CCN-CERT

centro criptológico nacional

Cyber threats and Trends 2019

CCN-CERT IA-13/19
EXECUTIVE SUMMARY

CCN-CERT

IA-13/19 EXECUTIVE SUMMARY

Edit:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.09.12 13:10:53 +02'00'

Índex

Foreword

For the eleventh consecutive year, the **National Cryptologic Centre**'s Computer Emergency Response Team (**CCN-CERT**) has drawn up the **Cyber Threats and Trends Report. Edition 2019**[1]. This is an extensive document with more than 128 pages (an extract of which is presented here), analyzing national and international cyber threats, as well as their evolution and future trends.

Much of the information contained in this Report is the result of the CCN-CERT's experience, which, as the **National Governmental CERT**, managed a total of 38,029 cybersecurity incidents during 2018, 2.7 % of which were classified as a "very high" or "critical" danger. In this year, the National Cryptologic Centre has once again confirmed how States and State-sponsored groups continue to represent the most significant cyber threat on the international scene.

Alongside this, attacks on the supply chain, actions by terrorist groups, jihadists and hacktivists, fake news, as well as personal data attacks (with the ultimate aim of committing certain crimes, stealing credentials, identity theft or espionage), were also highly present in 2018.

The matrix document, as well as this executive summary, analyses **the main cyber incidents of 2018**; the **methods of attack** used by the **threat agents** against their victims;

multiple existing **Vulnerabilities** that facilitate this situation and the main targets. It also looks at the measures required to improve security in companies and institutions.

Finally, and considering how cyber incidents were changing over this period, **trends** are addressed concerning the next few months during which state agents might be expected to continue their intrusion campaigns as part of their national strategies.

The purpose of this Executive Summary (as well as the General Report) is to be useful to information security managers at Spanish public sector entities, organizations of strategic interest and, in general, to our country's companies, professionals and citizens. This has the ultimate aim of strengthening national cybersecurity.

[1]CCN-CERT IA 13/19 available at the CCN-CERT website.
https://www.ccn-cert.cni.es/

2 Cyber incidents in 2018

The following sections look at the most significant basic aspects of cyber incidents in 2018.

2.1.Digital sovereignty of States

The use of technology manufactured in other States is a source of concern for Governments around the world, especially in Europe.

Digital sovereignty is understood as a country's drive to regain control of its own and its citizens' data. On the military side, it also includes the possibility of a state developing offensive and defensive cybersecurity capabilities without relying on foreign technology. On the economic side, it covers issues ranging from taxing large technology companies to setting up new locally-based companies.

2.2.States as the main source of threats

States, and groups sponsored by them, and their actions against other countries, their institutions, companies and citizens continue to represent the most significant cyber threat. The objective of this type of attack is always the same: steal information to improve its strategic, political, economic or innovative position (espionage). This now also includes an attempt to influence public opinion in the countries under attack or interrupt normal provision of essential services (sabotage).

In this type of attacks, it is common to use very simple techniques, such as phishing, which takes advantage of the victim's human vulnerabilities. It is used to collect sensitive or confidential information for a subsequent attack

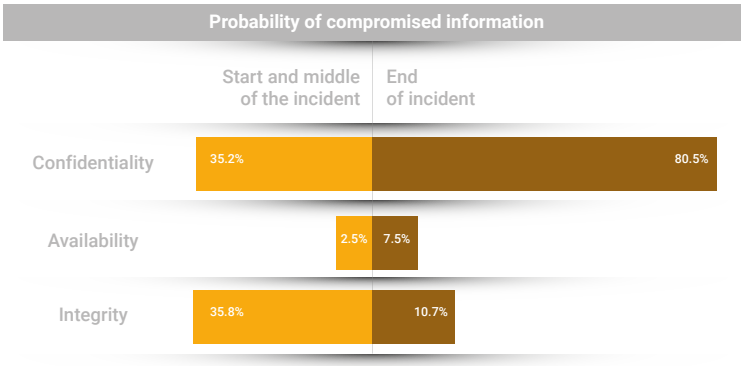
2.3.Attacks on the supply chain

In view of the effectiveness and benefits for attackers, it is foreseeable that this type of action will continue in the coming years, as this method offers attackers two advantages: they can use a trusted supplier as the source of the harmful distribution and limit the attack surface, without revealing their objectives.

2.4.Actions by terrorist groups, jihadists and hacktivists

During 2018, the threat from terrorist or hacktivist groups has remained stable. Although Jihadist groups have maintained their digital propaganda, recruitment and fundraising actions, they have so far not perpetrated any significant cyberattacks beyond website disfigurements and data theft.

2.5.Cybercrime and personal data



Over the last few years, attacks against personal data have increased, not only by cybercriminals or hacktivist groups, but also by States[2].The aim is usually to commit certain crimes, identity theft (credentials), impersonation or espionage.

Loss of data confidentiality is often the most frequent result of attacks, as demonstrated by targeted attacks (TBA) in connection with cyberspyware[3].

2.6.Abuse of fake data and news

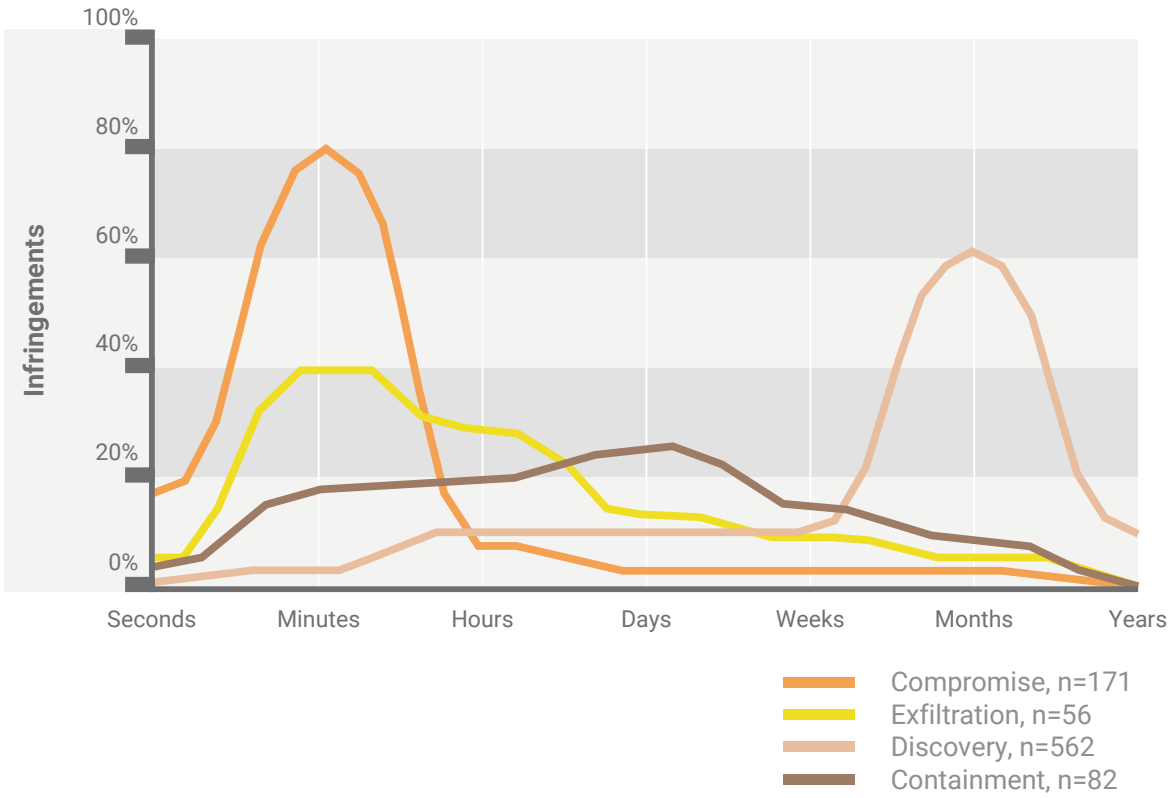
In the same way that fake news aims to influence individuals' opinions and behavior, personal information shared on social networks (Facebook, Twitter, LinkedIn, etc.), once properly analyzed and correlated, can enable sophisticated - and individualized - social engineering attacks.

2.7.Times involved in cyberattacks

In most cases analyzed, and when the attacks are successful, the time frame for the information system to be compromised is still very short. The time between the first hostile action and an asset being compromised is often measured in seconds or minutes. However, the time frame for discovery or detection, which depends largely on the type of attack, is usually expressed in days, weeks, or months.

[2]See: https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/ and https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN

[3]Figure source: Verizon: 2018 Data Breach Investigations Report.



Estimation of the times involved in cyberattacks. Source: Verizon

2.8.Facilitating elements of cyberattacks

Facilitating elements are entities or components that increase accessibility and/or effectiveness of further attacks or the methods used in their commission. Such is the case, for example, of criminals who exchange stolen information, leading to subsequent attacks; or entities that build, rent or release infrastructures to third parties (over the Dark Net) to commission such actions (botnets, for example), enabling threat agents with limited knowledge to perpetrate attacks easily and at an affordable price, etc...

Constant connection of new **IoT** devices to the Internet, thereby promoting the distribution of malicious code or participating in **DDoS** attacks, is also a significant factor facilitating this problem. In addition, **cryptojacking**, a method that seeks to make a profit from the processing capacity of victims' computers, will be one of the most serious threats in the coming years.

3 Threat actors

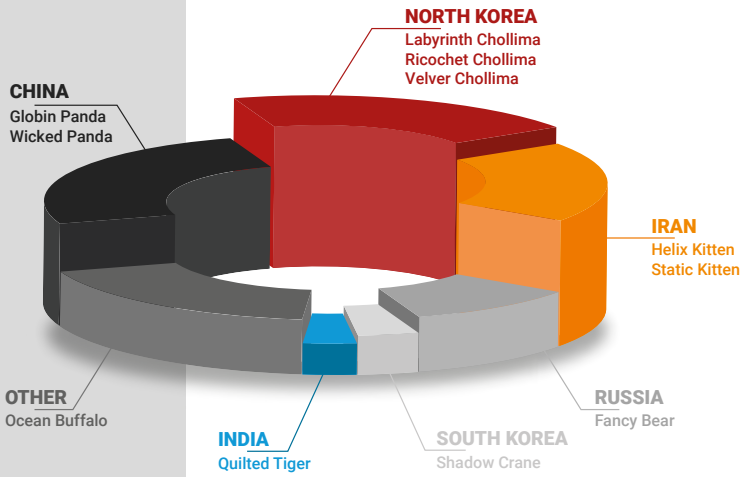
The number of threat agents has increased significantly due, in part, to easy access to new attack tools and continuing difficulty to prove authorship. In addition, it is increasingly common for different types of actors to use the same tools.

Code propagation

More than 60% of the world's email traffic in 2018 contained harmful cargo and was involved in more than 90% of cyber attacks.

3.1.States

There has been an increase in the use of harmful code by States, in an attempt to exploit vulnerabilities in Critical Infrastructure information systems.



Intrusions directed by adversaries in 2018

Main adversaries reported

Source: 2019 Global Threat Report.

The goal of these attacks has frequently been to obtain information on how well organizations have implemented their security measures, in order to get hold of enough data to plan future attacks. This activity has been detected, especially against European targets. In addition, **spearphishing** is still used for cyber espionage.

3.2.Cybercriminals

Cybercriminals continue to be one of the most active threat agent groups, featuring in more than 80% of malware activity.

MOST POPULAR METHODS

Propagation of malicious code through email: More than 60% of global email traffic in 2018 contained malicious cargo and was involved in more than 90% of cyberattacks.

Use of **cryptojacking/cryptomining malware** which, according to various estimates, has resulted in losses of $880 million.

Refining **phishing** using social engineering[4] techniques and constant innovation to persuade users of the authenticity of scams.

Innovation in the platforms of **Cybercrime as a Service**[5]. In addition to the improvements in the services offered, these developments allow greater ease of use, which contributes to extend its popularity and encourage more efficient attacks.

[4]See: https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf
[5]See: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

3.3.Cyberterrorism and Cyber jihadism

Monetization, propaganda and recruitment are the main objectives of this group of threat agents, which still has low action capacity. However, given the availability of Crime-as-a-Service and the potential to recruit humans, international analysis shows that cyberterrorism will increase significantly over the coming years.

