CCN-CERT
centro criptológico nacional

CYBER-THREATS AND TENDENCIES 2018 EDITION

CCN-CERT IA-09/18

EXECUTIVE SUMMARY

CONTENTS

PROLOGUE 1

This document is an extract from the **Threats and Trends Report. Edition 2018**, published for the tenth consecutive year by the National Cryptologic Center Computer Emergency Response Team **(CCN-CERT)**. It provides an analysis of national and international cyber threats, how they are developing and future trends. Much of the information gathered here is the result of experience at the National Governmental CERT which, in 2017, managed a total of 26,500 **cyber incidents**, 26.55% more than in 2016.

In its daily work, the National Cryptology Centre has been able to verify that state **players and professional criminals remain the most important threats**, while cyberwar, cyberconflicts and **hybrid warfare** are becoming increasingly present throughout the world, always supported by actions in cyberspace.

On the other hand, **the vulnerabilities of Internet of Things (IoT) devices**, everyday devices, have led to disruptive attacks that justify the need to improve digital resilience.

In addition, in 2017 we have seen how various cyber attacks have attempted to weaken democracies, interfering with their electoral processes and fuelling their internal conflicts.

In order to address current risks, the parent document and this executive summary analyse the **main cyber incidents of 2017**; the **attack methods** chosen by the **threat agents** against their victims; the multiple **vulnerabilities** that facilitate this situation; and the **main measures** to be taken into account in order to improve security.

Similarly, and taking into account the evolution of cyber incidents in the period under consideration, some **trends** are addressed for the coming months in which cyber attacks are expected to increase their degree of sophistication, virulence and boldness.

The Threats and Trends Report. Edition 2018 has been drawn up to be useful for ICT security managers in Spanish public entities, organisations of strategic interest and, in general, professionals and citizens of our country.

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.07.05 10:49:01 +02'00'

2 CYBER INCIDENTS

The following sections discuss the most significant cyber incidents of 2017, grouped by the motivation behind the threats.

CYBERCONFLICTS

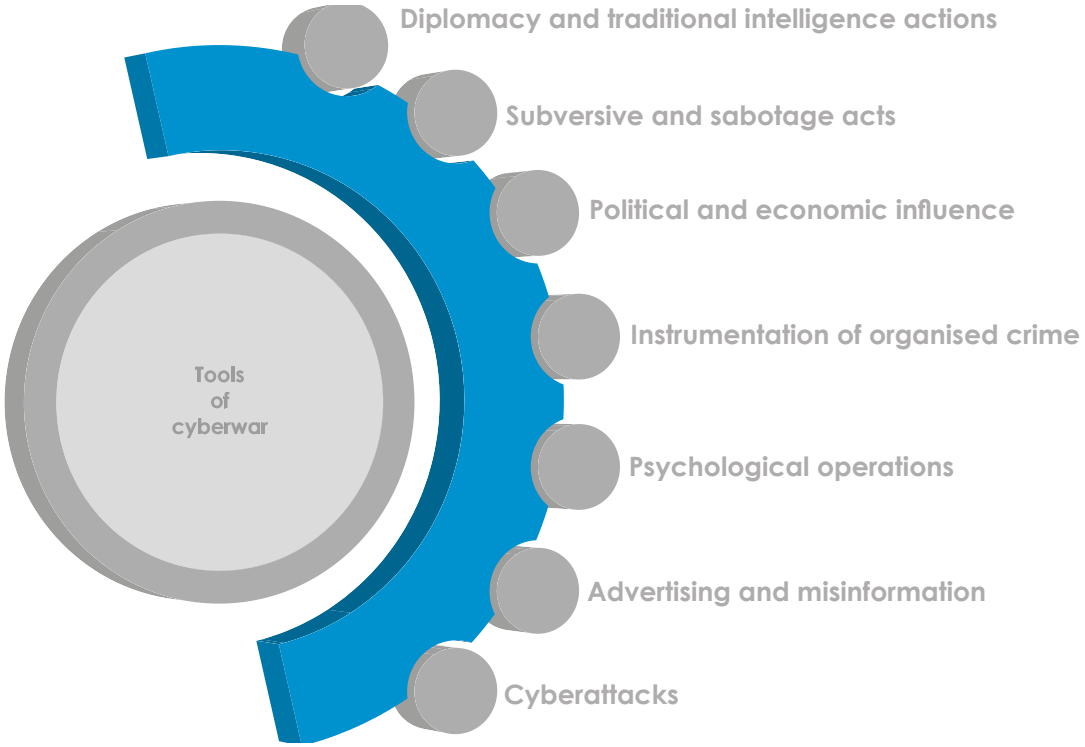
Digital theft, publication of information or interfering with the media or social networks have been used strategically by state players to **destabilise others and polarise the civilian population**. These attacks have been carried out under the cover of electoral processes or conflict situations.

