's Civil War: Control of the Internet (2018). Source: Recorded Future. Link: https://www.recordedfuture.com/yemen-internet-activity/

Unfin4Ished Business (2015). Source: PWC. Link: https://app.box.com/s/7ep6vyqosrj2b26t6udv30jjdevkpv6f

Unknown Threat Actor is Using a Compromised Website Belonging to a Government Institution of Middle-East in a Campaign Referring Commercial and Financ (2019). Source: Telsy. Link: https://blog.telsy.com/telsy-detected-a-malware/

Unknown Threat Actor Is Using Agent Tesla Variants Against Oil & Gas and Energy Sector (2019). Source: Telsy. Link: https://blog.telsy.com/agent-tesla-variants/

Unraveling the Lamberts Toolkit (2017). Source: Kaspersky Lab. Link: https://securelist.com/unraveling-the-lamberts-toolkit/77990/

Untangling Legion Loader's Hornet Nest of Malware (2019). Source: Deep Instinct. Link: https://www.deepinstinct.com/2019/12/18/untangling-legion-loaders-hornet-nest-of-malware/

Untangling the Patchwork Cyberespionage Group (2017). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/untangling-the-patchwork-cyberespionage-group/

Unveiling Careto - The Masked Apt (2014). Source: Kaspersky Lab. Link: https://app.box.com/s/aepgdq5vc2dxd2m9t0ab2v28rtwbhjua

Unveiling Patchwork the Copy Paste APT (2016). Source: Cymmetria. Link: https://www.cymmetria.com/wp-content/uploads/2016/07/Unveiling-Patchwork.pdf

Update on Pawn Storm: New Targets and Politically Motivated Campaigns (2018). Source: Trend Micro. Link: http://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns/?utm_campaign=shareaholic&utm_medium=twitter&utm_source=socialnetwork

Update: Hands in the MuddyWater – Playing with Iranian Cyber-Espionage Campaign (2018). Source: Emanuele De Lucia. Link: https://www.emanueledelucia.net/update-hands-in-the-muddywater-playing-with-iranian-cyber-espionage-campaign/

Updated BackConfig Malware Targeting Government and Military Organizations in South Asia (2020). Source: Palo Alto Networks. Link: https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/

Updated Karagany Malware Targets Energy Sector (2019). Source: Dell Secureworks. Link: https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

UPSynergy: Chinese-American Spy vs. Spy Story (2019). Source: Check Point. Link: https://research.checkpoint.com/upsynergy/

URI Terror Attack & Kashmir Protest Themed Spear Phishing Emails Targeting Indian Embassies And Indian Ministry Of External Affairs (2017). Source: Cysinfo. Link: https://app.box.com/s/aw4frbwy7jj5iqlhn9mas4qmc8ogfljg

Uroburos Highly Complex Espionage Software With Russian Roots (2014). Source: G Data Software. Link: https://app.box.com/s/dokswmrkrxmipfmdpsvelnq18w4ypogw

URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader (2018). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.12.18.ursnif-emotet-dridex-and-bitpaymer-gangs/URSNIF%2C%20EMOTET%2C%20DRIDEX%20and%20BitPaymer%20Gangs%20Linked%20by%20a%20Similar%20Loader.pdf

Use of Fancy Bear Android Malware tracking of Ukrainian Artillery Units (2016). Source: CrowdStrike. Link: https://app.box.com/s/8lj785rl608lsmf80bwvtuxb7b9mscxy

Use-after-free (UAF) Vulnerability CVE-2018-8373 in VBScript Engine Affects Internet Explorer to Run Shellcode (2018). Source: Trend Micro. Link: https://blog.trendmicro.com/trendlabs-security-intelligence/use-after-free-uaf-vulnerability-cve-2018-8373-in-vbscript-engine-affects-internet-explorer-to-run-shellcode/

Varenyky: Spambot à la Française (2019). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2019/08/08/varenyky-spambot-campaigns-france/

Vawtrak v2 (2016). Source: SophosLabs. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/sophos-vawtrak-v2-sahin-wyke.pdf

Vendetta-new threat actor from Europe (2020). Source: 360 SkyEye System. Link: https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/

"Venus 121 APT organization performs steganography technique and smartphone norin fusion attack

(2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2452"

Venus 121, North Korean defector sponsor 'Dragon Messenger' mobile APT attack (2019). Source: ESTsecurity. Link: https://blog.alyac.co.kr/2588

VERMIN: Quasar RAT and Custom Malware Used In Ukraine (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/

ViceLeaker Operation: mobile espionage targeting Middle East (2019). Source: Kaspersky Lab. Link: https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