3.4.Hacktivists

Hacktivists are still active in dissemination of confidential information collected on websites under attack, in development of DDoS actions and in disfigurement of web pages, with the aim of attracting media attention without generally seeking to monetize their actions.

From a technical point of view, Linux and Apache have been the main web platforms involved in their actions[6].

[6]See: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/web-defacements-exploring-the-methods-of-hacktivists

3.5.Internal actors

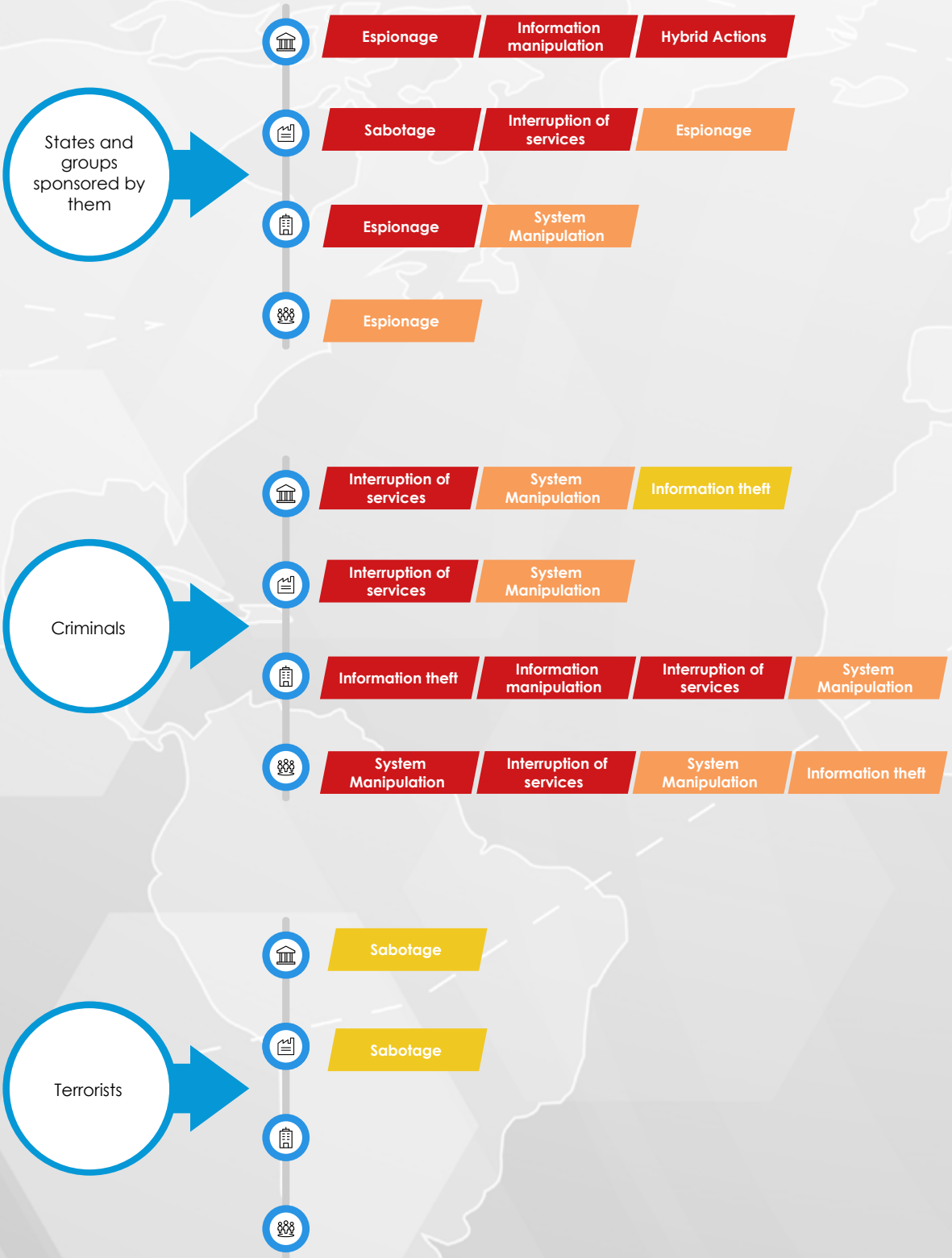
This group, also known as insiders[7], is responsible for about 25 % of incidents. Despite being perceived as one of the highest threats, only 64 % of organizations say they are investing in deterrence measures.

Most damage appears to be caused by unintentional employee actions[8], including accidental data disclosure, failure to recognize phishing attacks, or errors due to misconfiguration[9].

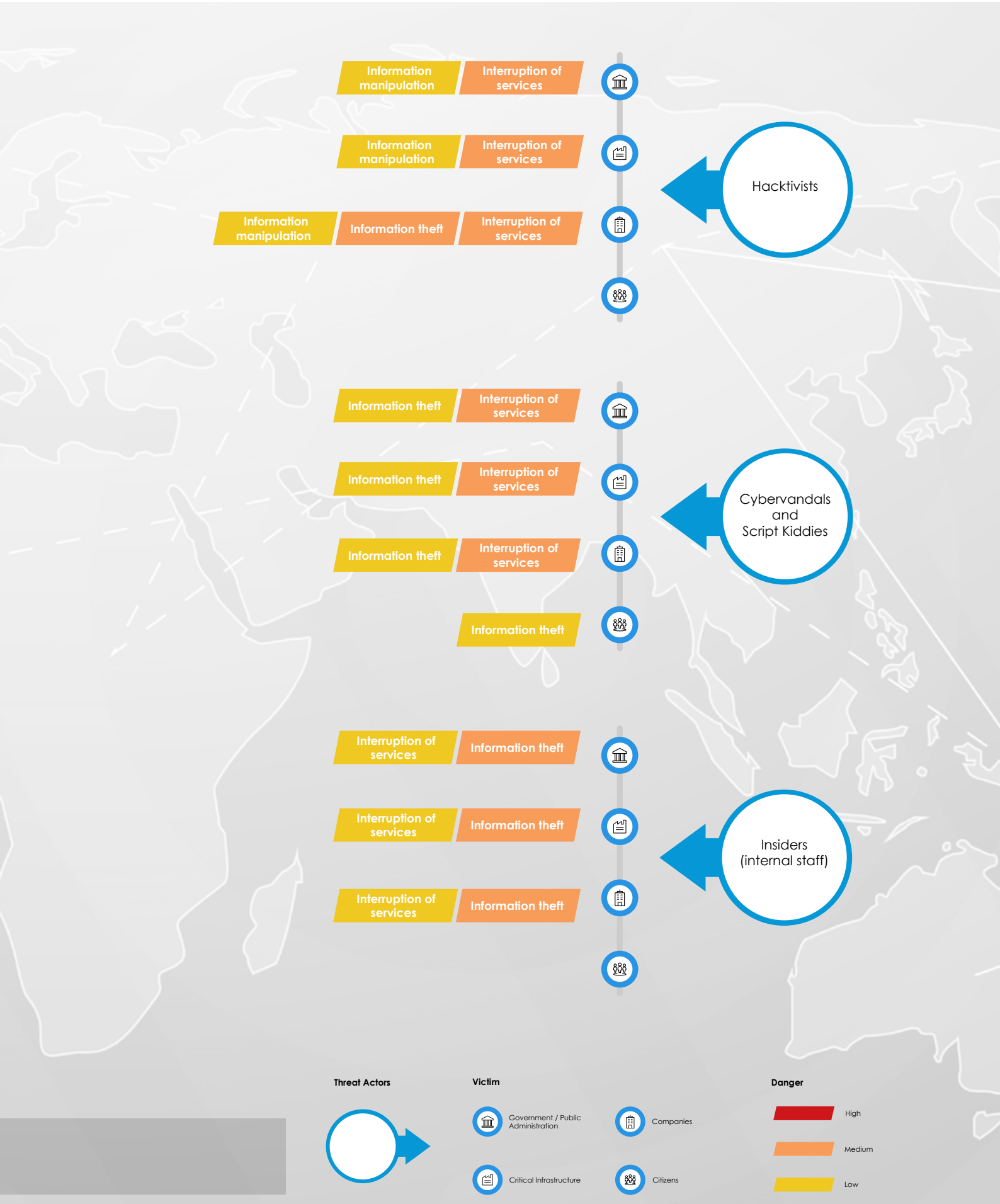
Internal threats, which are the second source of incidents, can also materialize indirectly, with attacks on the supply chain.

[7]People with access to the system from within the security perimeter. That is to say, with certain authorization to access.
[8]See: https://www.doxnet.com/2018/04/insider-use-and-abuse-identifying-internal-threats-and-how-to-mitigate-them/
[9]See: https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017

Cyber Threat 2018



Source This threat matrix is based on the typology of actors studied by M. de Bruijne, M. van Eeten, C. Hernandez Gañan and W. Pieters in "Towards a new cyber threat actor typology a hybrid method for the NCSC cyber security assessment" (NCSC (TU Delft 2017)).


Information manipulation
Interruption of services
Information manipulation
Interruption of services
Information manipulation
Information theft
Interruption of services
Hacktivists
Information theft
Interruption of services
Information theft
Interruption of services
Information theft
Interruption of services
Cybervandals and Script Kiddies
Information theft
Interruption of services
Information theft
Interruption of services
Information theft
Interruption of services
Insiders (internal staff)
Threat Actors
Victim
Government / Public Administration
Companies
Critical Infrastructure
Citizens
Danger
High
Medium
Low

4 Vulnerabilities

The following were the most significant vulnerabilities in 2018

4.1.Vulnerabilities in software and hardware

The number of known vulnerabilities in software products has been high and there are no indications that this situation will change in the coming years. There are clear trends in software that affect the security of the end product:

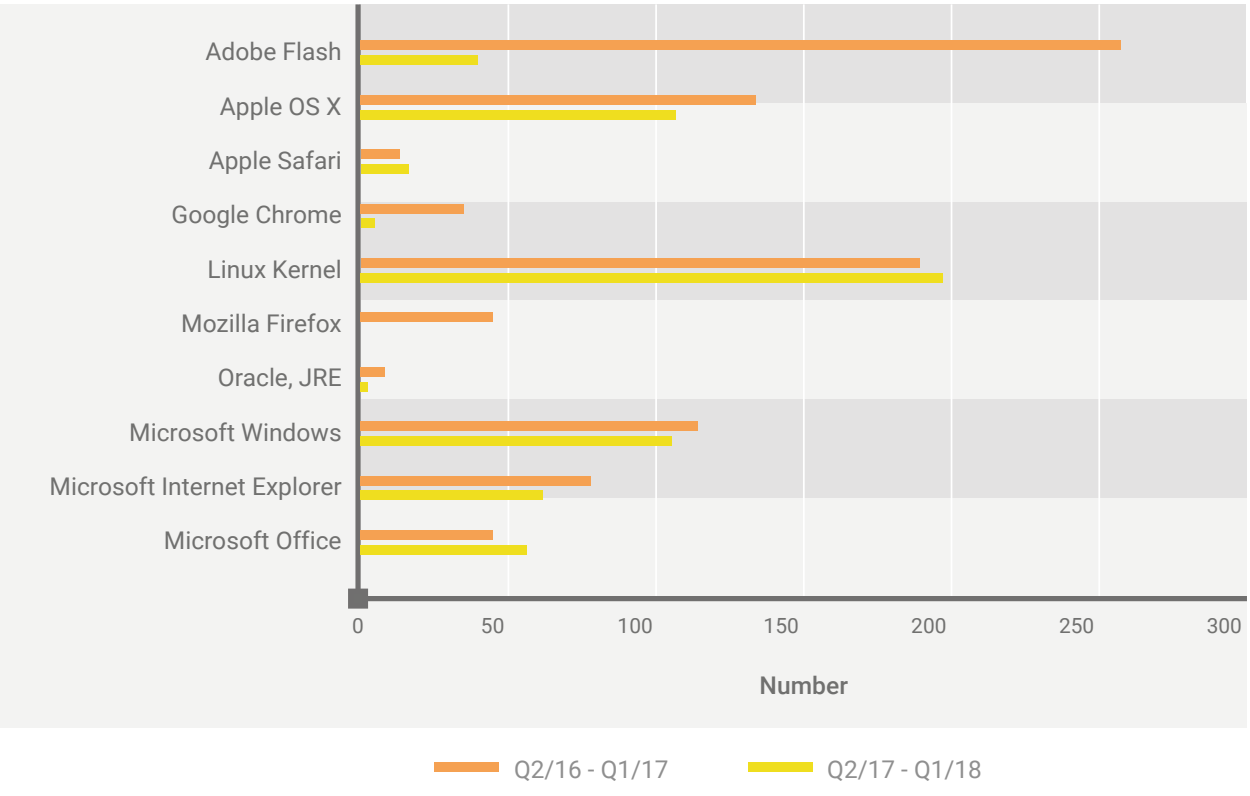
- Increased complexity of end-user applications
- Grouping of partially updated software components
- Uncontrolled integration of elements of external origin
- Speed optimizations at the expense of security
- Neglect of problem solving with reference to mitigation measures
- Rejection of security updates by many manufacturers

Among the most outstanding in software were anomalies in **Mozilla Firefox** and **Google Chrome**. It seems that neither browser has maintained entries in the MITRE CVE database.