The **victims** of this type of operation have mainly been **institutions and political parties** from various countries, including Spain.

INFLUENCING ACTIVITIES

These activities were based on extracting information on political parties and their members to influence democratic processes.

The German political party, the Democratic Union Christian (CDU); the En Marche! movement started by the French President Emmanuel Macron; and the Republican and Democratic Parties of the United States were victims of such cyberattacks in 2017.



CYBERESPIONAGE

During 2017, this problem affected all the countries in our western world. Cyberespionage represents a threat from attackers attempting to obtain **sensitive information** from both Spanish and Western companies and institutions.

SYSTEM DISRUPTION

The novelty in this type of attack lies in the use of **Internet of Things (IoT) devices** by end users to perpetrate significant DDoS[1] attacks. This was the case of the Mirai botnet or the LizardStresser botnet, which infected tens of thousands of consumer devices.

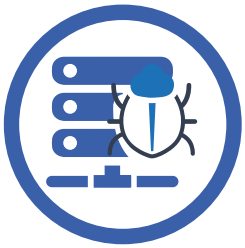
Similarly, Saudi Arabia's power grids, as well as certain government agencies, were also victims of cyberattacks in 2017, using the Shamoon malicious code.

FINANCIAL GAIN

Attacks were also carried out in 2017 in an attempt to obtain economic returns using a variety of methods.

CEO FRAUD

Criminals attempt to get a company's financial department to make financial transactions using domain names similar to the organisation in question.



MALWARE COBALT[2]

Sending emails to bank employees with a malicious attachment that allows access to the internal banking network and infects servers controlling ATMs.

CYBERPIRACY

In Italy, police arrested two individuals suspected of cyberpiracy in 2017 who were allegedly making investments on the basis of stolen information.

1. DDoS (Distributed Denial of Service): seeks to overload a server and thus prevent its legitimate users from using its services.
2. The leader of the cyber-crime group that uses the Cobalt malware (2016-2018) was arrested in Spain in March 2018. This malware was used to attack more than 100 financial institutions in over 40 countries, generating losses of one billion Euro.

3 THREAT ACTORS

This section will examine the threat actors who have intentionally developed or attempted to develop attacks. We will focus on their intentions, their capabilities and the changes that have been observed.

STATES

During 2017, government agencies from many countries all around the world, including Spain, were repeatedly victims of persistent large-scale cyberattacks, originating in other countries.

Western intelligence services have identified that **many countries are investing in building cyberdefence equipment** (essentially cyberwar or "hybrid warfare") intended to sabotage critical processes or aimed at influencing information operations.

States' methods of attack are becoming increasingly sophisticated and therefore more **difficult to detect**.

CYBER-CRIMINALS

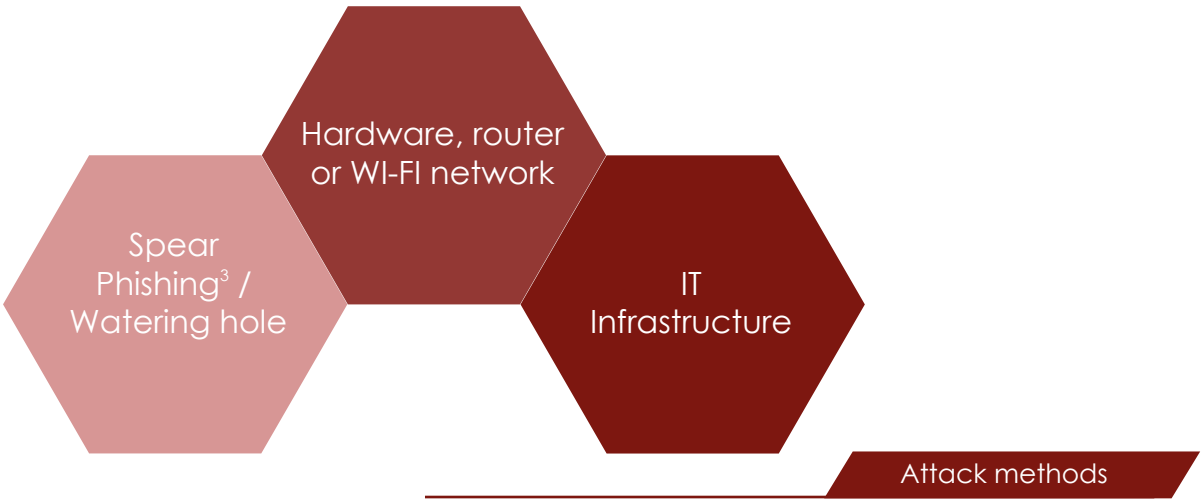
More often than in previous years, **cyber-criminals have targeted the systems of businesses, banks and other financial institutions** (so-called high-value targets), rather than just consumers.

In addition, in 2017, the **trend towards targeting specific organisations** (such as schools, hospitals or other health institutions) was confirmed, where the impact is greater than using untargeted attacks, i.e. without specific victims.