Vicious Panda: The COVID Campaign (2020). Source: Intel Security-McAfee. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.12_Vicious_Panda/Vicious%20Panda_%20The%20COVID%20Campaign%20-%20Check%20Point%20Research.pdf

Vietnamese Malware Gets Very Personal (2014). Source: Electronic Frontier Foundation. Link: https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal

Vinself Now With Steganography (2014). Source: Airbus Defence and Space. Link: https://app.box.com/s/uy1tzn58yjoarnrftgs9d8ieucwf4029

ViperRAT: The mobile APT targeting the Israeli Defense Force that should be on your radar (2017). Source: Lookout. Link: https://app.box.com/s/n2ruyugtbigi6yyvg6u2xmt32eyqn8gx

Visa Alert and Update on the Oracle Breach (2016). Source: Krebs on Security. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/BrianKrebs_Carbanak-Oracle-breach.pdf

Visiting The Bear Den A Journey in the Land of (Cyber-)Espionage (2016). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/ifsplrz92ssuo3mhgwadkgoc19e5y56e

Visiting The Bear Den A Journey in the Land of Cyber-Espionage (2016). Source: ESET WeLiveSecurity. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2016/ESET-Visiting_The_Bear_Den.pdf

Volatile Cedar Threat Intelligence And Research (2015). Source: Check Point. Link: https://app.box.com/s/jgl1n5xvzu3kp7aoi3cd9r407kjfzjcc

VPNFilter botnet: a SophosLabs analysis (2018). Source: SophosLabs. Link: https://news.sophos.com/en-us/2018/05/24/vpnfilter-botnet-a-sophoslabs-analysis/

VPNFilter botnet: a SophosLabs analysis, part 2 (2018). Source: SophosLabs. Link: https://news.sophos.com/en-us/2018/05/27/vpnfilter-botnet-a-sophoslabs-analysis-part-2/

VPNFilter EXIF to C2 mechanism analysed (2018). Source: Kaspersky Lab. Link: https://securelist.com/vpnfilter-exif-to-c2-mechanism-analysed/85721/

VPNFilter Update - VPNFilter exploits endpoints, targets new devices (2018). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

VPNFilter-affected Devices Still Riddled with 19 Vulnerabilities (2018). Source: Trend Micro. Link: http://newsroom.trendmicro.com/blog/security-intelligence/vpnfilter-affected-devices-still-riddled-19-vulnerabilities

Vulnerability, Malicious Code Appeared In The Mbr Destruction Function Using Hangul File (2014). Source: AhnLab. Link: https://app.box.com/s/q8gx5wedudaui491qn6i4d7dxsnmuyla

W32.Duqu - The precursor to the next Stuxnet (2011). Source: Symantec. Link: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

W32.Stuxnet Dossier (2011). Source: Symantec. Link: https://app.box.com/s/rpdy3pk00bmkhgmf1lsfuwt6edakh6k3

W32/Regin, Stage #1 (2014). Source: F-Secure. Link: https://app.box.com/s/358saagkwt3gqy6w62ed6xo33w175r0y

W64/Regin, Stage #1 (2014). Source: F-Secure. Link: https://app.box.com/s/2ifpyh8kjoxsvrj9dnqfxfrb2go1pu3a

WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group (2020). Source: NCCGroup. Link: https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

WastedLocker: Symantec Identifies Wave of Attacks Against U.S. Organizations (2020). Source: Symantec. Link: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

Waterbear is Back, Uses API Hooking to Evade Security Product Detection (2019). Source: Trend Micro. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.12.11.Waterbear_Back/Waterbear%20is%20Back%2C%20Uses%20API%20Hooking%20to%20Evade%20Security%20Product%20Detection.pdf

Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments (2019). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments?wpisrc=nl_cybersecurity202&wpmm=1

Watering Hole Attack On Aerospace Firm Exploits CVE-2015-5122 To Install Isspace Backdoor (2015). Source: Palo Alto Networks. Link: https://app.box.com/s/8izjpumhif40wt5jzbe6yej6j1sewt0b

Wave your false flags! Deception tactics muddying attribution in targeted attacks (2016). Source: Kaspersky Lab. Link: https://app.box.com/s/6smqqgagrck8ltwztwnw08x1ope6k0mi

Weaponizing a Lazarus Group Implant (2020). Source: Objective-See. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.02.22_Lazarus_Group_Weaponizing/Weaponizing%20a%20Lazarus%20Group%20Implant.pdf