Although entries are referenced in their own publications, they are not annotated in the public database so that a description of the vulnerability is not given, nor does it refer to the affected product.

Researchers from the Münster University of Applied Sciences, Ruhr University Bochum and KU Leuven (Belgium) also found serious weaknesses in the implementation of the **OpenPGP** and **S/MIME** email encryption

standards, which they published in May 2018. Based on such vulnerabilities, attackers could manipulate encrypted emails in such a way that the message content could be forwarded in plain text after being decrypted by the recipient.



Critical CVE of the most used software

A product that contains publicly known vulnerabilities at the time of purchase should be considered defective from an IT security perspective. Software maintenance by the manufacturer, including removal of vulnerabilities, should not only be the usual procedure and mechanism for satisfying the applicable legal regulations, but should also be requested by the consumer, as part of the service.

4.2.New forms of exploitation

In January 2018, research teams revealed two new families of hardware vulnerabilities, called **Spectre** and **Meltdown**, that would allow attackers to obtain confidential information by running the program code on the victim's computer.

As a new form of exploitation, it is worth mentioning the **GLitch** vulnerability, published by researchers at the Free University of Amsterdam, capable of perpetrating what are known as Rowhammer attacks through a computer's graphics processor. Also, by exploiting a vulnerability in **Apache Struts**, Equifax reported that the attackers had stolen data from 4.9 million Americans, causing Equifax a loss of $87.5 million.

4.3.DDoS attack through publicly accessible systems

As of February 2018, the use of so-called "Memcached" attacks was demonstrated in DDoS actions, through systems that were accessible to the public. Memcached systems are designed to temporarily store small amounts of data from other sources such as databases and APIs, to make websites faster. The systems do not require authentication for communications and have not been developed to be publicly accessible, thus enabling attacks by amplification.

According to Panda, the most powerful DDoS attack in history took place on February 28, 2018: 1.35 terabits per second of traffic to GitHub, the web platform for collaborative development projects. A few days later, the record was broken with an attack featuring traffic peaks of 1.7 Tbps.

In these actions, the attacker sends what appears to be a request in the name of the target, falsifying their IP address. Since the answers are longer than the request, the actor can use a relatively small bandwidth to set up a larger attack.

4.4.Medical and sanitary device security

Several laboratory tests in the United States have shown that medical devices such as pacemakers, defibrillators or respirators are vulnerable to cyberattacks. Consequently, cybersecurity must be integrated and implemented from early in development and manufacturing of these devices, to guarantee their use.

Authentication mechanisms in digital medical devices are often insufficiently protected and data encryption techniques for communication and storage are weak or even non-existent. In these circumstances, it would be possible to gain unauthorized access and manipulate the device without the patient's knowledge.

The most powerful attack in 2018

1.35 terabits per second of traffic to GitHub. the web platform for collaborative development projects. A few days later, the record was broken with an attack featuring traffic peaks of 1.7 Tbps.

4.5.Mobile banking security

Internet payments are increasingly made using mobile devices, encouraging financial institutions to offer online banking apps for these devices. Such banking applications are complemented by a second application, known as a "TAN application" that generates a number (TAN) to secure the transaction performed using the banking app.

To do this, the banking application and the application that generates the TAN usually operate with a single device. This poses a significant risk if the device is compromised, as the attacker could gain control of both applications. All of this leads to enormous current illegal trafficking of credentials.

4.6.Domotics and Internet of Things

There are two possible threat scenarios for IoT devices: in the first scenario, the system is compromised in order to cause direct or indirect damage to the user, as shown in the table below.

In a second threat scenario, the IoT device is compromised and can be used as a means to attack other targets. In these cases, as the computer does not register that its functionality has been altered, the attack often goes unnoticed.

Construction of botnets
Massive hijacking of poorly secured IoT devices allows creation of large botnets that can lead to DDoS attacks.

Identity concealment
Compromised devices can be used as proxy servers to hide new attacks.

Cryptocurrency mining
It is possible to use the collective computing power of the IoT devices involved in cryptocurrency mining. In this case, the attack is easier to detect, because it slows down normal operation of the equipment.

Clic-Fraud with advertising banners
The attacker uses many different IP addresses of hijacked IoT devices to generate clicks on advertising banners, videos or social network content. In this way, an economic benefit can be obtained with billing based on clicks. In addition, the advertiser is directly affected through the payment of a commission for simulated clicks.

4.7. Vulnerabilities in chips

The components that store cryptographic keys or implement cryptographic algorithms are essential in the most important security applications, such as secure authentication, encrypted communication or electronic signatures. Secure key storage, and particularly key processing, remains a major challenge as measurable physical phenomena inevitably arise that allow conclusions to be drawn about passwords.

Algorithmic weaknesses are another problem. Sometimes, secure cryptographic algorithms cannot be implemented due to the limited storage and processing capacity of the security elements. Very complex operations, such as key generation on RSA, are still time-consuming depending on the key length. The use of FastPrime, a proprietary algorithm for building large prime numbers, accelerates key generation; however, keys generated in this way are cryptographically weaker. Thus, with the help of the Coppersmith attack, an RSA module can be efficiently factored if the highest bits of one of the prime numbers are known.

5 Cyberthreats in 2018

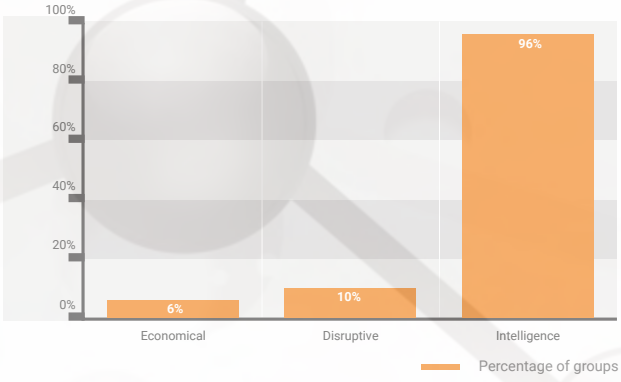
This section describes developments in methods, procedures and tools that threat actors have used during the period under consideration.

5.1.Advanced Persistent Threats (APT)

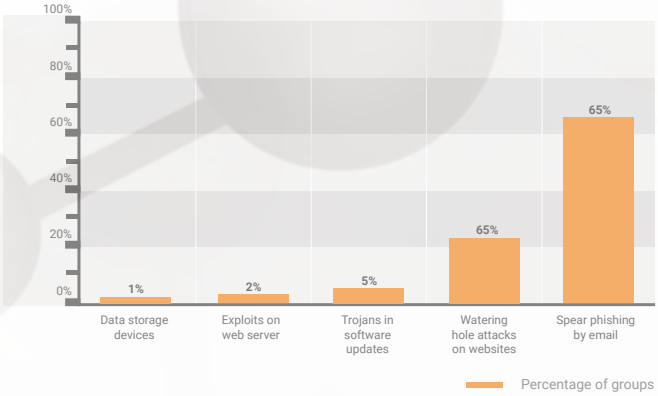
In relation to IoT devices, there are two possible threat scenarios: in the first scenario, the system is compromised in order to cause direct or indirect damage to the user, as shown in the table below.

This attack vector is also known as supply chain attack, since they initially attack suppliers of the actual target, using them as a bridge to reach the ultimate target's network. This is another mechanism currently used by groups such as **APT10** as part of the Cloud Hopper campaign.

A later phase of APT is lateral movement, during which the attackers extend their influence into the victim's net. They use legitimate management tools such as PowerShell or Windows Management Instrumentation, WM, or publicly available tools such as Cobalt Strike, Powershell Empire, and Koadic, making it difficult to classify attacks.



Targeted Attack Targets



Infection vectors in targeted attacks

For protection against TPA, the following key measures are recommended

- Use two-factor authentication for VPN and webmail as a phishing protection mechanism.
- Use blacklisted directories that hinder the initial execution of malicious code from mail or browser attachments.
- Restrict communication between customers to essential functions to make sideways movement more difficult for attackers.
- The layer model in Active Directory ensures that highly privileged access data is not used on low-privileged systems, requiring additional effort from attackers to obtain highly privileged access data.

Governmental Organizations	Defense
APT12/ NumberedP , APT28/ Sofacy, APT29/ CozyBear, APT32/Ocean-Lotus APT37/Reaper Bahamut, BlueMushroom, Cadelle/Chafer, Callisto, Charming-Kitten, Dark-Caracal, DarkHotel, Dropping-Elephant, Emissary-Panda, Extreme-Jackal, Gamaredon, Gaza-Cybergang, Greenbug, Hammer-Panda, Infy, KeyBoy, Lapis/TransparentTr., Longhorn, Lotus-Panda, Machete, Micropsia, Muddy-Water, Naikon/OverrideP., Leviathan, OilRig, Operation-Cleaver, Project-Sauron, Shamoon, Snake, Sowbug, Tick, TidePool/Ke3chang, Tonto, Transparent, Tribe, Tropic-Trooper/PirateP, Vermin, Viceroy-Tiger	**APT28/Sofacy, APT37/Reaper, AridViper, BlueMushroom, Callisto, Charming-Kitten, C-Major/ PureStrike, Dark-Caracal, Dropping-Elephant, Gamaredon, Gaza-Cybergang, Hammer-Panda, HelixKitten, Lotus-Panda, Machete Naikon/OverrideP, Leviathan, OilRig, Operation- Cleaver, Project-Sauron, Snake**

Opposition	Media	Energy
Ahtapot, APT32/Ocean-Lotus, Bahamut, BlackOasis, Bookworm, Charming-Kitten, Dark-Caracal, EnergeticBear, Flying-Dragon, Group5, Infy, Neodymium, Operation-Cleaver, Operation, Manul, Promethium, ScarCruft, Sima, Stealth-Falcon, SunTeam Temper-Panda, ZooPark	APT28/Sofacy, APT32/Ocean-Lotus, Bahamut, BlackOasis, BugDrop, Callisto, Charming-Kitten, Dark-Caracal, DarkHotel, Dropping-Elephant, GazaCybergang, Infy, Olympic-Destroyer, Operation, Manul, Sandworm, ScarCruft, Shrouded-Crossbow, Stealth-Falcon, SunTeam, Tick	APT10APT18/Wekby, APT29/CozyBear, Charming-Kitten, Electric-Powder, Emissary-Panda, Energetic-Bear, Gaza-Cybergang, Greenbug, HelixKitten, Kraken/Laziok, Longhorn, Machete, Muddy-Water, OnionDog, Operation-Cleaver, Sandworm, Shamoon, Tropic-Trooper/ PirateP

Financial	Video conference	NGO	Universities
APT18/Wekby, APT29/ CozyBear, BlueMushroom, Dark-Caracal, Dropping-Elephant, Emissary-Panda Energetic-Bear, Equation-Group, Gaza-Cybergang, Hammer-Panda, Longhorn, OilRig, Sandworm	APT18/Wekby, Codoso, Emissary-Panda, Hammer-Panda, HelixKitten, Longhorn, Machete, Muddy-Water, OilRig, Project-Sauron, Thrip	APT29/CozyBear, APT37/Reaper, Callisto, Charming-Kitten, DarkHotel, Hammer-Panda, Honeybee, Infy, NilePhish, Operation-, Cleaver, Rocket-Kitten	APT10/menuPass, BugDrop, Charming-Kitten, Codoso, Dark-Caracal, DarkHotel, Greenbug, DarkHotel, Longhorn, Leviathan, Rocket-Kitten