CYBER-TERRORISM AND CYBER-JIHADIST TERRORISM

Jihadist and terrorist groups are the main threat, although they do not yet appear to be able to develop sophisticated cyberattacks.

Their most obvious activities, for the purposes of propaganda, have been DDoS attacks and defacements[4].



3. Spear-phishing: targeted phishing that maximises the likelihood that the target will take the bait.
4. Deface or Defacement: Deformation or change caused intentionally on a legitimate web page through some kind of access to malicious code.

HACKTIVISM[5] IN CYBERSPACE

The threat posed by hacktivist groups, which generally carry out **cyber attacks for ideological reasons**, could grow in view of the increased availability of products, services and tools to develop attacks with a significant social impact.

CYBERVANDALS AND SCRIPT *KIDDIES*

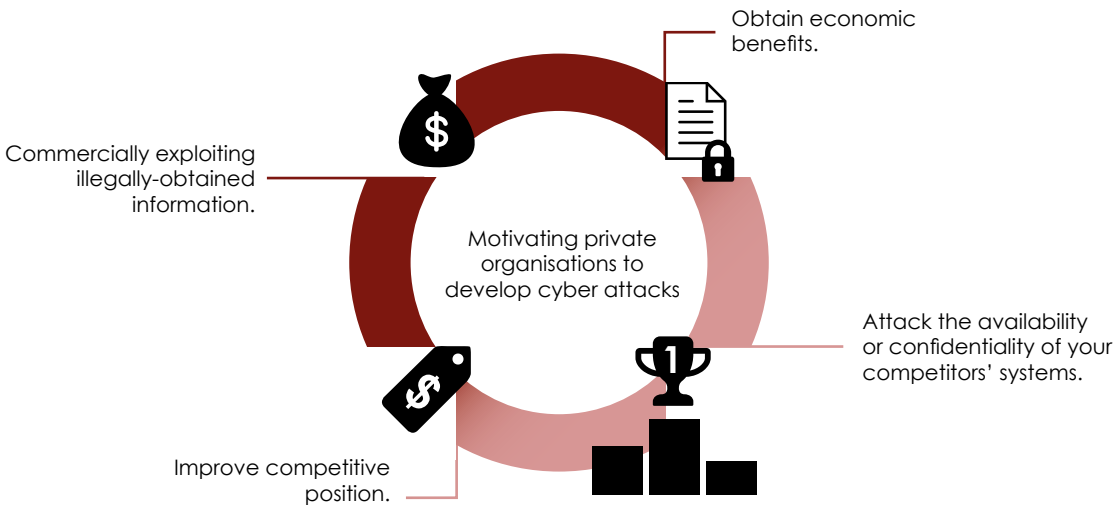
The public availability of tools to commit attacks has a special impact on the actions of these groups, who act merely to demonstrate their own capabilities.

INTERNAL ACTORS

These actions **have not changed substantially in 2017**. The perpetrated attacks were due to or the result of unconscious or careless behaviour.

