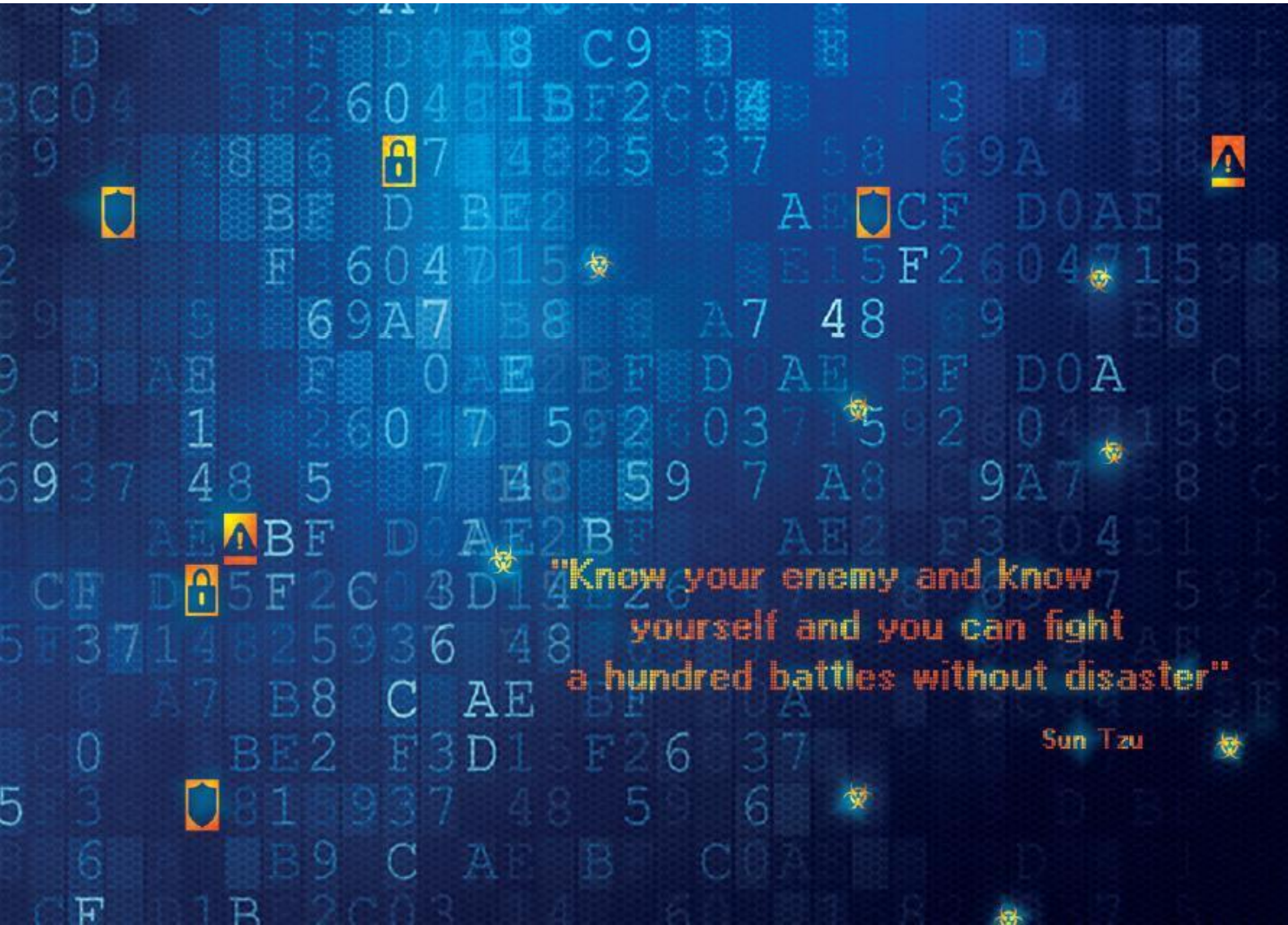
THALES

Press kit

The CyberThreat Handbook
by Thales & Verint

Who's who in CyberThreat?



1. About Thales

Thales (Euronext Paris: HO) is a **global technology leader** shaping the world of tomorrow today. The Group provides solutions, services and products to customers in the aeronautics, space, transport, digital identity and security, and defence markets. With **80,000 employees in 68 countries**, Thales generated sales of €19 billion in 2018 (on a pro forma basis including Gemalto).

Thales is investing in particular in digital innovations — **connectivity, Big Data, artificial intelligence and cybersecurity** — technologies that support businesses, organisations and governments in their decisive moments.

In a world that is increasingly mobile, interconnected and interdependent, customers come to Thales with big ambitions to help them make life better and keep us safer thanks to digital technologies.

To be sure the new technologies can be trusted, Thales **secures the digital transformation of the most critical information systems and protects every stage of the data lifecycle, from capture to completion.**

Our specialists in critical information systems and cybersecurity design and deliver a unique range of extraordinary high-technology solutions to meet the requirements of the most demanding customers — governments, institutions, large and critical infrastructure providers. To support their digital transformation, more than 50 countries and hundreds of enterprise customers **place their trust in Thales for their critical business processes and data security**.

2. Thales' Cyberthreat Intelligence Capability

« Know your enemy and know yourself and you can be fight a hundred battles » according Sun Tzu's, whose quote is on the cover of the report. No one can effectively fight your enemy without knowing him, his motivations, his financial and technical means, his attacks techniques, etc. But in the field of cyber threats, knowing one's enemy can be extremely complex:

- By nature, many cyber attackers have a **clear desire to conceal** themselves;
- Cyberattacks are extremely **diverse**, some targeting sectors, geographical areas or organizations more or less precisely, with very different motivations and a variable "performance" depending on the attacker groups.

- *What cyberthreat intelligence is about*

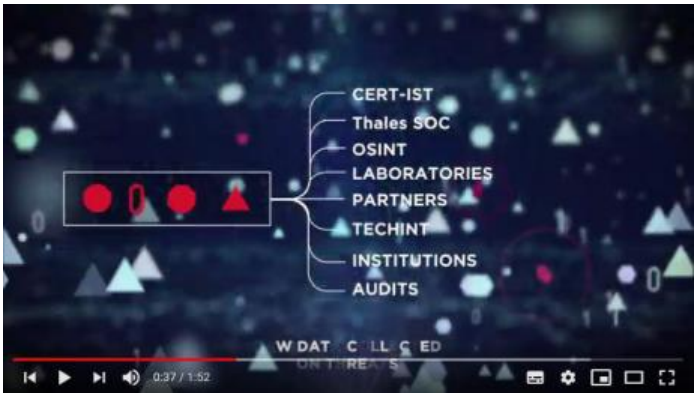
Thales' cyber threat intelligence service collects, analyzes, then sorts and correlates data related to each type of cyberattack, the attacker and its operating mode.

Thales' ambition is to **understand cyber threats in order to better detect them**: the purpose of this threat analysis is to interconnect with cyberattack detection tools (such as the detection probe and the SOC) and analyze threats in order to constantly adapt the relevance of detection rules.