High Technology	Transport	Aerospace	Health	Legal
APT18/Wekby, Charming-Kitten, Codoso, LEAD/Winnti, Tick	Cadelle/Chafer, NanHaiShu, OilRig, OnionDog, Project-Sauron, Shamoon	APT28, Dropping-Elephant, Emissary-Panda, Leviathan, Hammer-Panda, Greenbug, Longhorn	APT10/menuPass, Leviathan, LEAD/Winnti	APT29/CozyBear, Codoso, Dark-Caracal, DeepPanda, Leviathan

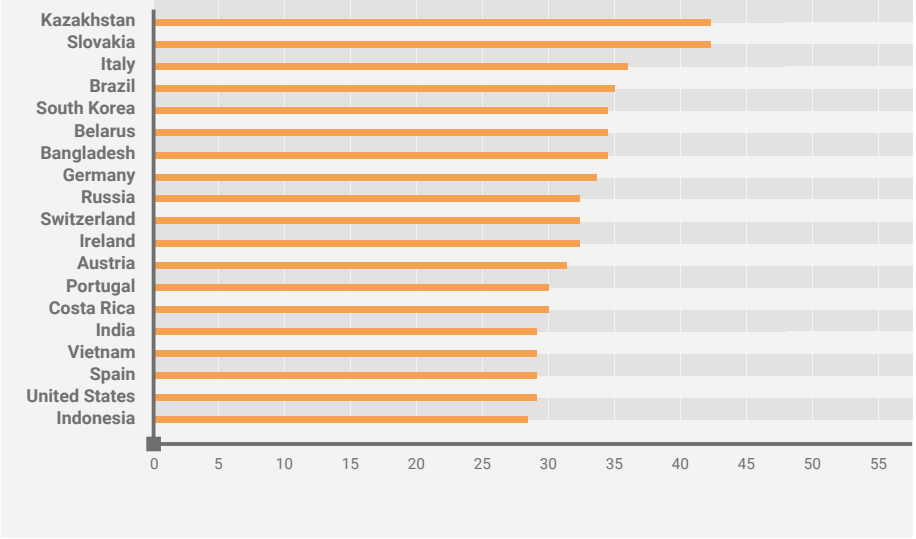
Source: BSI, evaluation of public reports

5.2.Cyber Espionage

Cyber espionage is becoming a common practice in certain states, usually targeting industrial sectors, critical and strategic infrastructures around the world, in an attempt to obtain state secrets or geopolitical and commercial benefits.

The number of economically focused and State-sponsored cyberattacks has increased throughout 2018. These actions, also targeting use of IoT, are also on the rise in the public service sectors. In addition, the use of APT indicates that many attacks directed against the financial sector originate from the tactics, techniques and procedures of cyber espionage, used by actors such as Cobalt Group, Carbanak and FIN7.

Operational technology (OT) networks in industries are an ideal field of action for cyberthreat actors. These agents use remote administration tools (RAT) that are already installed in industrial control systems (ICS).



Countries where RATs were used in espionage incidents during the first semester of 2018. Source: Securylist

5.3.Hybrid Threats

So-called "hybrid threats" are coordinated and synchronized actions usually originating in States or agents sponsored by them, which deliberately attack systemic vulnerabilities of States and their institutions, through a wide range of media and in different target sectors: political, economic, military, social, informational, infrastructure and legal, using cyberspace as the most versatile and appropriate tool for their purposes. This is therefore the phenomenon resulting from convergence and interconnection of different elements which, taken together, constitute a more complex, multidimensional threat.

5.4.Attacks on Industrial Control Systems (ICS)

Industrial Control Systems have been frequent victims of undirected attacks, infecting operator workstations or other control components with ransomware. The entry vectors were mainly phishing emails and removable media, although there were also cases where the infection occurred as a result of the use of incorrectly configured remote maintenance systems. In all cases, the malicious code exploited known vulnerabilities of obsolete software and inadequate segmentation between office networks and production networks. All indications show that such incidents will continue to pose a significant threat to the ICS in the coming years.

The progressive introduction of "Industry 4.0"[10] also offers new starting points for criminal activities

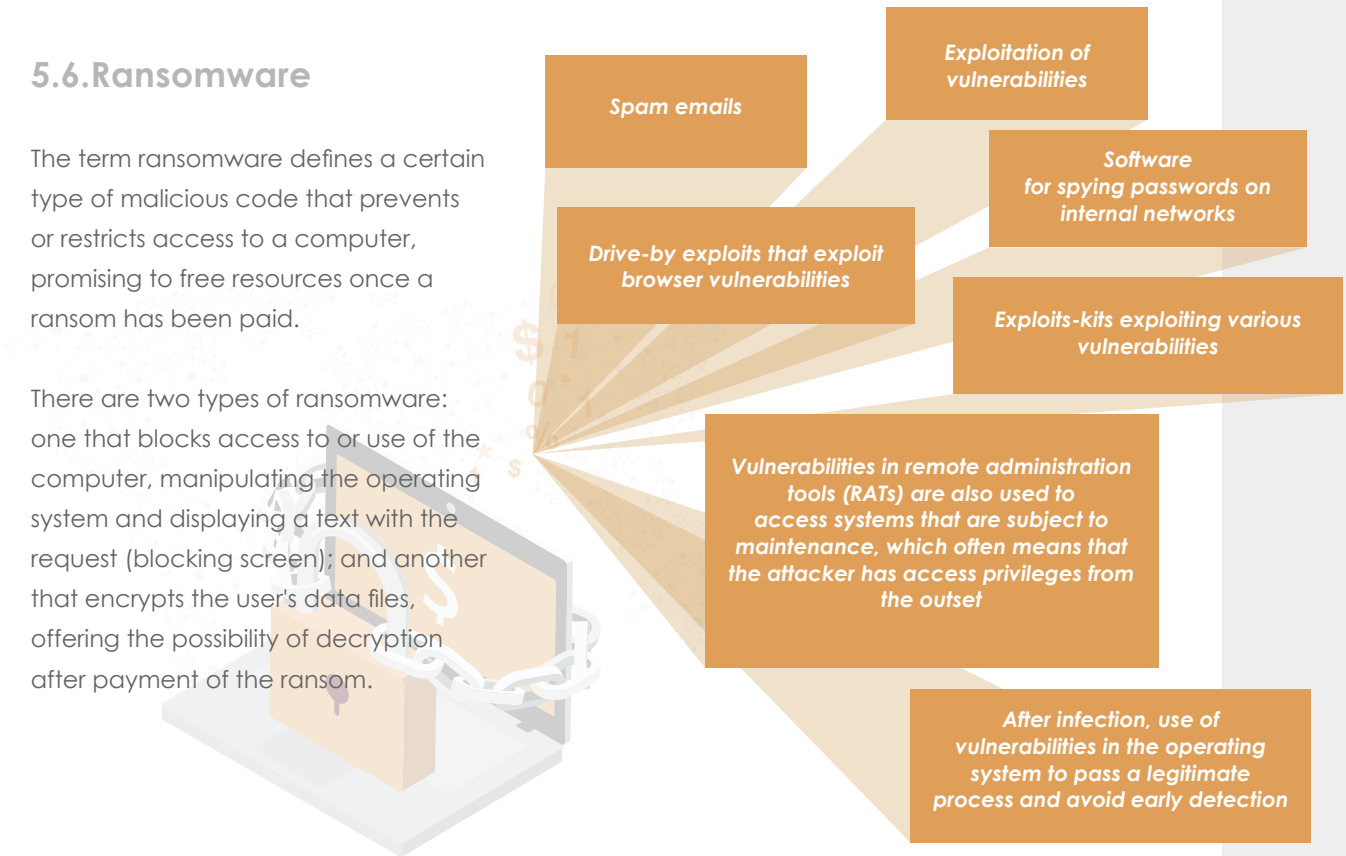
5.5.E-mail address

During 2018, the main cyberattacks of this type were the cases of phishing or spear-phishing perpetrated by criminals, States or actors sponsored by them with the aim of developing espionage or sabotage actions. According to Verizon, States used phishing techniques in 70 % of their cyberattacks[11].

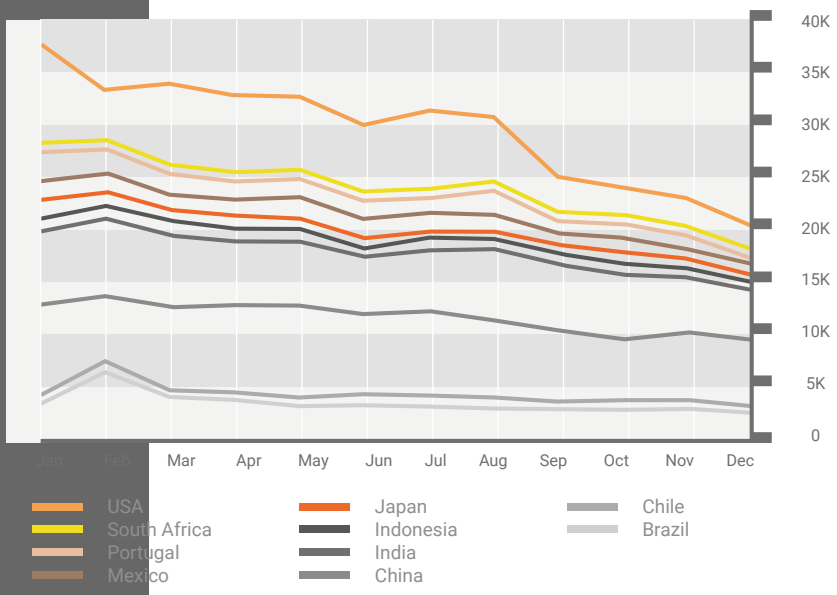
5.6.Ransomware

The term ransomware defines a certain type of malicious code that prevents or restricts access to a computer, promising to free resources once a ransom has been paid.

There are two types of ransomware: one that blocks access to or use of the computer, manipulating the operating system and displaying a text with the request (blocking screen); and another that encrypts the user's data files, offering the possibility of decryption after payment of the ransom.

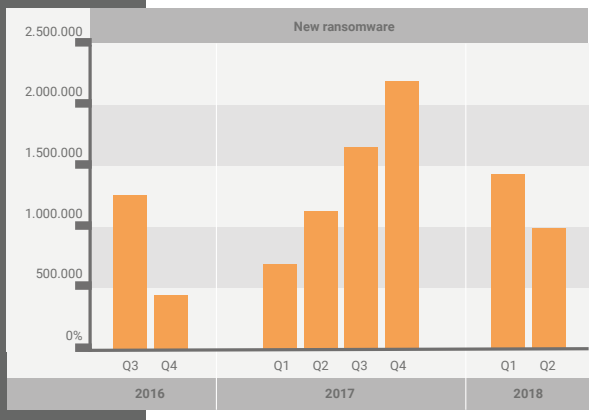


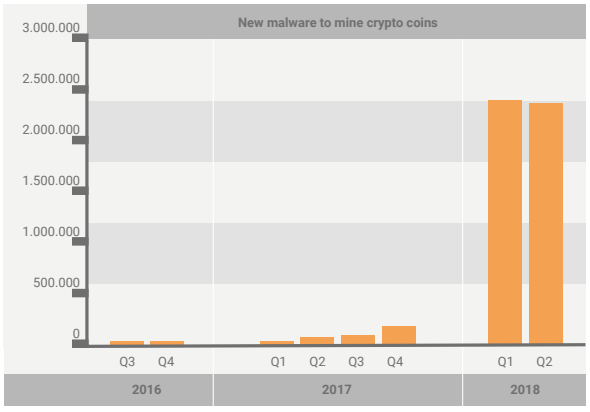
[10]Industry 4.0 and its synonym, the recently initiated Fourth Industrial Revolution, where artificial intelligence would be the central element, related to the growing accumulation of large amounts of data, the use of algorithms to process them and the massive interconnection of digital systems and devices. (Source: Wikipedia)
[11]Verizon op. cit.



Ransomware penetration by country/month during 2018 (Source: Symantec).