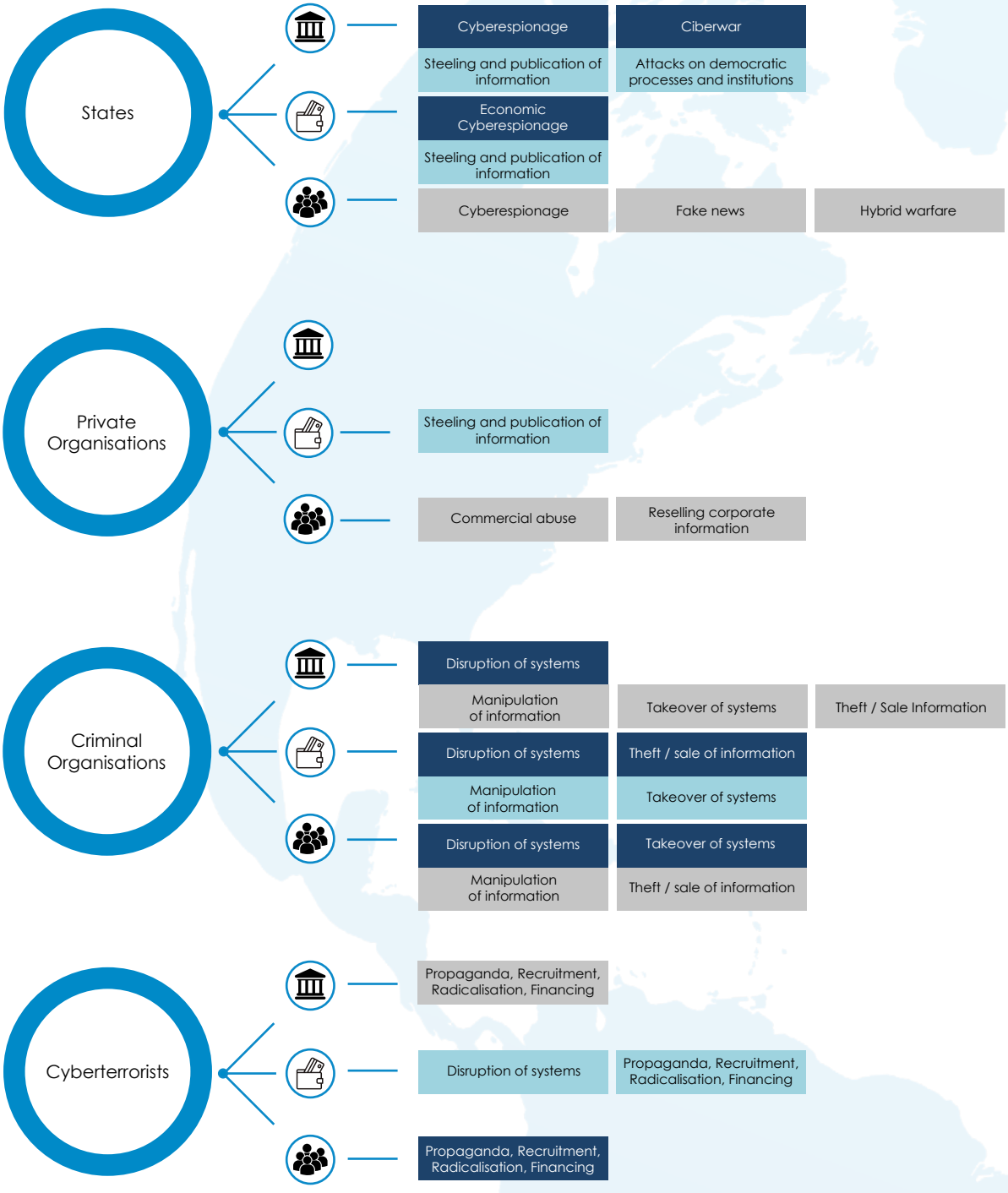
PRIVATE AGENCIES

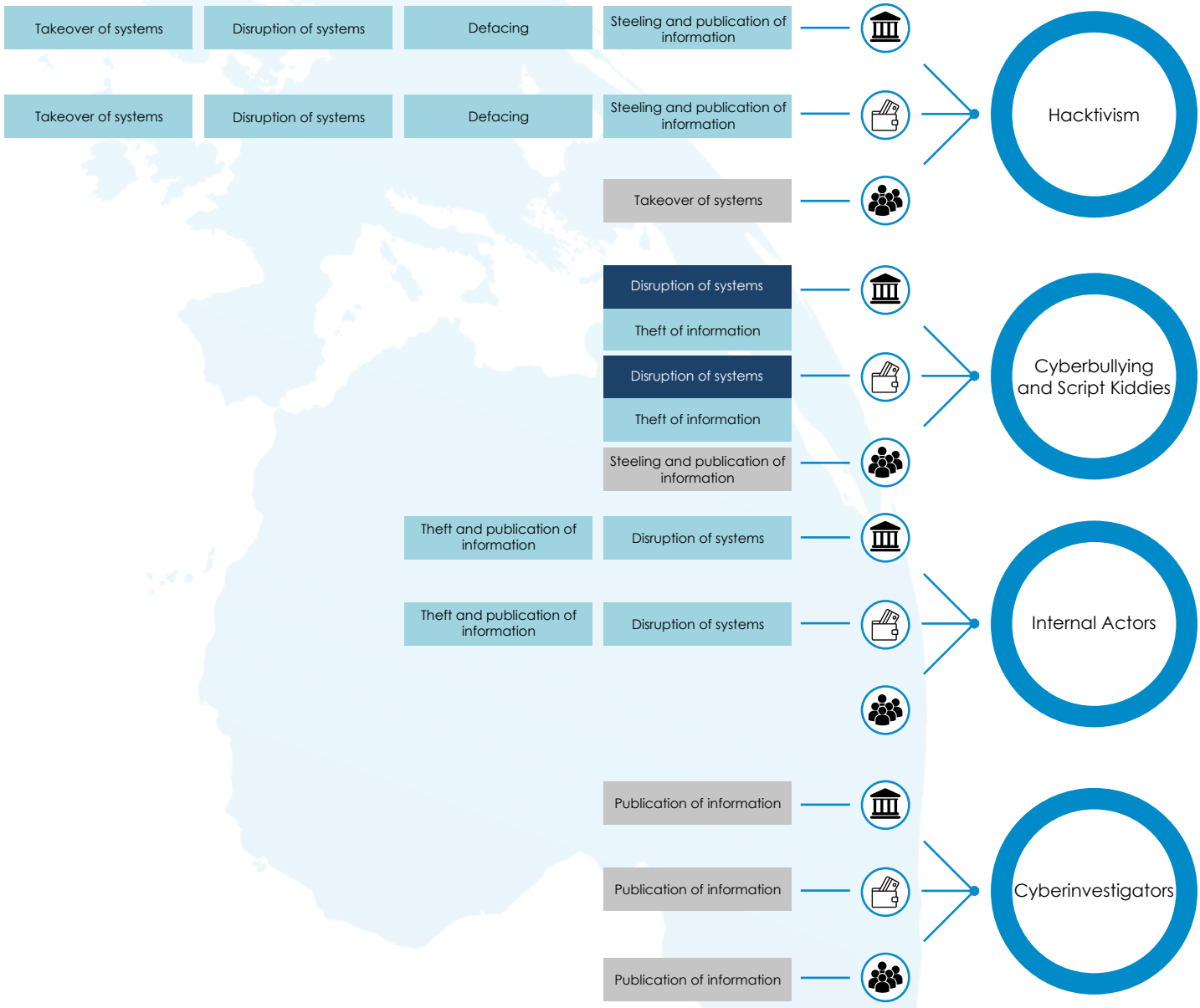
As shown in the graph below, there can be different characteristics and, correlatively, reasons for cyber attacks developed by private organisations.