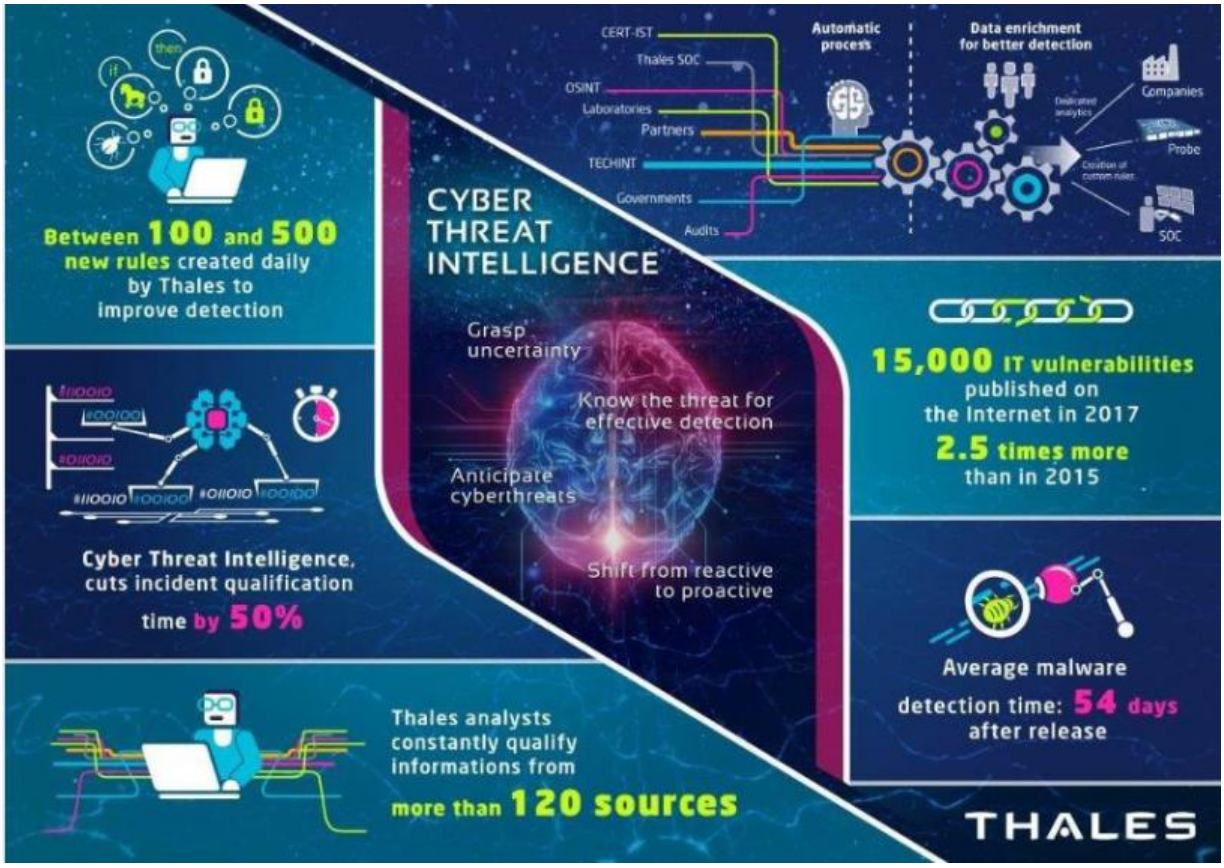
This service is based on data that is collected using a **large number of resources**, whether human, public, private, technical or not. This multi-source approach is also based on **international cooperation** (with companies such as Verint or ESET), which makes it possible to expand the number of sources and provide a global response to international cyber threats.

To that effect analysts continuously work on **data gathering, analysis and retrieval**. They also analyse malware in order to develop reports on the behaviour of hackers and to **provide feedback of information to clients under attack**. The service possesses a database that lists the attacks the methods and techniques that they use to inflitrate a system. Therefore the centre concentrates on the following questions: who attacks who ? when and with which technique ? What are their motivations?

By sharing their analyses of cyber criminals' behaviors and operating methods, Thales teams improve their knowledge of cyber threats, which helps strengthen detection abilities, anticipate new risks and better collectively combat cyberattacks.



Discover how CyberThreat Intelligence works on the following video: https://www.youtube.com/watch?v=iTmCgHIyy8M&list=PLypm7oU4utZVyK3tWuEhEYLjBfQ5Fck9w&index=30



- ***A day in the life of a CTI analyst***

The service is divided into three bureaus: the Technical Analysis Bureau, the Strategic Context Bureau, and the Bureau of automatization and Delivery. The Technical analysis bureau conducts investigations on cyberattack campaigns that involve Thales and its partners, by examining events reported by Thales entities and by the cybersecurity Operation Center teams. The role of the Strategic Context Bureau is to render information on an attack to make it comprehensible to the entity under attack, by establishing links between the attacks and the events which may have triggered them (eg. Financial, legal, social events). And lastly, the Automatisation and Delivery Bureau collects Big Data which will subsequently places at the client's disposal.

You are willing to learn more about CTI? Meet our experts, Quentin, Nicolas and Romain, explaining how the Thales CTI capability operates on a daily basis.

> ***Episode 1***: Quentin talking about the Technical Analysis Bureau

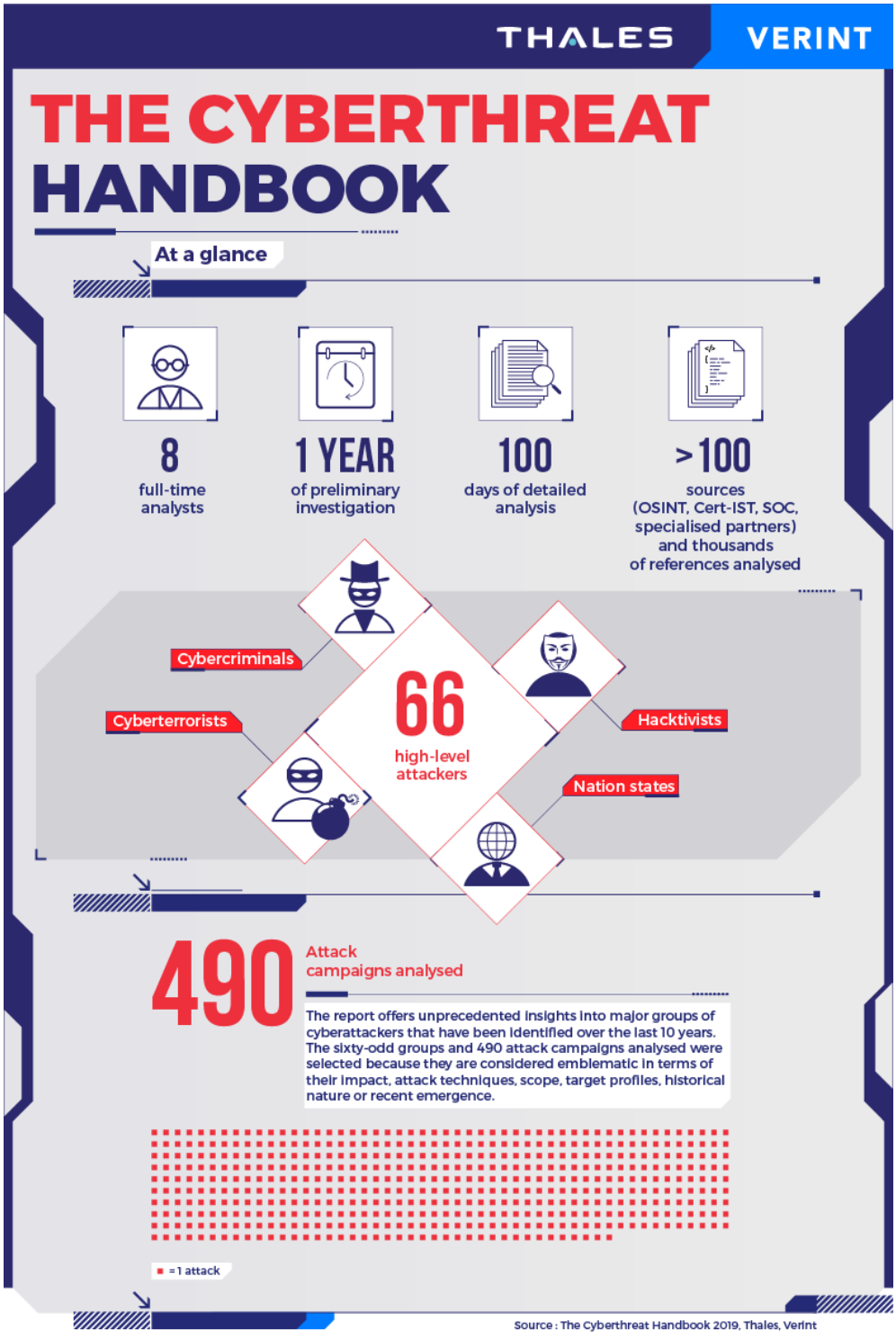
> ***Episode 2***: Nicolas talking about the Strategic Context Bureau