Webmail Server APT: A New Persistent Attack Methodology Targeting Microsoft Outlook Web Application (OWA) (2015). Source: Cybereason. Link: http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Labs-Analysis-Webmail-Sever-APT.pdf

Welcome Chat as a secure messaging app? Nothing could be further from the truth (2020). Source: ESET WeLiveSecurity. Link: https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

West African Financial Institutions Hit by Wave of Attacks (2019). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/african-financial-attacks

Whack-A-Mole: The Impact of Threat Intelligence on Adversaries (2018). Source: Cylance. Link: https://threatvector.cylance.com/en_us/home/whack-a-mole-the-impact-of-threat-intelligence-on-adversaries.html

What is the Hainan Xiandun Technology Development Company? (2020). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2020/01/09/what-is-the-hainan-xiandun-technology-development-company/

What the continued escalation of tensions in the Middle East means for security (2020). Source: Cisco Talos. Link: https://blog.talosintelligence.com/2020/01/mideast-tensions-preparations.html

What we know about the South Korea NIS's use of Hacking Team's RCS (2015). Source: Citizen Lab. Link: https://citizenlab.ca/2015/08/what-we-know-about-the-south-korea-niss-use-of-hacking-teams-rcs/

What's in a Name... Server? (2016). Source: ThreatConnect. Link: https://www.threatconnect.com/blog/whats-in-a-name-server/

When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users (2018). Source: Amnesty International. Link: https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/

When Governments Hack Opponents: A Look at Actors and Technology (2014). Source: USENIX. Link: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/marczak

When The Lights Went Out: Ukraine Cybersecurity Threat Briefing (2016). Source: Booz Allen Hamilton. Link: https://app.box.com/s/pbj4aeiapdbblzs19gzymgsk73sxbe56

Where There Is Smoke, There Is Fire: South Asian Cyber Espionage Heats Up (2013). Source: ThreatConnect. Link: https://app.box.com/s/s0c49bv6hitrhmcafk0phnnuer3e63v1

Whitefly: Espionage Group has Singapore in Its Sights (2019). Source: Symantec. Link: https://www.symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore

Who else works for this cover company network? (2020). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2020/01/13/who-else-works-for-this-cover-company-network/

Who is behind this Chinese espionage group stealing our intellectual property? (2017). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2017/04/26/who-is-behind-this-chinese-espionage-group-stealing-our-intellectual-property/

Who is GOSSIPGIRL? (2019). Source: Chronicle. Link: https://medium.com/chronicle-blog/who-is-gossipgirl-3b4170f846c0

Who is Mr An, and was he working for APT10? (2018). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2018/08/31/who-is-mr-an-and-was-he-working-for-apt10/

Who is Mr Dong? (2017). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2017/05/05/who-is-mr-dong/

Who is Mr Gao? (2018). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2018/08/02/who-is-mr-gao/

Who is Mr Guo? (2019). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2019/07/17/who-is-mr-guo/

Who is Mr Wang? (2019). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2019/07/19/who-is-mr-wang/

Who is Mr Wu? (2017). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2017/05/02/who-is-mr-wu/

Who is Mr Zeng? (2019). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2019/07/22/who-is-mr-zeng/

Who is Mr Zhang? (2018). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2018/08/06/who-is-mr-zhang/

Who was behind this unprecedented Cyber attack on Western infrastructure? (2018). Source: IntrusionTruth. Link: https://intrusiontruth.wordpress.com/2018/07/17/who-was-behind-this-unprecedented-cyber-attack-on-western-infrastructure/

Who Wasn’t Responsible for Olympic Destroyer? (2018). Source: Cisco Talos. Link: http://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html

WHO'S HACKING THE HACKERS: NO HONOR AMONG THIEVES (2020). Source: Cybereason. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.10.WHO_HACKING_THE_HACKERS/2020_03_Threat_Alert_Hacking_the_Hackers.pdf

Who's who in the Zoo Cyberespionage operation targets Android users in the Middle East (2019). Source: Kaspersky Lab. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2019/ZooPark_for_public_final_edited.pdf

Wicked Rose And The Ncph Hacking Group (2012). Source: iDefense Verisign. Link: https://app.box.com/s/0cp8nyd339dnbak96x2klgz1kxm36xd2

Widespread DNS Hijacking Activity Targets Multiple Sectors (2019). Source: CrowdStrike. Link: https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

Wild Neutron _ Economic Espionage Threat Actor Returns With New Tricks (2015). Source: Kaspersky Lab. Link: https://app.box.com/s/anoc1ews8p5jil4pewlafksf3d4oym5x