5. Hacktivism or cyberactivism. Anti-social digital activism. Its practitioners aim to control computers or websites to advance their cause, defend their political position, or disrupt services, preventing or hindering legitimate use.

CYBER THREATS 2017





Legend

Threat Actors

Victim

- Public sector
- Private organization
- Citizens

Danger level of the threat

- No new threats have emerged
  There are enough measures in place to eliminate the threat
  There have been no significant incidents resulting from the threat
- New trends associated with the threat
  Limited measures to eliminate the threat
  The number of incidents has not been particularly significant
- Developments related to the threat
  The measures have a limited effect on the threat
  Significant number of incidents resulting from the threat

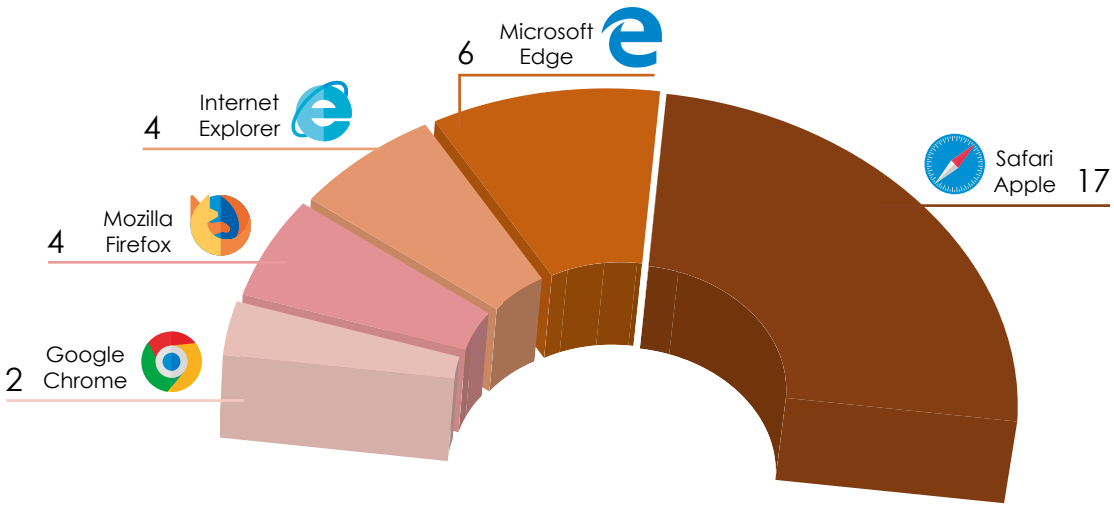
Source: Cyber Security Assessment Netherlands. CSAN 2017 and own elaboration.

4 VULNERABILITIES

This section details the most significant vulnerabilities in 2017.

BROWSERS AND WEB INFRASTRUCTURES

A recent Google Project Zero report shows that all known desktop browsers have associated **security vulnerabilities.**



In addition, a significant number of **websites have adopted CMS**[6] which makes them particularly tempting targets for attackers, as they have vulnerabilities resulting from the **use of *plugins***[7] or outdated extensions, such as WP Statistics (WordPress[8] plugin).

HARDWARE Y FIRMWARE[9]

Although there is **no known malicious code capable of exploiting these vulnerabilities**, its hardware architecture depth makes it very difficult to detect. One example of this is **Spectre**, a hardware vulnerability that would allow the attacker to obtain information stored in programs or processes.

Although the manufacturers involved have already responded to these vulnerabilities, **the effectiveness of security updates cannot be demonstrated immediately.**

6. CMS: Content Management System.
7. Plugin: an application that relates to another application to provide it with a new and, generally, very specific function.
8. Wordpress: content management system or CMS focused on the creation of any type of website.
9. Firmware: it works as the link between the instructions (software), which arrive at the device from the outside, and the various electronic parts (hardware).