> ***Episode 3***: Romain talking about the Bureau of automatization and Delivery

3. The Thales and Verint Cyberthreat Handbook

- *The first report of its kind in the world*

This report is the first of its kind in the world in terms of the quality of its content. It is the result of thousands of hours of information gathering, cross-checking and analysis by our teams of experts, who have conducted an in-depth investigation of attackers' motivations and techniques over a significant period of time.



- *Key findings : four major categories of cyberattackers*

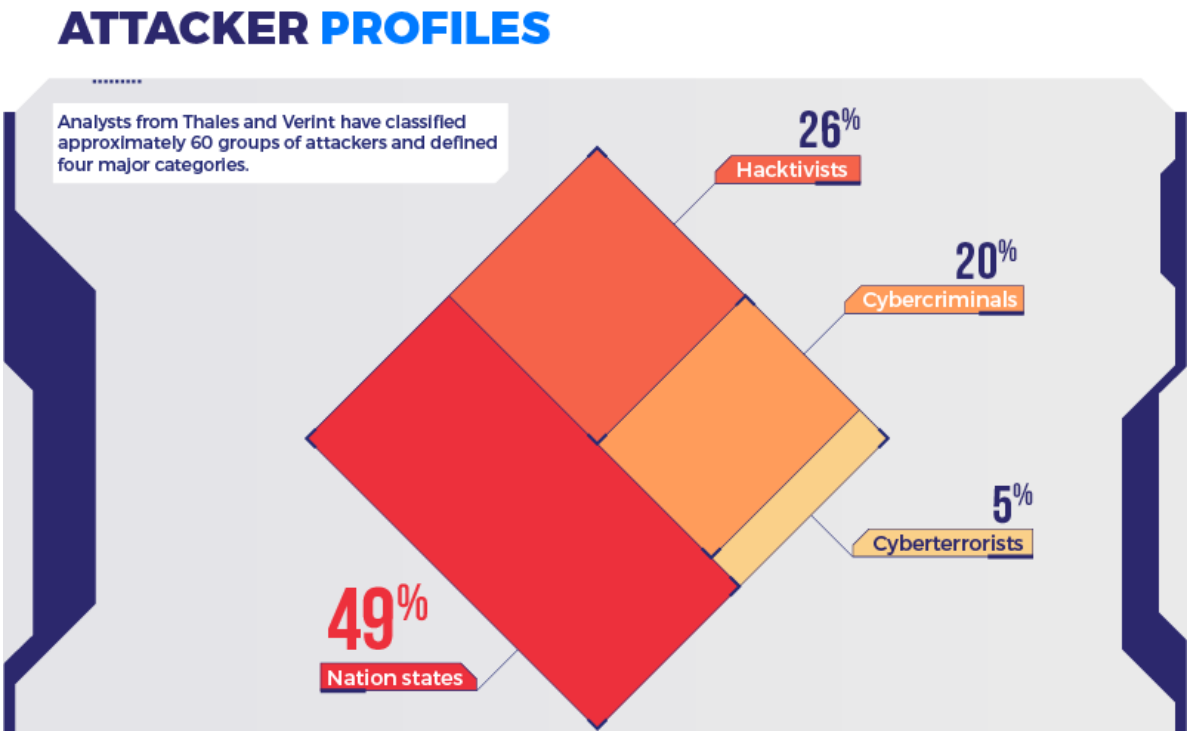
Analysts from Thales and Verint have defined four major categories of attackers based on their motives and ultimate objectives. Out of approximately sixty major groups of attackers analysed:

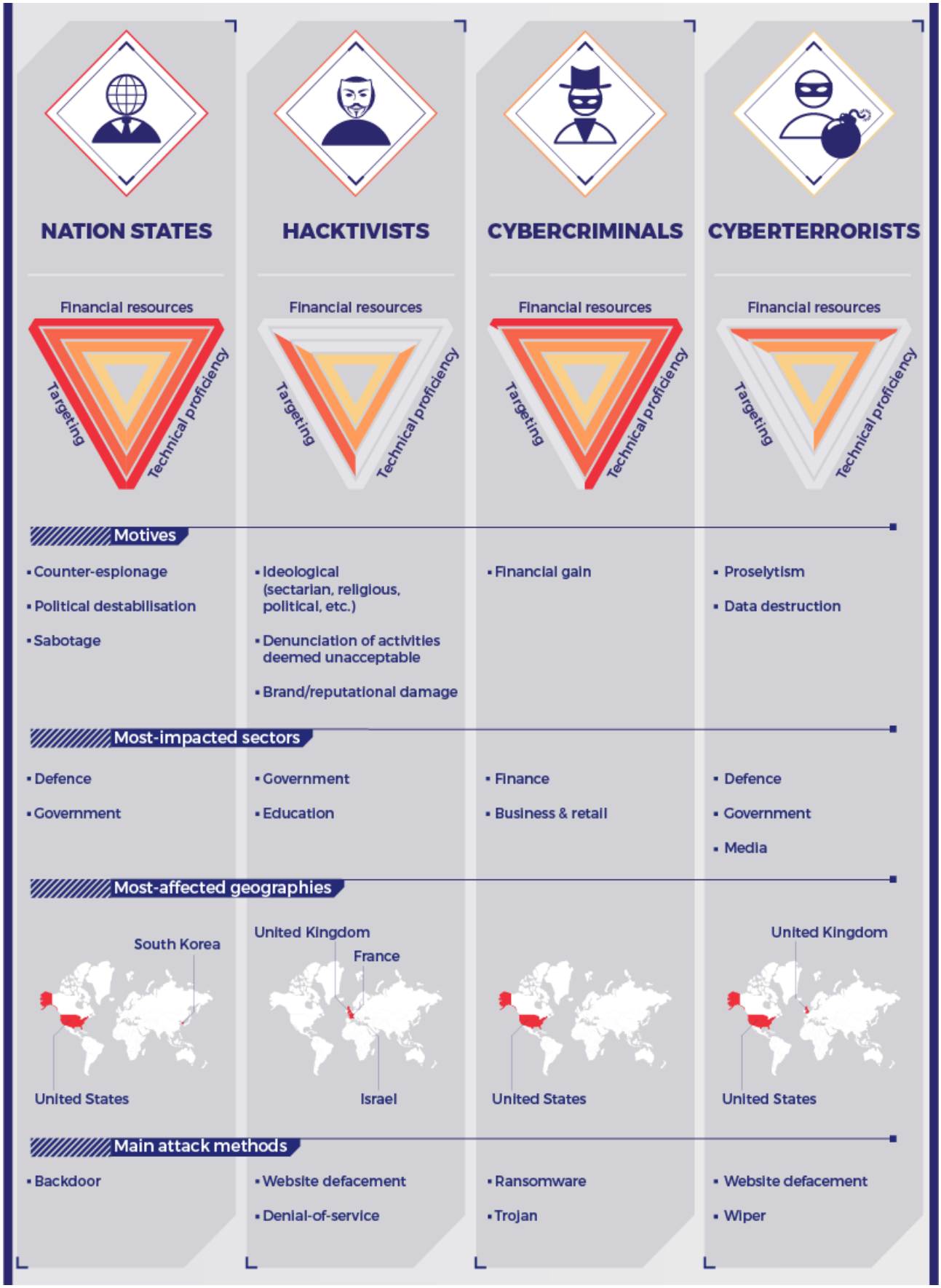
- 49% are state-sponsored groups often aiming to steal sensitive data from targets of geopolitical interest. This category accounts for a high proportion of the total, largely as a result of the substantial financial and human resources available to these groups of attackers, which help to make their activities particularly effective.