Like the botnet services available for DDoS attacks, there are now also offers from Ransomware-as-a-Service. However, ransomware appears to be on the decline as other models, such as crypto mining, become more profitable or promise more consistent profits.





Correlation between ransomware and cryptojacking detection volume (Source: McAffee)

5.7.Spam and Phishing

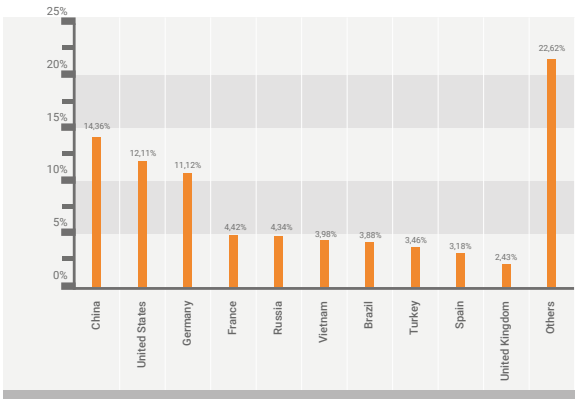
Unsolicited emails are often referred to as spam and are divided into three categories:

Conventional Spam
Often used to advertise products or services, as well as part of fraud attempts.

Malware Spam ("malspam")
Used by threat agents to infect recipients' systems with malicious code. Malware can come in an email attachment or be introduced indirectly through a link in the body of the email or in attachments. This link leads to the malware or a website that contains drive-by exploits.

Phishing
It encourages users to deliver information, such as logging in to websites controlled by threat agents.

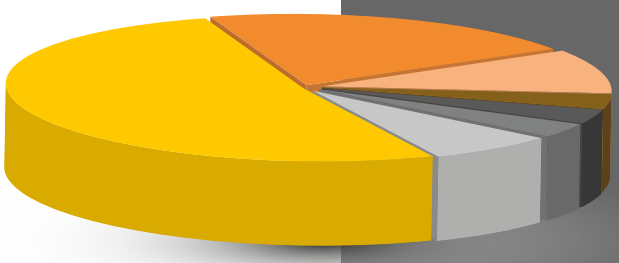
In most cases, spam is sent through compromised servers, infected client systems, or legitimate email accounts, using stolen login information.



Distribution of the origin of spam actions (Source: Securlist)

Frequently, systems that distribute spam are assembled into a botnet, making it easier for attackers to market their activities as a service.

Dates	52,20%
Unknown	20.80%
Software	10.00%
Storage	3.30%
Pharmaceuticals	3.30%
Stores	3.20%
Other	7.20%



Distribution of spam by areas (Source: BSI)

The **Necurs** botnet has remained the largest sender of spam messages. However, smaller malspam campaigns have still been seen outside this botnet. Botnets concerned with the diffusion of **Emotet** are of particular interest. This malicious code uses Outlook data obtained during an infection to send an email that claims to be from a person already in contact with the potential victim.

Phishing has been shown to be the preferred way of engaging organizations [12]: 75% of EU Member States reported cases of phishing[13]. One last fact: more than 90% of harmful code infections and 72% of data violations in organizations originated from phishing attacks[14].

75 % of EU Member States revealed cases of phishing.

THESE ARE THE MOST

significant events of 2018 concerning phishing

- Phishing attacks have become more **specific**.
- Change of objective: from consumer to **organization**.
- Increase in phishing attacks on **mobile devices**: they have increased by around 85 % per year since 2011. Advanced actors use mobile phishing techniques, e.g. Dark Caracal and Pegasus.
- Growth of phishing sites using **HTTPS**: By 2017, one-third of phishing websites were accessed through HTTPS mechanisms.
- The problem of B**usiness Email Compromise (BEC)** remains: this type of phishing attack aimed at executives and employees of economic or human resources departments in an attempt to steal money from their organizations. From October 2013 to May 2018, 78,000 BEC attacks have been reported worldwide, with estimated losses of $12 billion.
- **Spearphishing** is the de facto delivery method for APT groups: 71 % of APT groups have used spearphishing as a vector of infection. During 2018, the highest-profile organized crime groups were FIN7 and Cobalt Group. In addition, state actors continue to use it as the main vector of infection for their cyber espionage and service interruption operations.
- Trends in **malicious attachments**, the most common are Microsoft Office documents, data files, JavaScript files, Visual Basic scripts, and PDF documents.

[12]See: https://www.fireeye.com/company/press-releases/2018/new-fireeye-email-threat-report-underlines-the-rise-in-malware-l.html
[13]See: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
[14]See: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

5.8.Malicious code

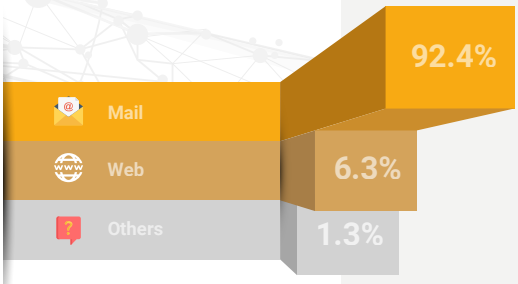
EMalicious code or malware is an integral part of most attack scenarios. As in previous years, it remains one of the greatest threats to consumers, businesses and the public sector.

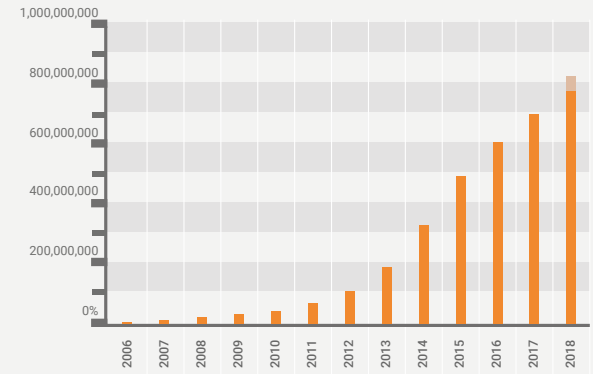
The last months of 2017, 2018 and the first months of 2019 have shown the following:

- Although adware is one of the easiest ways to distribute malicious code, there have been few developments of this threat.
- 94% of all malicious executables have been polymorphic malware.
- 79% of the malicious code detected in organizations was directed at Windows, 18% to Linux and 3% to Mac systems.
- The first malware for the Unified Extensible Firmware Interface (UEFI) has been discovered.
- Most mobile malicious code was hosted in third party application stores and the application categories for this mobile malware were mainly Lifestyle (27 %) and Music&Audio (20 %).
- The pre-installed malware trend has been maintained.
- Remote access Trojans are still increasing. FlawedAmmyy is the first RAT to appear on the list of the top ten most important malware[15].
- Endpoints are increasing as threat targets, probably due to the diffuse perimeter of organizations and the use of mobile devices[16].

Frequency of malware vectors

Traffic Types

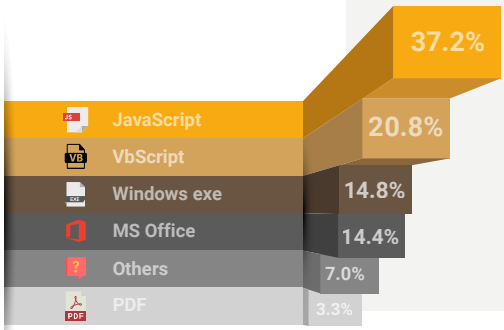




Evolution of malicious code in recent years (Source AV-Test)

Frequency of malware file types

File Types

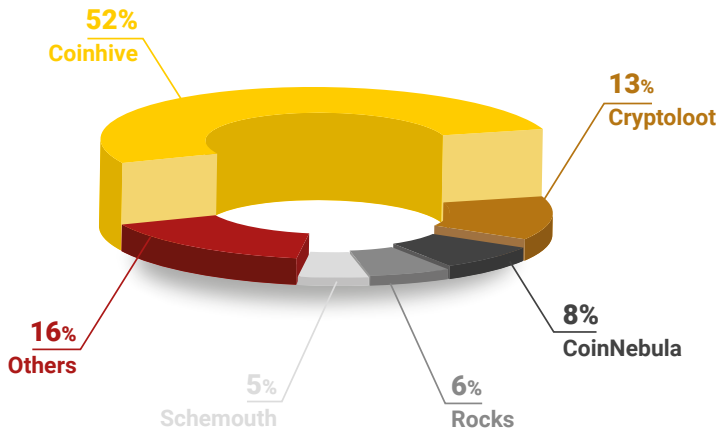


Although malicious code remains the most common cyberthreat[17], it has been seen that States have increased the use of legitimate software and bona fide providers to access specific victims, making it difficult to prevent and detect such attacks.

[15]See: https://www.zdnet.com/article/this-remote-access-trojan-just-popped-up-on-malwares-most-wanted-list/
[16]See: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
[17]See: ENISA: Threat Landscape Report 2017 (at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017)

5.9.Cryptojacking

Cybercriminals are increasingly trying to make a profit through cryptojacking, i.e. using the computing power of third-party computer systems for cryptocurrency mining. This comes down to direct monetization based on the generation of crypto coins. The cryptominer trend follows closely the flow of money and the valuation of market prices of crypto coins[18].

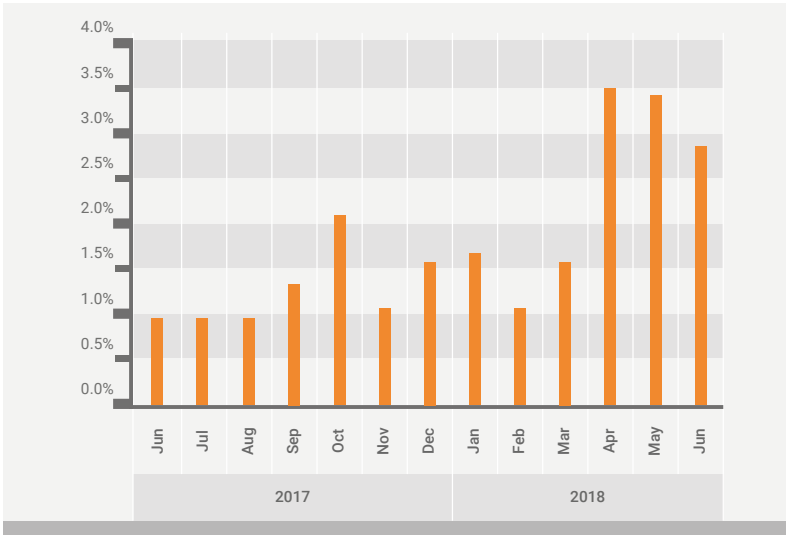


Top Global Malware Crypto Coins

In addition to traditional computer systems, IoT devices and mobile devices are also used to extract crypto coins.

In addition to traditional computer systems, IoT devices and mobile devices are also used to extract crypto coins[19].

Although it is too early to say, we may be witnessing a transition from traditional ransomware to cryptographic malware. A general worrying trend for critical infrastructure has also been observed, as it could have an impact on the stability and responsiveness of the operations of such systems. Percentage of ICS systems attacked by cryptocurrency mining[20].