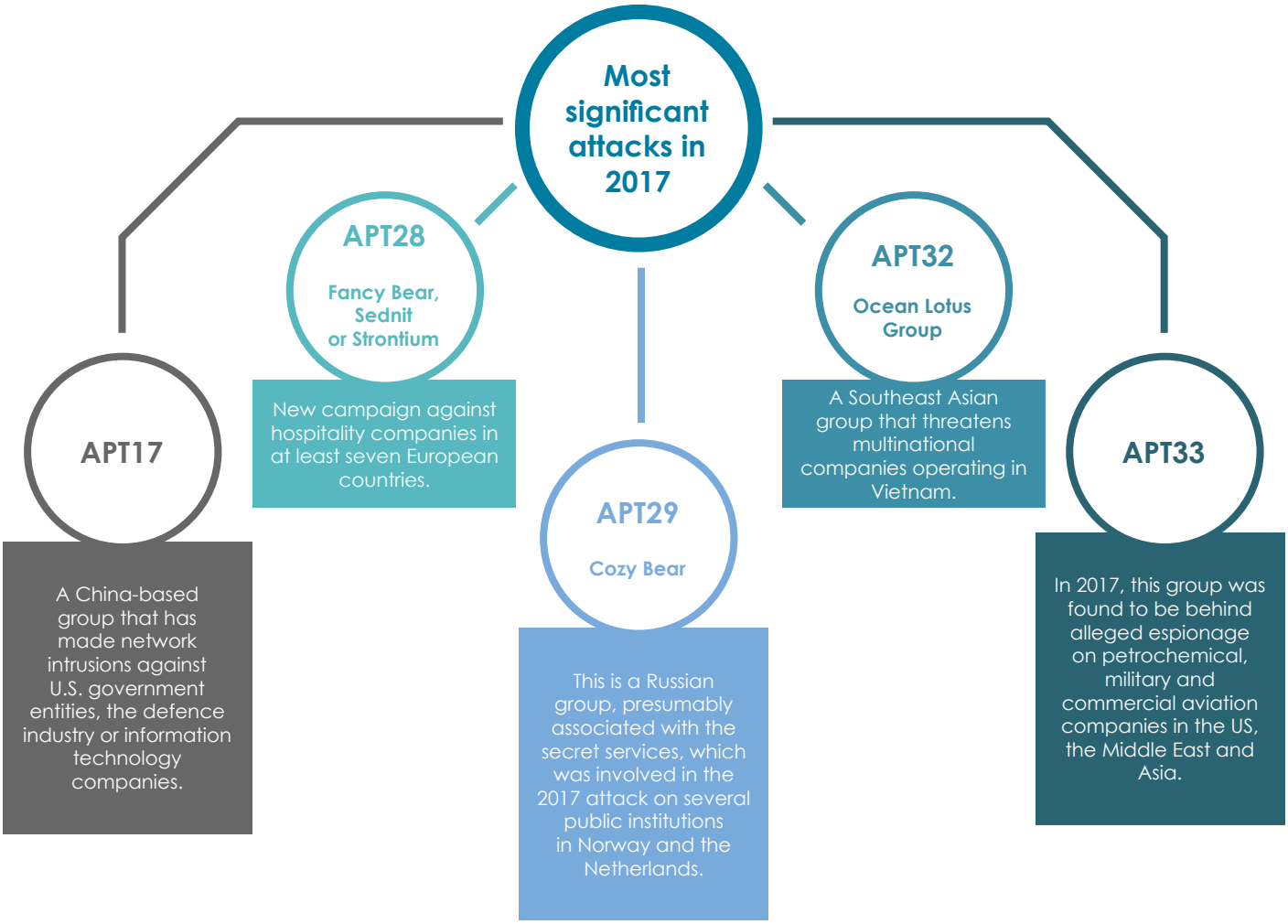
CYBER THREATS IN 2017

5

Techniques such as ransomware[10] or APTs[11] are still preferred by criminal groups and states, respectively. In any case, they are always looking for new and more effective methods. This section deals with these developments.

APT (ADVANCED PERSISTENT THREAT)

This targeted, **state-led cyber-espionage attack** uses various types of malware to steal intellectual property, trying to stay hidden for as long as possible.