- Hacktivists (26%) are ideologically motivated and are generally aiming to denounce the activities of organisations they deem unacceptable by damaging their brands or public image.

- This category is closely followed by cybercriminals (20%) who are driven by financial gain and mainly target businesses and the financial sector.

- Cyberterrorists account for 5% of the groups analysed. They generally either conduct propaganda campaigns to recruit new sympathisers, or attempt to destroy their victims' data.



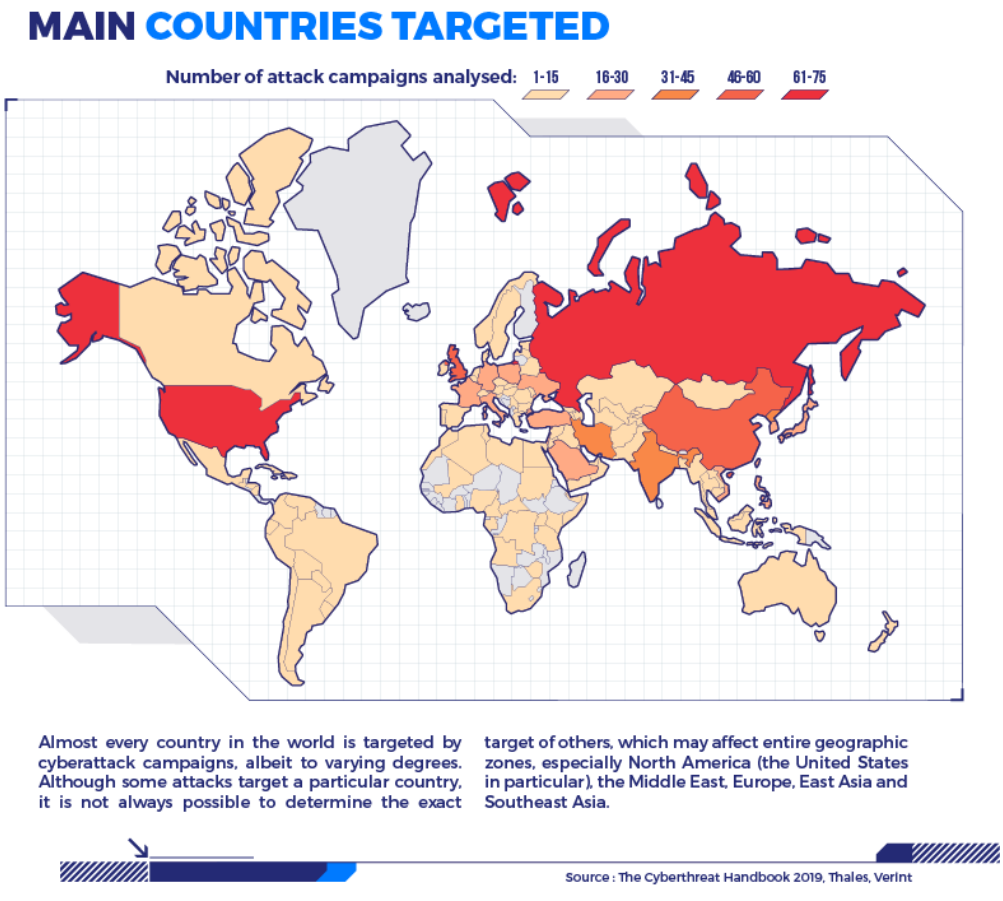

NATION STATES
HACKTIVISTS
CYBERCRIMINALS
CYBERTERRORISTS
Financial resources
Targeting
Technical proficiency
Motives
Counter-espionage
Political destabilisation
Sabotage
Ideological (sectarian, religious, political, etc.)
Denunciation of activities deemed unacceptable
Brand/reputational damage
Financial gain
Proselytism
Data destruction
Most-impacted sectors
Defence
Government
Government
Education
Finance
Business & retail
Defence
Government
Media
Most-affected geographies
South Korea
United States
United Kingdom
France
Israel
United States
United Kingdom
United States
Main attack methods
Backdoor
Website defacement
Denial-of-service
Ransomware
Trojan
Website defacement
Wiper

- *Most-targeted countries and geographies*

Cyberthreats are global and almost every country in the world is targeted, albeit to varying degrees, as the map below illustrate. Although some attacks target a particular country, it is not always possible to determine the exact target of others, which may affect entire geographic zones.

Two major observations:

- All the world's major economic, political and military powers are priority targets of cyberattackers. The 12 countries in the world with the highest GDP are all at the top of the list of targets, headed by the United States, Russia, the European Union (particularly the United Kingdom, France and Germany) and China, followed by India, South Korea and Japan. At the other end of the scale, African countries have been relatively unaffected by major cyberattacks.
- The list of most-targeted countries is also a reflection of regional geopolitical or economic tensions, in particular in four specific geographical zones:
    - North Korea and South Korea
    - Eastern Europe (Ukraine, Poland) and Turkey
    - Southeast Asia
    - Near and Middle East, including Iran, Israel and Saudi Arabia