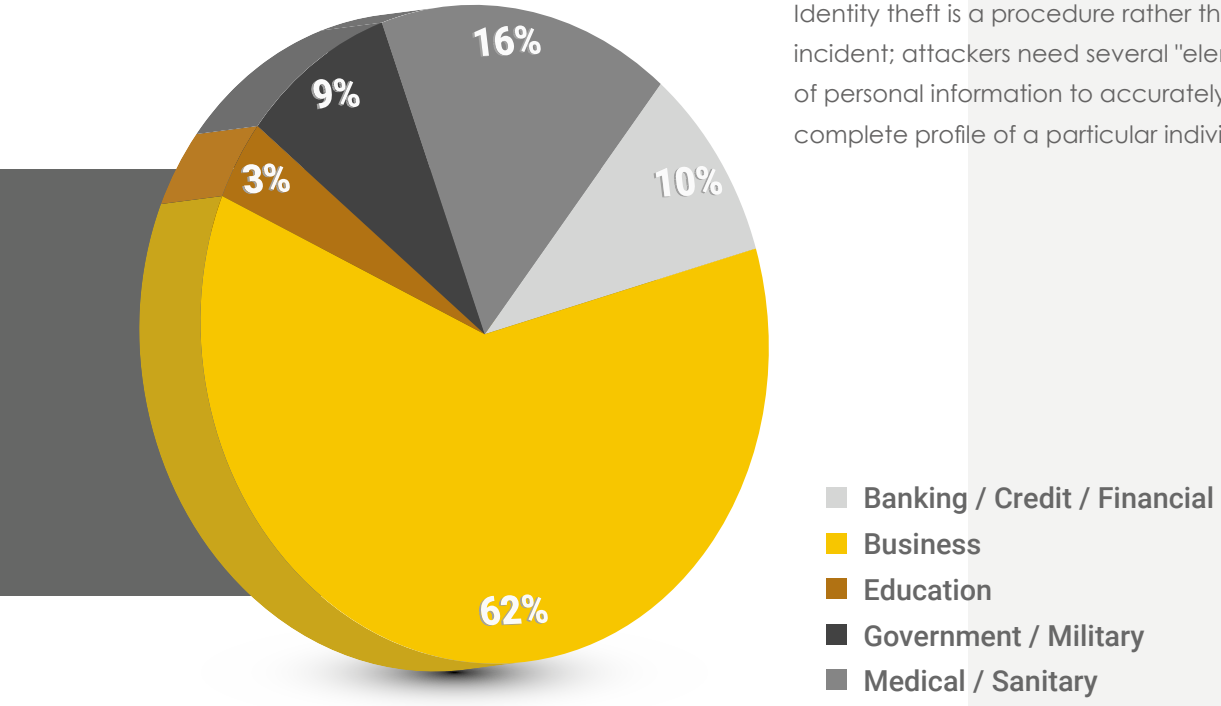


Percentage of ICS systems attacked by cryptomining

[18]See: https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf
[19]See: Avast: Cybercriminals could build cryptomining armies using vulnerable IoT devices at Mobile World Congress 2018 (en https://press.avast.com/cybercriminals-could-build-cryptomining-armies-using-vulnerable-iot-devices-at-mobile-world-congress-2018)
[20]See: https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/

5.10.Identity Theft

Identity theft is a procedure rather than an isolated incident; attackers need several "elements" or "pieces" of personal information to accurately "construct" the complete profile of a particular individual.



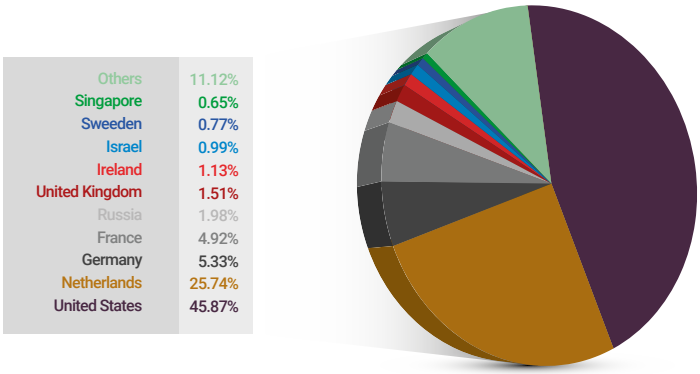
Number of records compromised during 2018 in different sectors (Source: Idtheftcenter)

5.11.Web Attacks

This type of attack focuses on web systems and services to engage the victim, including exploitation of browsers, web sites, exploitation of the content management system (CMS) and web services themselves. Drive-by, waterhole, redirection and man-in-the-browser attacks are some of the best-known categories of such actions. During 2018, web-based attacks continued to be one of the most important threats as they were very widespread. This is some of the most significant evidence from 2018:

- APT, malicious code campaigns and watering hole attacks.
- Extensions for browsers.
- Greater commitments related to content management systems (CMS): In early 2018, several attacks were observed against Drupal delivering crypto-miners and social engineering tools[21]. Later, in September 2018, there was a wave of attacks targeting vulnerable Wordpress sites[22].
- The trend towards exploits based on web browser (drive-by) continues.

[21]See: https://blog.malwarebytes.com/threat-analysis/2018/09/mass-wordpress-compromises-tech-support-scams/
[22]See: https://labs.sucuri.net/?note=2018-09-18



Distribution of web-based attacks by country in the second quarter of 2018. Source: (Securelist)

Attacks on web applications

Attack frequency has decreased slightly. However, the so-called "automated attacks", which show more efficient exploitation capabilities, remain very dangerous vectors.

The most significant issues of this type of attack are:

- ***SQL injection*** continues to lead this type of attack: they continue to be the majority in this type of action (51%) despite being the best-known variant for both attackers and victims.
- Inclusion of local files and **cross-site-scripting** are the second and third most frequent attacks: 34% and 8%, respectively.
- **Dead codes**, also known as orphaned routes/APIs, are obsolete or abandoned portions of web applications, which unjustifiably increase the attack surface on interconnected systems[23].
- There has been no significant increase in vulnerabilities in the financial sector, retail trade and health care[24].
- Attacks on **legacy applications** are still top of the list.

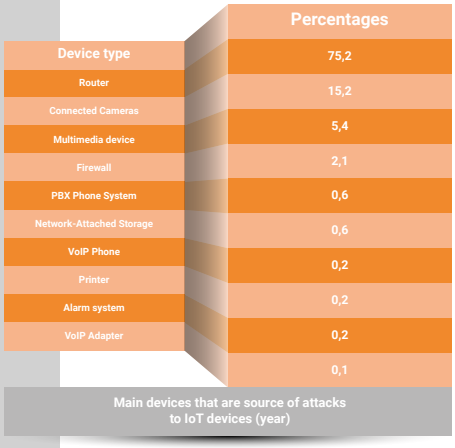
5.12.Botnets, IoT, Iot botnets and Android

The threat from botnets remains high, and while attackers initially focused on traditional computer systems, the attack surface has been expanded to mobile devices and IoT devices. During 2018, botnets were mainly used for information theft, denial of service (DDoS) attacks, and sending spam with malicious code. The most significant aspect has been the increase in the appearance of botnets that compromise home electronic devices connected to the Internet, using them as bots. It should also be noted that approximately 25% of botnets point to Android systems, while the remaining infections are predominantly on Windows systems.

On 5th December 2017, nearly 1.5 million infections were detected worldwide in a single day. By mid-2018, there was a clear drop of 42%.

Routers and connected cameras are the main source of attacks, amassing 90% of the harmful activity.

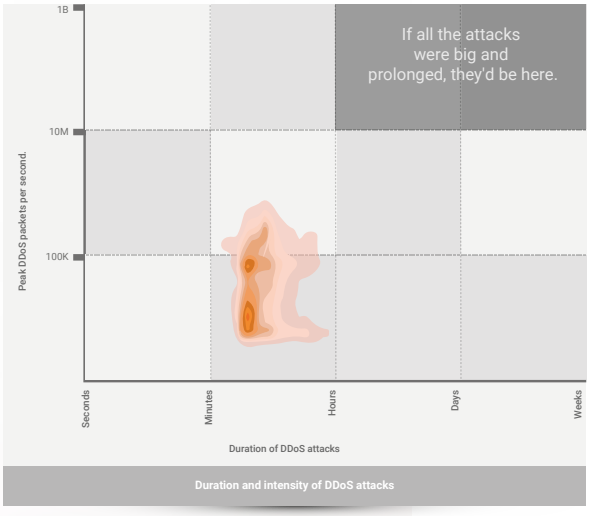
[23]See: https://info.tcell.io/hubfs/DemandGen_Content/Research%20Papers/tCell_wp-stateofsecurity-2018-web.pdf
[24]See: https://info.whitehatsec.com/rs/675-YBI-674/images/WhiteHatStatsReport2018.pdf



5.13.DDoS Attacks

The number of DDoS attacks continues to increase, namely by around 16%.

- **Connected Services Internet:** Several researches indicate that APIs are becoming a very popular attack surface among threat agents. Hostile action against such technologies would make it possible to disrupt services in different organizations, even in specific sectors, such as health.
- **DDoS and geopolitical attacks:** DDoS attacks have arisen, directed against authorities or political candidates from different countries.
- **DDoS attacks as a service:** The cost for these providers to run simple DDoS attacks is around five dollars. Its cost can vary according to the different capacities offered: parallel attacks, limits per day and multiple attack vectors. In 2018, the UK National Crime Agency, together with the Dutch National High-Tech Crime Unit, dismantled a major DDoS platform known as "webstresser.org" that had been used to launch between four and six million attacks worldwide[25].
- **Multivector DDoS Attacks:** Akamai reported a series of specific attacks targeting DNS servers for nearly 2 days, intermittently, which also included another vector (based on PSH / ACK - TCP) with a peak of 120 Gbps (18.6Mpps). In addition, a malicious actor introduced a set of traffic generators into a YouTube tutorial that could reach a maximum of 170 Gbps (65Mpps). Other multivector attacks that misuse the IKE and IPMI protocols support theories that the Mira" code continues to be used[26].
- **IOT and DDoS attacks:** The first quarter of 2018 saw an increase in the number and duration of detected DDoS attacks.



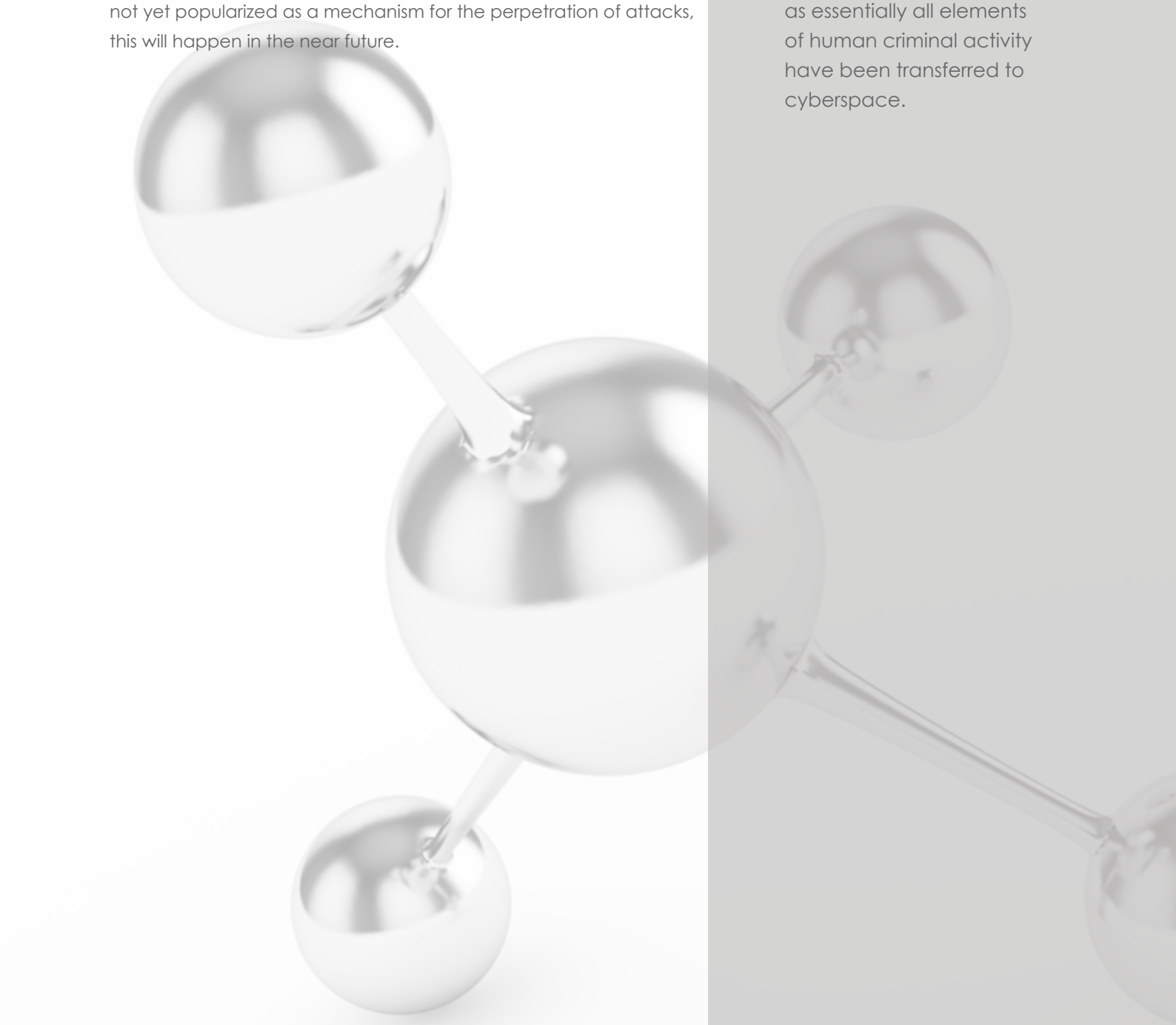
[25]See: https://securitybrief.com.au/story/it-s-an-active-buyer-s-market-for-ddos-as-a-service-netscout y https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf
[26]See: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf

5.14.Cryptography

Aspects that can cause a cryptographic system to fail are:

- Security holes in the hardware (e.g. Spectre and Meltdown).
- Errors in implementations.
- Protocol-level errors.
- Use of obsolete standards (for example, ROBOT).
- Weaknesses in password generation (for example, ROCA).
- Inadequate random number generators.