WildPressure targets industrial-related entities in the Middle East (2019). Source: Kaspersky Lab. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2020/2020.03.24_WildPressure/WildPressure%20targets%20industrial-related%20entities%20in%20the%20Middle%20East%20_%20Securelist.pdf

WIN32/INDUSTROYER A new threat for industrial control systems (2017). Source: ESET WeLiveSecurity. Link: https://app.box.com/s/ec8zyav7snvm6vsfhy8ocvvngphe8lqp

Windows Defender ATP device risk score exposes new cyberattack, drives Conditional access to protect networks (2018). Source: Microsoft. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2018/2018.11.28.Tropic_Trooper_microsoft/Tropic_Trooper_microsoft.pdf

Windows zero-day exploit used in targeted attacks by FruityArmor APT (2016). Source: Kaspersky Lab. Link: https://securelist.com/windows-zero-day-exploit-used-in-targeted-attacks-by-fruityarmor-apt/76396/

Winnti Abuses GitHub for C&C Communications (2017). Source: Trend Micro. Link: https://www.threatminer.org/_reports/2017/Winnti Abuses GitHub for C&C Communications - Trend Micro.pdf

WINNTI Analysis (2015). Source: Novetta. Link: https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf

Winnti Evolution - Going Open Source (2017). Source: ProtectWise. Link: https://www.protectwise.com/blog/winnti-evolution-going-open-source.html

Winnti Group: Geostrategic and TTP (Tactics, Techniques and Procedures) (2019). Source: S2 Grupo. Link: https://lab52.io/blog/winnti-group-geostrategic-analysis-and-ttp/

WINNTI GROUP: Insights From the Past (2020). Source: Quointelligence. Link: https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/

Winnti Group’s skip-2.0: A Microsoft SQL Server backdoor (2019). Source: ESET WeLiveSecurity. Link: https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2019/2019.10.21.Winnti_skip_2.0/Winnti%20Group%E2%80%99s%20skip%E2%80%912.0_%20A%C2%A0Microsoft%20SQL%20Server%20backdoor.pdf

Winnti: More Than Just A Game (2013). Source: Kaspersky Lab. Link: https://app.box.com/s/dlzp6f7hv9q3r0kreqvu8yyt36lzdbxw

Winnti: More than just Windows and Gates (2019). Source: Chronicle. Link: https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a

Wiper Malware: A Detection Deep Dive (2014). Source: Cisco Talos. Link: https://app.box.com/s/efz1qmraxgqzenl5mzyeqtrh8kg1nktb

WIRTE Group attacking the Middle East (2019). Source: S2 Grupo. Link: https://lab52.io/blog/wirte-group-attacking-the-middle-east/

WitchCoven: Exploiting Web Analytics to Ensnare Victims (2015). Source: FireEye. Link: https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf

WOOL3NH4T – ROCKET KITTEN -RAW VIDEOS (2019). Source: Treadstone 71. Link: https://cybershafarat.com/2019/04/30/woolenhat/

World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks (2013). Source: FireEye. Link: https://app.box.com/s/dbgzho741wbtce2r5hppvocy6cwjbcbk

Worm War: The Botnet Battle for IoT Territory (2020). Source: Trend Micro. Link: https://github.com/fdiskyou/threat-INTel/raw/master/2020/2_5249083500438488420.pdf

Xbash Combines Botnet, Ransomware, Coinmining in Worm that Targets Linux and Windows (2018). Source: Palo Alto Networks. Link: https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

Xtremerat: Nuisance Or Threat? (2014). Source: FireEye. Link: https://app.box.com/s/s7kamaz3bmziz8vu1fvwz2e9m13xiysg

You Only Click Twice: Finfisher's Global Proliferation (2013). Source: Citizen Lab. Link: https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

YTY Framework in New Targeted Campaign Against Pakistan Government (2019). Source: Threat Recon Team. Link: https://threatrecon.nshc.net/2019/08/02/sectore02-updates-yty-framework-in-new-targeted-campaign-against-pakistan-government/

Zebrocy’s Multilanguage Malware Salad (2019). Source: Kaspersky Lab. Link: https://securelist.com/zebrocys-multilanguage-malware-salad/90680/

Zero-day exploit (CVE-2018-8453) used in targeted attacks (2018). Source: Kaspersky Lab. Link: https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/

"Zero-day in Windows Kernel Transaction Manager (CVE-2018-8611) (2018). Source: Kaspersky Lab. Link: https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/"

Zoxpng Analysis (2014). Source: Novetta. Link:
https://app.box.com/s/8wxap100crzcd96a05ajsj9vodpjauau