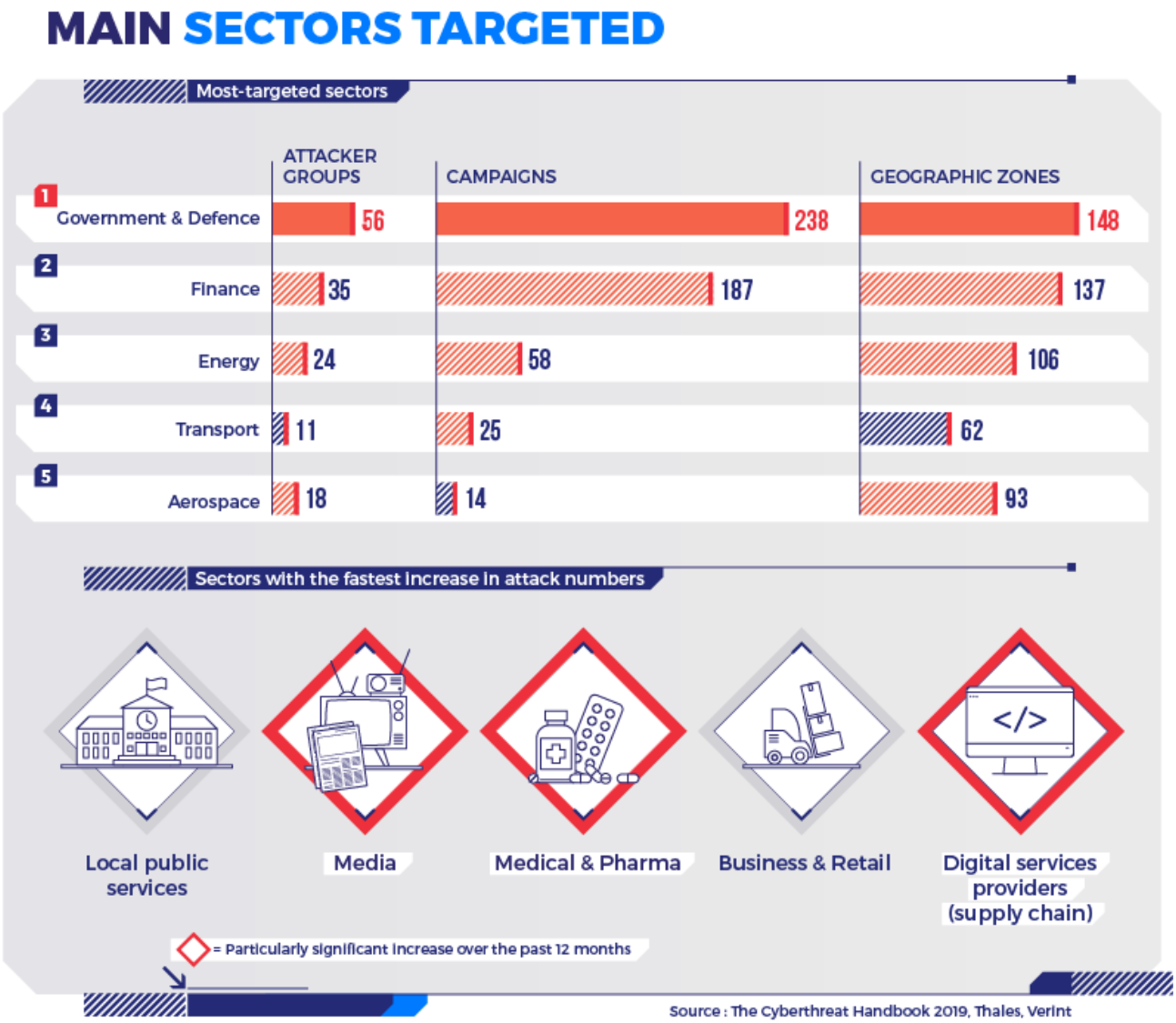
- *Most-targeted sectors*

Unsurprisingly, the adversaries with the greatest technical, financial and human resources tend to target nation states, their defence capabilities and other major players in the state sector. These

attackers, who are usually state-sponsored themselves, carry out targeted attacks on a specific country or one of its sovereign industries.

Financial services are the second-largest sector affected by cyberattackers. Motivated by financial gain, they conduct worldwide offensives targeting all the players in the global financial system: 137 different geographic zones have been targeted by groups of attackers focusing in this sector.

The energy sector has also been targeted in numerous attacks, with 24 groups of attackers affecting 106 countries; and the spectrum of attack techniques is also very broad, with more than 230 families of malware identified in attacks targeting this sector alone.



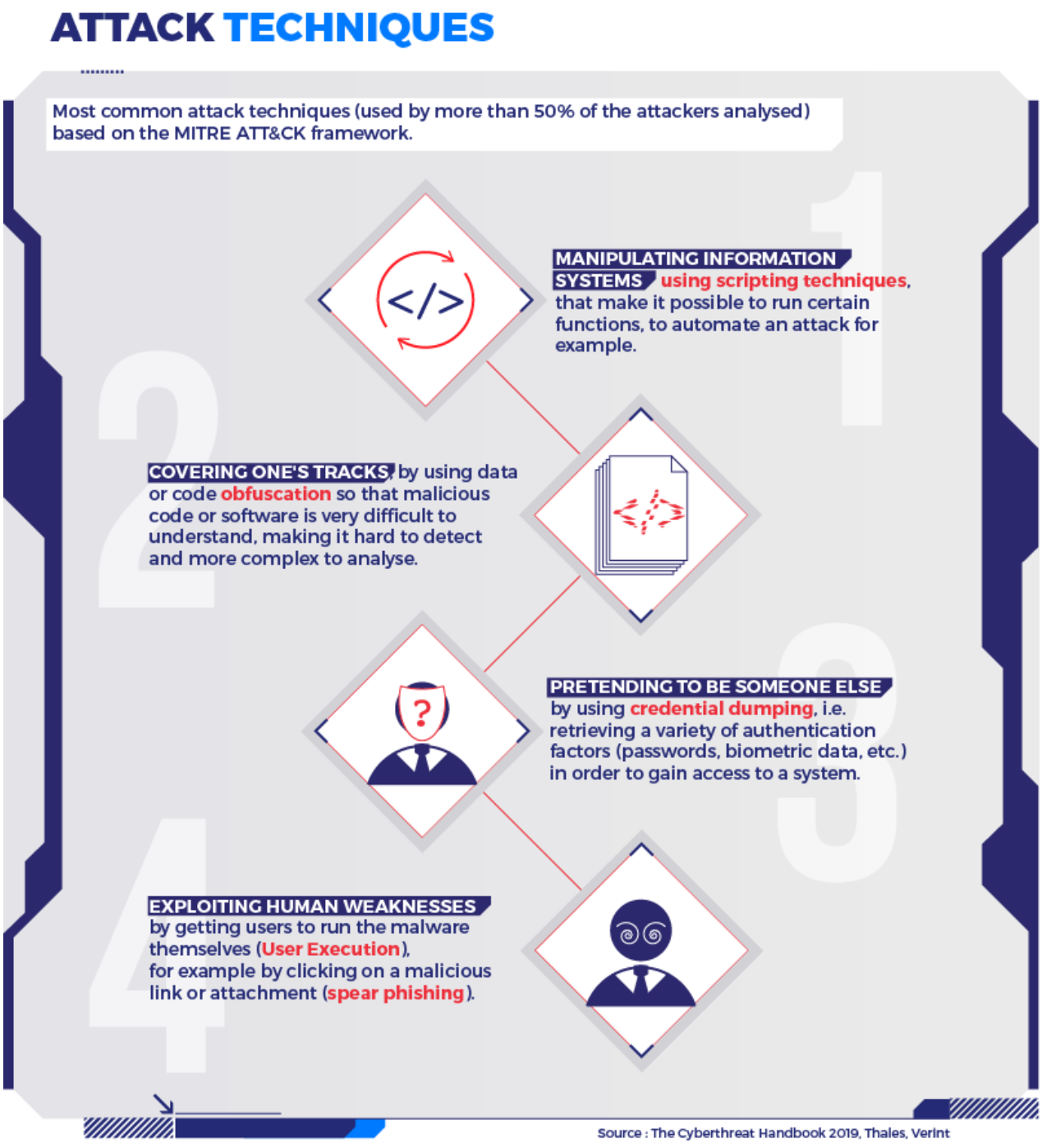
- ***Attack techniques, tactics and procedures***

Despite concerted efforts to raise user awareness, phishing is still a widely used attack technique, particularly sophisticated forms such as spear-phishing, which uses emails targeted at specific individuals. The perpetrators of many of these highly personalised attacks, which are made via email, have collected information about the target beforehand in order to extract as much personal information as possible and ensure that the email is not identified as spam.