Side channel attacks, which involve physical implementation of a system or device, have led to developing Machine Learning (ML) techniques to recognize patterns in data measurement. Although not yet popularized as a mechanism for the perpetration of attacks, this will happen in the near future.



The economic impact of cyberattacks

According to McAfee estimations, cybercrime would represent a global cost of nearly $600 billion (or 0.8% of global GDP). However, criminal activity on the Internet is much broader than economic cybercrime, as essentially all elements of human criminal activity have been transferred to cyberspace.

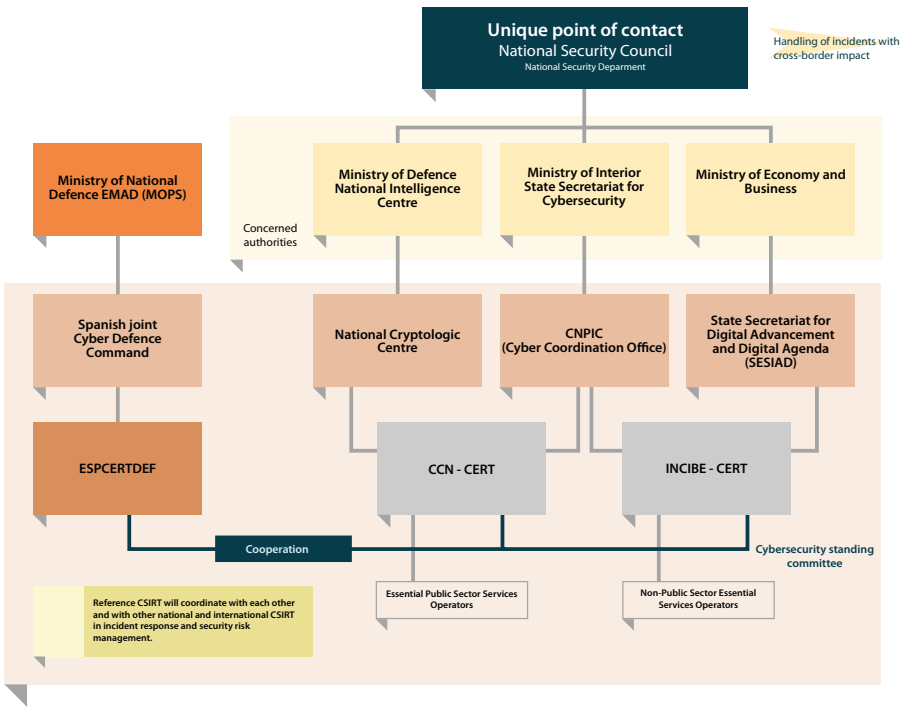
6 Measurements

This section describes the main measures taken during the period under review to prevent attacks or mitigate their effects.

6.1.Strategic and legal framework

2018 has witnessed the development and/or entry into force of several European and national legal initiatives on issues related to cybersecurity,

- **National Cybersecurity Strategy**. In 2018, work began on updating the 2013 National Cybersecurity Strategy (it was finally published in the Official State Gazette on 30th April 2019).
- Full application of **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016** on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- **Royal Decree-Law 12/2018, of 7 September, on the security of networks and information systems**, in compliance with the mandate to transpose Directive (EU) 2016/1148 of the **European Parliament and of the Council, of 6th July 2016**, establishing that the CCN-CERT shall act as the reference incident response team for the public sector and as the national coordinator of the technical response in cases of special gravity and requiring a higher level of coordination.



The Development Regulation for this Royal Decree-Law is being developed at the time of writing this report.

Resolution of April 13rd 2018, of the Secretary of State for Public Function, approving the **Technical Instruction on Security for Notification of Security Incidents**, which establishes the criteria and procedures for notification by the Public Sector to the National Cryptologic Centre (CCN) of those incidents that have a significant impact on the security of the information they handle and the services they provide.

Cybersecurity Act

Proposed in 2017, it includes a comprehensive set of measures to tackle cyberattacks and build robust cybersecurity in the European Union. It also includes a permanent mandate for the EU Cybersecurity Agency, ENISA, and a stronger foundation in the new cybersecurity certification framework to help Member States respond effectively to cyberattacks with a greater role in cooperation and coordination at UE level.

Furthermore, it creates a framework for European cybersecurity certificates for products, processes and services that will be valid throughout the EU. This rule is currently under discussion by Parliament and the Council

.

Organic Law 3/2018, dated 5th December, on the Protection of Personal Data and the guarantee of digital rights

It reinforces legal certainty and transparency while allowing its rules to be specified or restricted by the law of the Member States, as far as this is necessary for reasons of consistency and for the national provisions to be comprehensible to the addressees.

Proposal for a Regulation to pool resources and expertise in cybersecurity technologies[27]

in the European Commission, which is considering setting up a Network of Cybersecurity Competence Centers to better channel and coordinate available funding for cooperation, research and innovation in this area.

Access to electronic evidence

In April 2018, the EC proposed two rules to make it easier for law enforcement and judicial authorities to obtain the electronic evidence needed to investigate and prosecute individualized criminals and terrorist organizations. Such rules are a regulation for cross-border access to electronic evidence (e-evidence) and a directive complementing it with the aim of harmonizing the appointment of legal representatives of online companies[28].

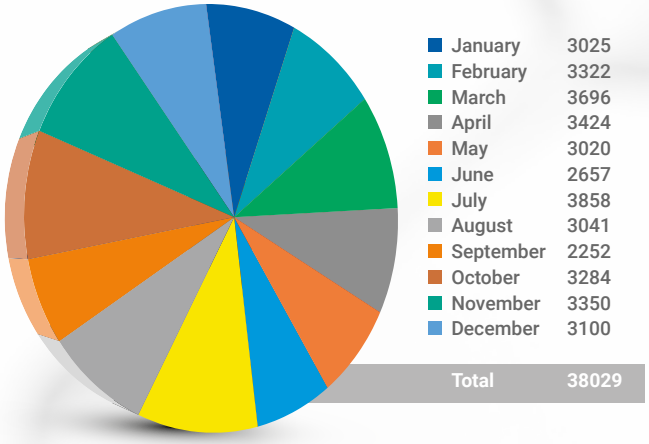
National Security Framework Certification Council (CoCENS)

The National Security Framework Certification Council (CoCENS) has been set up and it is made up of representatives from all the parties involved: the National Accreditation Entity (ENAC), the Ministry of Finance and Public Function, the Spanish Data Protection Agency, the National Cryptology Centre and all the public and private ENS Certification Entities. Its objective is to assist proper implementation of the National Security Framework and, consequently, provide the most reliable public services.

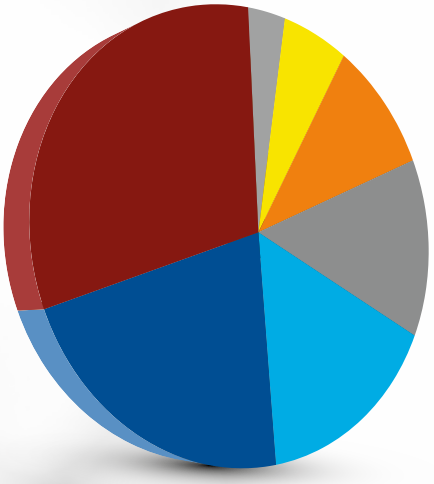
[27]Proposal for a "Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", COM (2018) 630, dated 12th September.
[28]Proposal for the "Regulation on European Production and Preservation Orders for electronic evidence in criminal matters", COM (2018) 225, dated 17th April, and proposal for a "Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226, dated 17th April.

6.2.Work of the National Cryptologic Centre (CCN)

In 2018, the CCN-CERT managed a total of 38,192 security incidents, an increase of 43.65% over 2017.

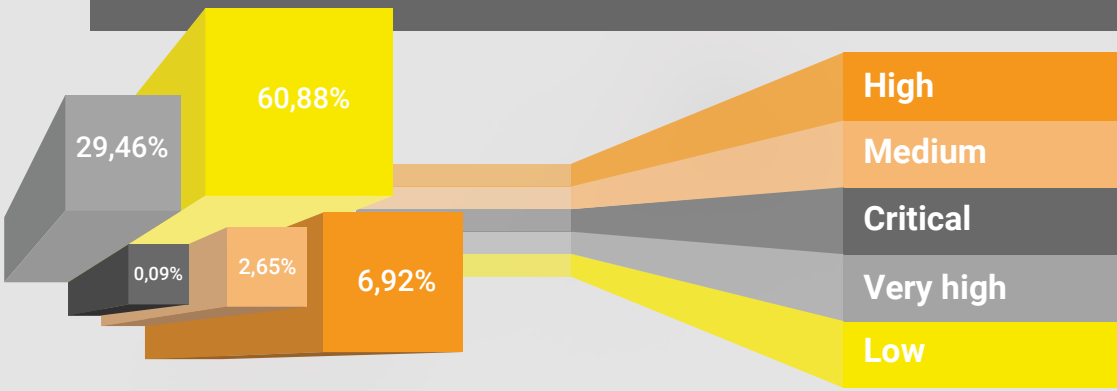


Number of incidents managed by the CCN-CERT in 2018

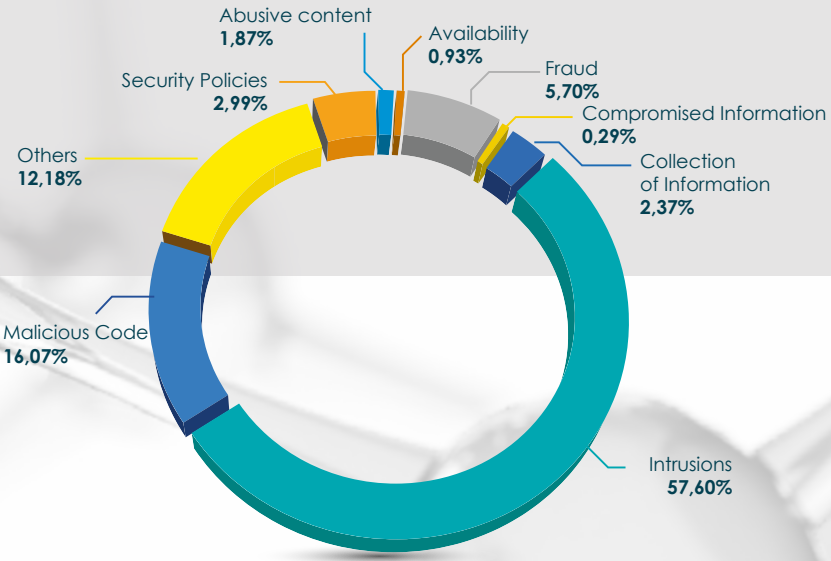


Number of incidents managed per year

2.7% of the incidents managed had a "Very High" or "Critical" danger level, i.e. the CCN-CERT had to deal with an average of 2.8 incidents of this type per day.



Dangerousness of incidents managed by the CCN-CERT in 2018



Typology of incidents managed by the CCN-CERT in 2018

The cyber incidents detected in this period have affected multiple sectors: Public Administration and, in general, Public Sector, Aeronautical Sector, Financial Institutions, Energy Sector, Health System, Air Transport and ICT Services and Infrastructures.