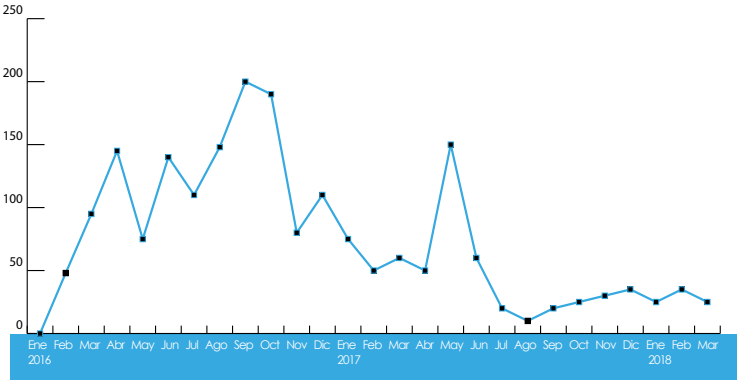
10. Ransomware: malicious code for data hijacking. Form of exploitation in which the attacker encrypts the victim's data and demands payment for the decryption key.
11. APT (Advanced Persistent Threat): This is a targeted cyberespionage or cybersabotage attack carried out under the auspices or direction of a state, for reasons beyond mere financial/criminal or political protest.

ATTACKS AGAINST THE ADVERTISING INDUSTRY

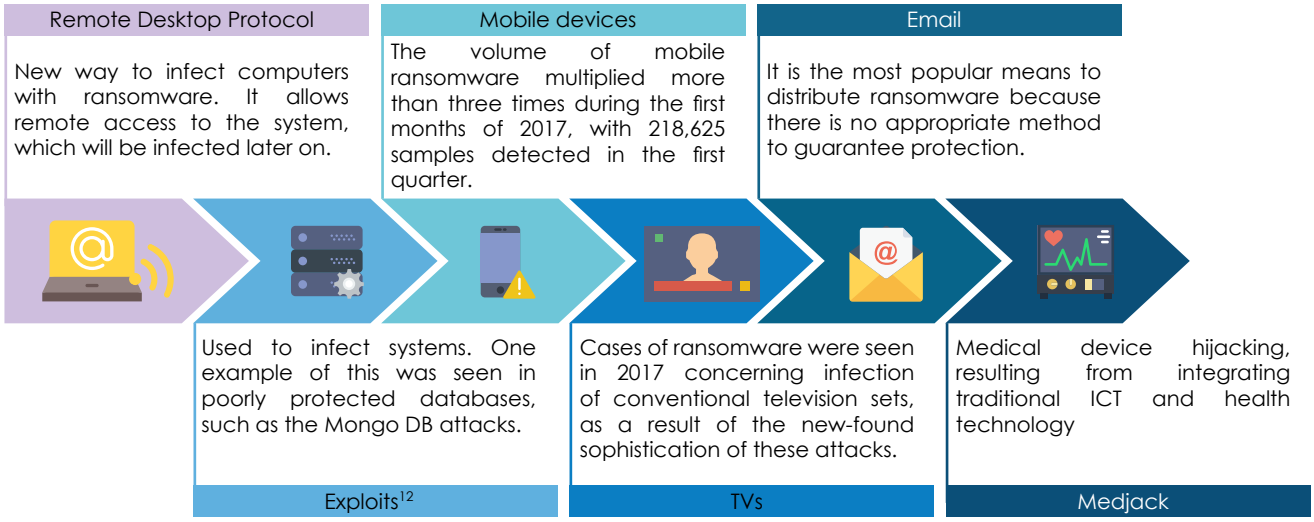
Infecting systems by **distributing malicious code through advertisements on websites** (known as "malvertising") appears to be on the rise. RiskIQ reported a **132% increase in the total number of malicious advertising cases worldwide**. According to PageFair figures, use of adblockers has increased by around 20% to combat these attacks.

RANSOMWARE

Although ransomware has become more sophisticated in recent years, there has been a **decline in the number of attacks**.



The following diagram shows some of **the methods of infection using ransomware** seen in 2017.



During 2017, evidence has been found that the health sector is the most frequently attacked area by this threat.

12. Exploit: A program that exploits or takes advantage of a vulnerability in a computer system for its own benefit. Exploit zero-day: exploiting a vulnerability immediately after it is discovered, benifitting from the time required by manufacturers to fix reported vulnerabilities.

PHISHING AND SPAMMING

In 2017, **phishing campaigns[13] increased in both volume and sophistication.** This method is the most successful infection vector for both targeted (cyberespionage) and unnamed (ransomware) attacks. At present, attacks are focusing on specific targets, thus it is becoming more targeted.

Spear phishing	A method adapted to the target that is used to attack a particular entity. It is difficult to determine how harmful it is since it generally uses a collection of all kinds of public information.
New attack method that hires cybercriminals and allows to obtain passwords from victims by simulating user service web pages such as Gmail, Facebook or Yahoo.	**Phishing as a service**
BEC / Whalling[14]	Spear-phishing attacks against top executives, usually with the intention of stealing money from their organisations or victims. It can also be used for cyberespionage.

Spam[15], on the other hand, has improved its quality, although the number of attacks using this type of messages seems to have decreased. However, it remains the primary means of **delivering unnamed malicious code** through harmful attachments and URLs.