Code or data obfuscation is another widespread attack technique, the purpose being to make malicious code or software as difficult as possible to understand. Credential dumping is also a popular technique whereby an attacker retrieves a variety of authentication factors (passwords, biometric data, etc.) in order to gain access to a system.

Another observation reported in The Cyberthreat Handbook is that malware programs are evolving, with two major trends:

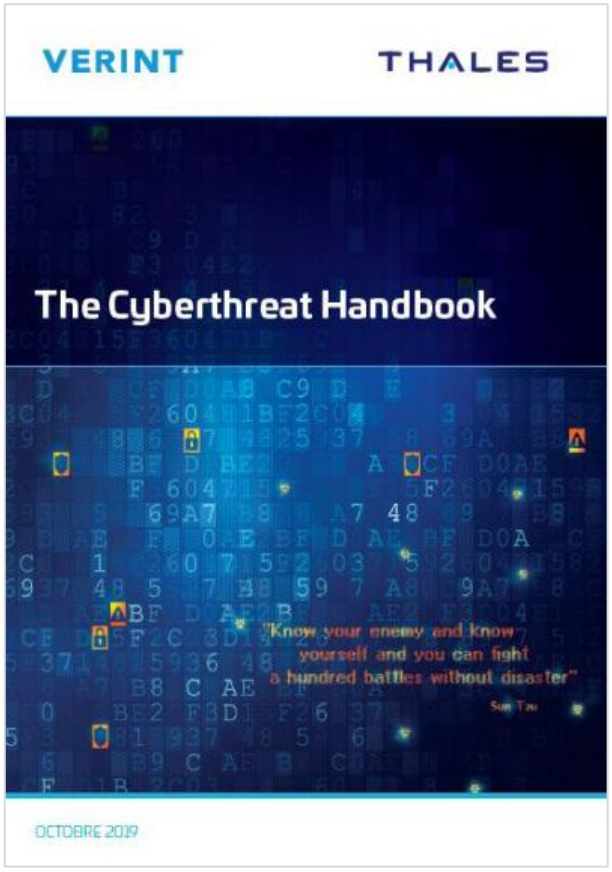
- Attackers tend to use specific types of malware, such as malicious software targeting connected devices, or ransomware that encrypts the victim's data until a ransom is paid.
- "Malware as a service": there is evidence that attackers increasingly buy malware developed by other groups of attackers, who make it a specialty. This practice saves the attackers a lot of time, as they do not need to develop the malware themselves; it also makes the analysts' task more complex in that groups of attackers can no longer necessarily be characterised by the malware they use.



- *Supply chain attacks: a particular focus in the future*

The main common denominator among all groups of attackers is their ingenuity and determination to constantly evolve and find ways to circumvent the cyberprotection measures in place within businesses, organisations and administrations. A growing number of groups of attackers are now focusing on vulnerabilities in the supply chain, and in particular on smaller partners, suppliers and service providers without the human and financial resources required to make substantial investments in cybersecurity. These are then used as trojans and have increasingly become a target for attackers seeing them as a way to access larger organisations.

- *Executive summary and methodology*



Produced by Thales and Verint, the Cyberthreat Handbook is an original proposal for an environmental analysis of the cyberthreat landscape. This is a dynamic directory which, in its first version, aims to provide a synthetic and rigorous analysis of 66 groups of attackers of global importance today. This work in no way claims to be perfectly exhaustive. The aim is to provide an introduction to cyberthreats from open sources that Thales and Verint consider reliable.

In the form of dedicated ratings cards, the report sets out to familiarise the reader with groups of different profiles. There are cyber-attackers sponsored by Nation States, high-flying cyber-criminal groups, hacktivist groups and cyber-terrorists. This panorama shows that the threat is extremely diversified, both technically, with varied modus operandis, and in terms of performance, some of them demonstrating an extremely high level of technical sophistication such as the ATK91 group (Xenotime, Triton, TEMP.Veles) capable of infiltrating and manipulating critical infrastructure and industrial control and security systems (ICS) with its Triton malware.

Several criteria have been used to define what we call the importance of these threats. Some groups will be considered relevant because of their recent nature and performance. In this respect, ATK120 (Lyceum/Hexane), discovered at the end of August 2019, makes a sensational entry into the cyberthreat landscape and has been integrated into this work in this regard. Others have not been active for several years, but their status as Advanced Persistent Threats (APT), characteristic of state-sponsored groups and their past campaigns, leads us to consider them as still part of the same landscape. Nor can the ATK2 group (APT17), for example, whose campaigns seem to have weakened in intensity since 2014, be ignored since during its last campaign it managed to compromise the websites of the GIFAS, the French aerospace industry association, and the systems of some of its members. More generally, groups are chosen because of their nuisance and/or destruction capacities, their difficulty in detection, their agility and their own or higher interest motivations. It would clearly be illusory to hope to map all known attacker groups, first because they are extremely numerous, and also because attack modes are sometimes strongly replicated from one group to another. For example, the IceFog backdoor of the Chinese group of the same name has been widely distributed and used

by other groups of Chinese origin. Effective as this program may be, the simple fact of using it is not enough to justify the inclusion of all the groups that might be in a position to use it. By its very nature, the cyber threat landscape also a highly complex matter to study, with many cyber attackers operating in the shadows, with a clear desire to conceal themselves.

The attacker groups profiled in this report all have one thing in common: they are all significant attackers, in terms of the number of campaigns conducted, the technical competence they demonstrate, the agility of their operating methods and the strength of their motivations. In a word, they are all determined opponents, capable of carrying out significant attacks. Their level of "performance" is variable, as indicated by the scoring system we have established for the purposes of this report. For each of these attackers, we provide a brief description. We detail their names in the various known sources, their nature (state-sponsored, criminal, hacktivist or terrorist), their known targets in terms of sectors of activity and geographical areas, the language they use and their assumed origin, motivations and objectives. We also contextualise the activity of some groups in light of international events that may have occurred during their attack campaigns. These same campaigns are also detailed and illustrated in a timeline for each of the ratings cards in order to trace known activity. Each card also explains the malware used, whether specific to the attacker group or used by others, the legitimate tools used and the vulnerabilities exploited. Finally, we dissect the attacker's usual modus operandi by explaining its Tactics, Techniques and Procedures (TTP) according to the matrix developed by MITRE ATT&CK®. By the same token, the objective is to be able to formally identify a group at the time of an attack by a detailed knowledge of its habits.

The Cyberthreat Handbook thus brings together analyses of nearly 490 attack campaigns conducted in some 40 activity sectors in 39 countries by 66 attackers of various kinds (49% state-sponsored, 26% hacktivist, 20% cybercriminals and 5% terrorists). Most often, state-sponsored groups focus on stealing sensitive data from geopolitical targets of interest and/or critical infrastructure providers, generally using backdoor techniques. Hacktivists pursue ideological motivations (community, religious, political, etc.), denouncing facts deemed unacceptable by conducting DDoS attacks, proselytising or spreading disinformation through defacement. What we call cybercriminals are groups seeking substantial financial gains, for example through the use of ransomware. Finally, cyber-terrorists either have a proselytising approach, in order to find new adepts, or seek to destroy data, with the use of wipers for example, or infrastructures, with defacement and the use of publicly available pentest tools.

Analysis of this broad range of attackers makes it possible to reconstitute the idiosyncrasies of certain types of groups. The most virulent and well-trained attacker groups do not necessarily develop their own malware, for instance. Most use malware developed by others, who make it a specialty. Some design digital weapons, others use them as part of a well-structured offensive strategy. Groups of Chinese origin, for example, have thus developed a habit of sharing their most successful malware with other groups. The other growing trend is the purchase of botnet malware on the Dark Web from the highest bidder to distribute much more developed malware in a second phase.