Outstanding Cyber incidents in 2018

It is worth highlighting attacks on the financial sector, with the aim of stealing money, which has earned attackers an estimated profit of more than 1,000 million dollars since 2014. In the **banking sector**, in March 2018, Carbanak-Cobalt cyberattacks were detected thanks to a security company and a foreign CERT working together.

The **CCN-CERT**, in turn, concentrated its work prior to the cash-out, which largely avoided even more serious consequences.

The aggression vector was spear-phishing, attacking unpatched vulnerabilities. The progress of the attacks on the victim's networks was less than two weeks to total control. The most notable aspect is that publicly available tools (Powershell and Cobalt Strike Beacon) were used, but not purpose-built tools.

In the **Aerospace sector**, in April 2018, attacks by the group known as **Emissary Panda** -whose presence has been maintained for more than two years, leaked more than 200 Gb of data from entities in that sector.

In this case, the attack vector was "abandoned" web servers, i.e. unpatched, located in the DMZ.

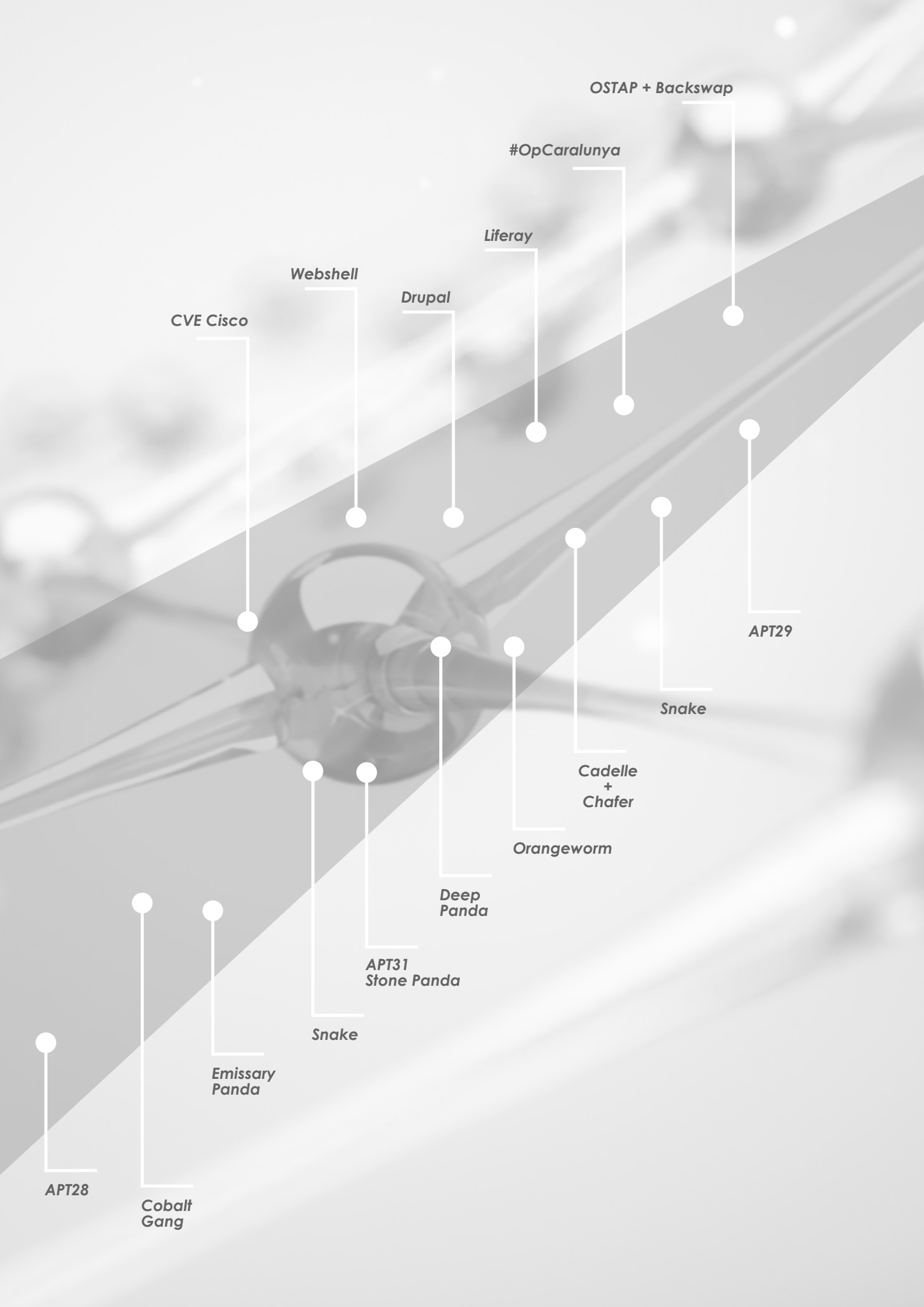
The most significant aspect of **Emissary Panda**'s cyber-attacks was the absence of malicious code: access was gained through webshells (China Chopper) and information theft via HTTP requests.

In the **Government sector** (Public Administrations), the main actor has continued to be APT29 which, in November 2018, launched a global campaign targeting approximately 3,000 victims.

The attack vector was the use of an OS functionality, which allowed malicious code to be installed and run.

Again, the attackers dispensed with specific materials, using Cobalt Strike Beacon, a tool available to the public.

Public Administrations
Aeronautical
Banking
Energy
Health
Air Transport
ICT


OSTAP + Backswap
#OpCaralunya
Liferay
Webshell
Drupal
CVE Cisco
APT29
Snake
Cadelle
+
Chafer
Orangeworm
Deep
Panda
APT31
Stone Panda
Snake
Emissary
Panda
APT28
Cobalt
Gang

The resources generated by the CCN-CERT

53 new CCN-STIC Guides

72 technical reports, 30 threat reports, 26 malicious code reports and 4 best practices reports.

A total of 22 face-to-face courses

7 on-line courses and 13 distance learning courses through VANESA. The first edition of the STIC Course on Security in Network Infrastructures and the STIC pilot course on Security Audits have been presented.

In terms of talent detection

the **ATENEA** Security Challenges Platform continued in 2018, hosting activity from more than 5,000 users and more than 70 security challenges; ATENEA ESCUELA joined in, incorporating more than 60 security challenges.

New solutions and versions

New solution for management and evolution of a subject's exposure levels.

</ana>

Development of version 7.2, a new set of threats. In 2019, the PILAR-Cloud project began, the aim of which is to have the latest version of this tool in the cloud, with a new user interface.

</pilar>

Development of version 2.0 of CLARA, facilitating its integration with ANA.

</clara>

It streamlines incident analysis through the new intelligence engine and new interface.

</reyes>

Finally,

the following table shows the results of the implementation of the analysis tools **MARTA**, **MARIA** and **CARMEN** (detection of commitments by APT).

</marta>

314
Total of binaries uploaded

1796
Total of analyses performed

</maria>

267
Total users

343
Total analysis
Pos. 167 / Neg. 182

70,81%
Best detection ratio

1,86%
Worst detection ratio

carmen
Ciberinteligencia Avanzada

54 Operational sites around the world

28 Implantations in organizations and companies

Integration with Reyes, Marta, Claudia and Panda

Full HTTP **headers** and PCAP file uploads

vSOC

The CCN is working on implementation and promotion of virtual Security Operations Centers (vSOC) in its community of reference, with the objective of improving skills for surveillance, detection and response to any possible attack, as well as optimizing their resources based on the information they manage and the services they provide.

Collaboration agreement with the Ministry of Justice

During 2018, the Ministry of Justice signed a collaboration agreement with the CNI-CCN to develop the Security Operations Centre of the Subdirectorate General for New Justice Technologies.

7 Trends

In 2019, state agents will continue to run intrusion campaigns as part of their national strategies and will certainly use their e-skills to do so.

Entities in government, defense, think tanks and NGOs will continue to be the primary targets of their operations. These intrusions are likely to be supported by suppliers in the telecommunications and technology sectors, and may include supply chain commitments, as has been observed in previous years.
Future cyberattacks are expected to increase in volume and sophistication. The following paragraphs outline what might be expected in the immediate future.

1. Increase State-sponsored cyberattacks

Internet-connected information systems are vital to most national economies and are therefore an obvious target in the event of conflict or controversy. There are many examples: from conventional cyberattacks to actions comprised of so-called hybrid threats. The next few years will see new actions of this kind.

2. Attacks on the supply chain

In 2019, supply chain attacks will increase as large corporations open up to greater risk as trust in their partners increases.

Because of these dangers, many third-party companies have created supplier risk management processes within their organizations. Teams managing these risks within organizations will become more common as supply chain attacks increase.

3. The cloud as a target

During 2018, there have been many incidents related to cloud computing and they are expected to continue and evolve in the coming years, because the cloud contains a lot of data and attackers follow the same steps.

4. Sophistication of harmful code

Threat agents are constantly refining their malicious code tools to make them more efficient. The use of advanced persistent threats (APT) will increase as attackers need to invest time and effort to carry out significant actions (e.g. cyber espionage).

5. Cyber-attacks aimed at people

Human beings remain the weak link in all security systems, so as the effectiveness of protection against malicious code increases, threat agents will change their target, attacking people. It might be expected, over the next few years, to see an increasing volume of phishing emails and fake websites designed to mislead users and facilitate access to sensitive data, such as passwords or credit card numbers.

6. Use of intelligent devices in cyberattacks

Devices connected to the Internet via Wi-Fi (professional, commercial or domestic) offer new ways for threat agents to penetrate internal networks, attacking connected devices, including computers, and generally for the purpose of stealing data or personal information.

7. Permanence of DDoS attacks and their relationship with IoT

DDoS attacks remain one of the preferred weapons of certain types of attackers. Overloading an unprotected website with excess traffic, using botnets, will continue to be a common scenario.

It is to be expected that more poorly protected IoT devices will be used for other harmful purposes. Among the most problematic, there are attacks against IoT devices that connect the digital and physical worlds. An increasing number of attacks on these devices that control critical infrastructure, such as power distribution and communications networks, are to be expected, and as home devices become more pervasive, future attempts by States to use them as a weapon are likely.

8. Increase of Cryptojacking

Using the appropriate malicious code, threat agents can take control of users' computers to "mine" coins, thereby preventing the full power of the machine from being used. This type of attack will increase and become more sophisticated in the future.

9. Malicious code will be more misleading

The next few years will see new malware variants that are more difficult to detect and could reside on infected systems for a very long period of time.

10. Automated learning to block new threats

The development of new types of malicious code continues at an incessant pace. Machine Learning tools, which monitor computer activity to automatically detect and block suspicious processes, even before malware has been officially identified, will become primary tools. This proactive protection will be vital in defeating cybercriminals, especially those who use malware with stealth techniques.

11. AI as a tool in cyberattacks

The fragility of some artificial intelligence technologies will become a growing concern in 2019. Somehow, the emergence of critical AI systems as targets will begin to reflect the sequence seen 20 years ago on the Internet, quickly attracting the attention of cybercriminals.

Reciprocally, defenders will increasingly rely on AI to counter attacks, identify vulnerabilities, and strengthen their systems against possible attacks. Over time, this security-oriented artificial intelligence could also improve our understanding of the trade-offs of providing personal information in exchange for use of an application or other additional benefit.

12. L5G Adoption Will Expand Attack Surface

In 2018, several implementations of 5G network infrastructure were initiated, and 2019 is expected to be a year of accelerated activity. Although it will take time for these networks, telephones and other devices to be widely deployed, growth will occur rapidly.

Although smartphones are the focus of interest for 5G technology, it is likely that the number of phones with this capacity will be limited during 2019 and 2020. However, over time, more IoT devices will connect directly to the 5G network rather than via Wi-Fi routers. This will make devices more vulnerable to direct attack. For home users, it will also make it more difficult to monitor all IoT devices.

Generally speaking, the ability to back up or easily transmit massive volumes of data to cloud-based storage will give attackers new targets.

13. Increased legislative and regulatory activity

Full implementation of the GDPR in the European Union is only one precursor to several security and privacy initiatives in countries outside Europe. For example, Canada has already implemented legislation similar to GDPR and Brazil has passed similar privacy legislation, which will come into force in 2020.

Attribution and responsibility are two of the most important aspects when it comes to defeating cyberattackers. With no risk or repercussions for harmful activity in cyberspace, threat agents will continue to attack.

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

centro criptológico nacional

IA-13/19