Idiosyncrasy is also sometimes a matter of geography. Not all attacker groups use the same attack techniques according to their geographical origin. For example, very few Chinese cyber-criminal groups use ransomware, preferring crypto-mining for the vast majority of their attacks. Middle Eastern cyber pirates favour the fraudulent use of social networks, encrypted messaging (WhatsApp, Telegram, etc.) or develop malware dedicated to mobile applications (especially running on Android). The North Korean groups — each of which specialises in monitoring a specific subject (espionage of the defence sector in the US and Europe / espionage of South Korea / financial crime) — are now pooling their attack infrastructures. This strategy makes it very complex to attribute certain attacks to a particular group and leads most observers to amalgamate them under the generic name of Lazarus. These "geographical" specificities can be explained, as in the case of North Korea or China, by the fact that these attacker groups communicate with each other and share attack techniques, often because they are sponsored by the same state entities. They

are also sometimes based on technical limitations (for example, the relative unavailability of the Play Store in the Middle East), which directs attackers towards certain modus operandis rather than others. However, this geographical characterisation of attackers through the tools used is not systematic. Russian attackers, whose motivations are varied, use the full cyber arsenal at their disposal, for example.

This broad analysis also makes it possible to identify trends in technical behaviour. In the context of supply chain attacks, for example, as the global defences of organisations are strengthened, attackers are forced to put in place more elaborate tactics to circumvent them. These attacks therefore remain very effective and there is a large increase in indirect attacks, passing through the suppliers of the various organisations. These are then used as trojans. They may be the company's usual service providers to target computer components integrated into the company's systems (mobile applications, code lines, software suppliers, etc.) or connected objects such as surveillance cameras. Another emerging trend is the increasingly widespread use of certificate malware signatures, whereby hackers sign their malware with stolen legitimate certificates so as not to arouse the suspicions of many antivirus programs.

We also note that some techniques remain widely used because they are tremendously effective. Most often their success is based on the exploitation of human carelessness and error. Spear-phishing, although as old as cyber itself, thus continues to be effective and widely used.

The main sectors of activity targeted also tell us a lot about the typical profiles that emerge from the analysis. More than half of the groups target government institutions, often defence organisations, followed by the financial, transport, energy and aerospace sectors. It is not surprising that the most competent and motivated opponents are primarily targeting states, their defence capabilities and all the major players in this sector. These attackers, most of whom are themselves state-sponsored, carry out targeted attacks on geopolitical rivals or their strategic operators. Finance is the second sector most affected by attacking groups. Essentially cyber-criminals, these profiles are driven by a quest for significant financial gain. Their offensives are therefore global and target all players in the global financial system. To our knowledge, 137 different geographical areas have been targeted by attacker groups in this sector. The same applies to attacks against major energy players, most often multinationals, with 24 attackers affecting 106 countries,. The energy sector has also been the subject of very diversified attacks, with our analysts identifying more than 230 different malware families in use cases. This is probably due to the increasing number of compromises on proto-IoT or SCADA systems, on which attacks are also developing in the transport sector.

In general, this "top 5" tells us that systems in critical sectors are clearly the most targeted, and that "cyber Pearl Harbor" scenarios involving future smart cities and their key infrastructures, for example, are highly likely. In addition, there are also increasing attacks on the health sector for the theft of targeted personal data or information on highly sensitive and valuable pharmaceutical products. In the era of informational crisis, the media sector is also increasingly being targeted. Most often they are watering hole attacks consisting in imitating an official website to disseminate false information or more sophisticated Strategic Web Compromise (SWC) attacks consisting in compromising an official website for the same reasons.

The Cyberthreat Handbook also proposes to offer a new and accurate vision of the cyberthreat landscape by establishing a scoring by attacker based on the MITRE ATT&CK matrix. The purpose is to illustrate the level of threat represented by each. This is the second main purpose of this report: to provide a quantified estimate of the level of threat posed by attackers. By knowing their usual tactics, we can establish whether the potential for nuisance and/ or destruction is more or less important with regard to their techniques (whether these techniques are more or less easy to implement, whether they allow the attacker to control all of part of a system, whether attackers focus on a limited range of techniques or an elaborate arsenal, and whether they can change techniques regularly and demonstrate a high degree of agility). All these indications are objective parameters that allow us to build an indicative score for each attacker.

The MITRE ATT&CK matrix defines 12 tactics that can be used by an attacker to carry out its campaigns. Each of these 12 tactics encompasses 9 to 68 techniques identified by the MITRE matrix. It is on this model that the Thales/Verint scoring of attackers has been built. For some attackers, the score is not indicated because their techniques are not known. Thus, if an attacker's score is presented as low or even zero, it doesn't necessarily reflects its true technical level. The latter can be important but unknown, which reinforces the threat generated. The score is extracted from the following formula:

$$Score_{complexity} = \frac{Number\ of\ malware\ allowing\ this\ technique}{Number\ of\ attackers\ using\ this\ technique}$$

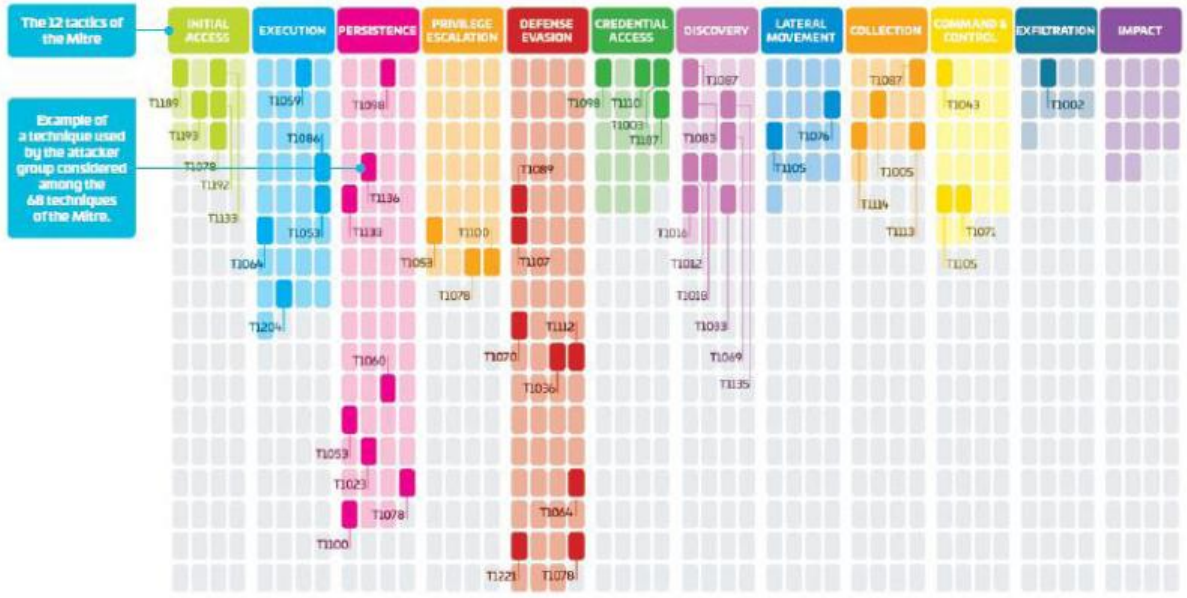
$$Score_{interest} = f(required\ permissions, impacted\ tactics, scarcity)$$

$$Score_{technique} = f(Score_{complexity}, Score_{interest})$$

$$Score_{tactic} = \sum Score_{technique}$$

$$Score_{attacker} = Average\left(\frac{Score_{tactic}}{Score_{maximum}}\right) \times 100$$

Example of profiling an attacker group



On this example the attacker group uses 11 tactics among the 12 of the Mitre and 44 techniques.

- ***Download the full report***

For more information, download the full report here:
https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK

4. A few examples of hackers' profiling

- FIN7, from the cybercriminal family

FIN7 is a financially motivated group that is active since at least 2013, which primarily targets the retail, hospitality and restaurant sectors, mainly in the US. There are assumptions that this is the same group as Carbanak, but it appears that these are two separate groups using similar tools, and therefore are currently tracked separately. Its main goal is to steal financial assets from companies, such as debit cards, or to get access to financial data or computers of finance department employees in order to conduct wire transfers to offshore accounts.

The group's often use phishing as their main attack vector, including tailored spear-phishing campaigns. In addition, the group used a front company dubbed "Combi Security", purportedly headquartered in Russia and Israel, to provide a guise of legitimacy and to recruit hackers to join the criminal enterprise.

- Anonymous Italia, from the hacktivist family

Anonymous Italia is one of the oldest hacktivist groups appearing on the Italian cyber-threat landscape, in 2012. The group is characterized by an anarchist ideology, with a strong sense for social justice, environmental issues. This highly ideological imprinting translates into a clear aversion towards Italian political institutions and security forces. In this context, we identify recurring patterns in the hacktivists' target selection. In fact, police, political parties, and government institutions have always been among their preferred targets.

Of note, many attacks were apparently conducted in cooperation with two other Italian hacktivist groups, namely LulzSec ITA, and AntiSecurity ITA, characterized by a similar ideology. Throughout its long activity, the group executed hundreds of data leaks, defacements and DDoS attacks. Notable was the 2015 attack against the Ministry of Defense (with thousands of leaked records), which also led to the arrest of two prominent members of the collective, who used the aliases Aken and Otherwise. Interestingly, the latter contributed to the development of a "serverless" portal for coordinating the group's operations, named Osiris, demonstrating significant technical capabilities. Of note, the group is also actively involved in the promotion of real-world operations, such as #OpGreenRights, #OpPaperStorm, and the Million Mask March.

- Turla, from the State-sponsored family

Turla alias Uroburos, Waterbug or Venomous Bear, is a cyber espionage threat actor active since at least 2008,when it breached the US Department of Defence. It is a Russian-speaking group and widely believed to be a Russian state-sponsored organization.

In 2015, Kaspersky described this Group as one of the "several elite APT groups have been using — and abusing — satellite links to manage their operations — most often, their C&C infrastructure".

During 2018 and 2019, Turla continues to target governments and international organizations in multiple waves of attacks and continues to improve its tools. The most recent attack targeted an Iranian APT group called OilRig.

Turla's attack on one of Iran's most successful groups combines opportunism and international interests. It should be recalled that since 2014 and the annexation of the Crimea, Western pressures and the fall of the oil price have plunged Russia into recession. For this reason, Russia has moved closer to Saudi Arabia, whose alliance with the United States had weakened under the Obama era in the alder of the Iranian nuclear agreement, supported by the former US President. It seems that the change in American diplomatic line since the election of Donald Trump has not diverted Saudi Arabia from this alliance. This rapprochement of interests is denounced by Iran, most recently at the OPEC meeting in Vienna in July 2019. The reason for the tension is also economic as both

- ***Lazarus, from the State-sponsored family***

Lazarus is not a single Threat Group. It represents the Bureau 121 which is one of the eight Bureaus associated to the North-Korean Reconnaissance General Bureau. The Bureau 121 is the primary office tasked with cyber operations. It was reorganized in September 2016 and it is now composed of:

- Lab 110 : It is the key cyber unit under the RGB; it applies cyberattack techniques to conduct intelligence operations
- Office 98: Primarily collects information on North Korean defectors, organizations that support them, overseas research institutes related to North Korea, and university professors in South Korea.
- Office 414: Gathers information on overseas government agencies, public agencies, and private companies.
- Office 35: Office concentrated on developing malware, researching and analyzing vulnerabilities, exploits, and hacking tools.
- Unit 180: Unit specialized in conducting cyber operations to steal foreign money from outside North Korea.
- Unit 91: focuses on cyberattack missions targeting isolated networks, particularly on South Korea’s critical national infrastructure such as KHNP and the ROK Ministry of National Defense, stealing confidential information and technology to develop weapons of mass destruction.
- 128 and 413 Liaison Office: Responsible of hacking foreign intelligence websites and train cyber experts.

- ***United Cyber Caliphate, from the cyberterrorists family***

United Cyber Caliphate (UCC) or Islamic State Hacking Division is a name of an umbrella for several hacking groups working for the Islamic State of Iraq and Levant (ISIS or ISIL) terrorist organization. The organization emerged in April 2016. Mostly known for its campaign against US military and governmental personal.

On April 4, 2016, the Cyber Caliphate Army (CCA), the principal ISIS hacking unit, and other pro-ISIS groups like the Sons Caliphate Army (SCA) and Kalacnikov.TN (KTN) merged and formed The United Cyber Caliphate (UCC). UCC groups include:- Cyber Caliphate, or Cyber Caliphate Army (CCA) was established shortly after the establishment of the Islamic State. The Key person behind the group was Junaid Hussain (Abu Hussain al Britani), or TriCK.

The most important cyber-terrorist attack of the CCA occurred on January 2015 when the Twitter and YouTube accounts of U.S Central Command and later on the Twitter accounts of the magazine Newsweek were hacked. - The Sons Caliphate Army (SCA) was established in 2016, as a subgroup of Cyber Caliphate.

Mostly known for disrupting social media traffic on Facebook and Twitter, CCA claimed to have hacked 10,000 Facebook accounts, more than 150 Facebook groups and over 5,000 Twitter profiles. - Kalashnikov E-Security Team was established in 2016. This group is focused on tech security advisory for ISIS jihadists. It also uploaded ISIS-related jihadi literature, sharing posts from cyber jihadi groups, reporting successful attacks on websites and Facebook pages and publishing various web-hacking techniques. Gradually, the hackers started to conduct or assist in defacing hacks.

5. Other Cyberthreat Intelligence reports made by Thales

Thales – Verint 2018: The Threat Landscape Report

The 'Threat Landscape Report' is the first fruit of the collaboration between Thales and Verint, the strategic partnership between worldwide key players in the cybersecurity industry. Both companies combined their vast knowledge and expertise in order to provide meaningful insights into the dynamic cyber threat landscape and growing diversity in cyber security threats in Europe.

The report looks at new and technologically advanced cyber threat capabilities which are forcing companies to adopt a more proactive security posture

Download the report: http://www.thalesgroup-events.com/ReportThalesVerint

THALES - SEKOIA 2019 - Report on financial sector cyber threats

The financial sector is one of the favorite targets of cyberattackers. Cash dispensers, financial transactions, bank data theft, etc..; cybercrime causes the loss of billions of dollars for the global financial industry, a risk that sector stakeholders can no longer take. In their report on cyberfinancials, Thales and SEKOIA bring a detailed light on cyber threats in the financial sector.

Download the report: http://www.thalesgroup-events.com/ReportTHALESSEKOIA

Key findings: https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/news/thales-and-sekoia-release

6. Any questions?

PRESS CONTACTS

Thales, media relations
Constance Arnoux
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com

FIND OUT MORE

Thales Group
Télécharger les photos
@Thalesgroup