INTERNET OF THINGS (IOT) - BOTNETS

The vulnerabilities of Internet of Things (IoT) devices, such as the **absence of encryption** in the few and non-existent **software updates**, have been especially exploited in 2017 to spy on their users or to manipulate their environment.

In this period of time, numerous devices such as routers, webcams or digital television receivers have been used to **carry out DDoS or ransomware attacks via botnets[17]**.

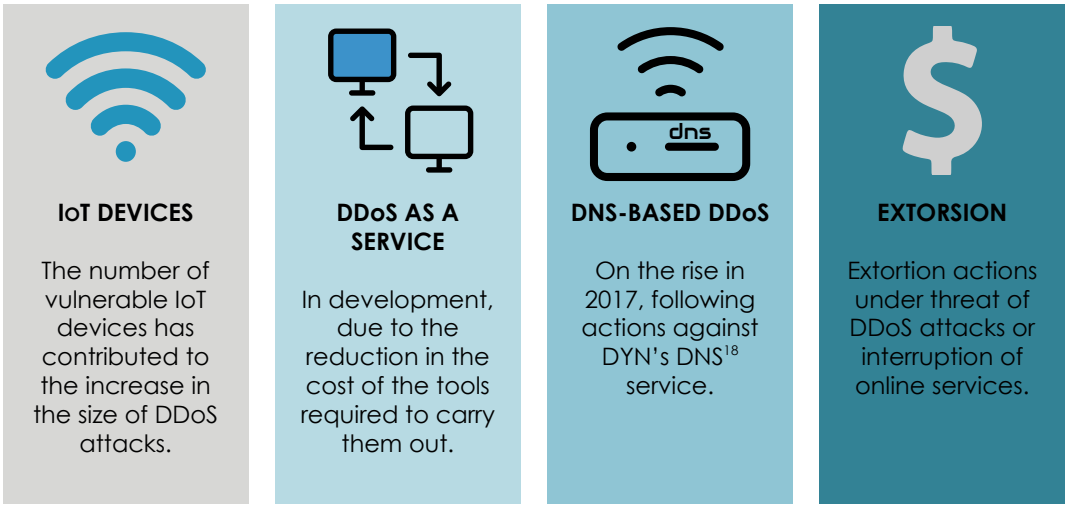
The possibility of perpetrating this type of action is often based on the public availability of attack tools.

13. Phishing: A method of attack that seeks to obtain personal or confidential information from users by deception or swindling. This approach impersonates a trusted entity in cyberspace.
14. Whaling: "whaling or big fish fishing", referring to the highest executive officers of the organisation.
15. Spam: Spam that is sent randomly in batch processes.
16. URL (Uniform Resource Locator): Text documents, photographs, audio and more types of digital content, have a URL when they are published on the Internet and are used to locate them.
17. Botnet: Infected computers´ network by a remote attacker. Equipment is at its mercy when you want to launch an attack such as sending spam or distributed denial service.

DENIAL OF SERVICE ATTACKS (DDoS)

According to the Kaspersky study, **33% of organisations faced a DDoS attack in 2017**, 16% more companies than in 2016. This data shows that these attacks, in addition to having increased in number compared to the previous year, have also increased in size (at the end of 2017, the Mirai botnet formed the largest DDoS attack in history by bandwidth, more than 1 Tbps).

TYPE OF ATTACKS

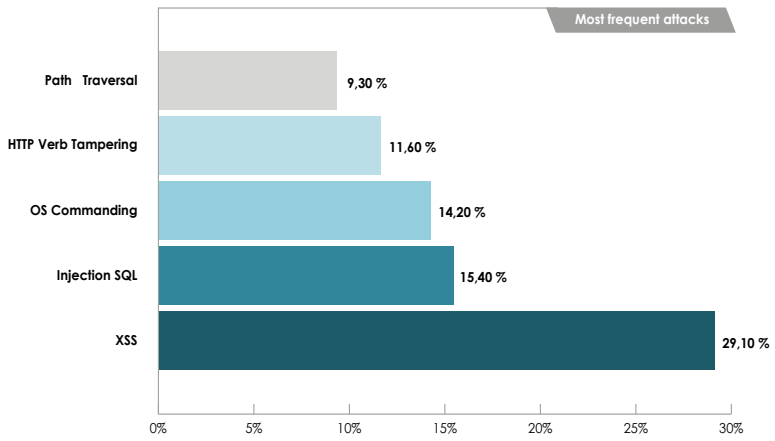


WEB ATTACKS

40% of web attacks are aimed at **obtaining information**, with web applications sponsored by the public and financial sectors reporting the highest number of attacks in 2017.

The most significant aggression vectors during 2017 were, according to Positive Technologies, Cross Site Scripting (XSS) and SQL injection.

In addition, web-based attacks, which make use of their enabled systems and services, have been one of the most significant threats in 2017 and will continue in the coming years.



Data from the fourth quarter of 2017
Source: Positive Technologies

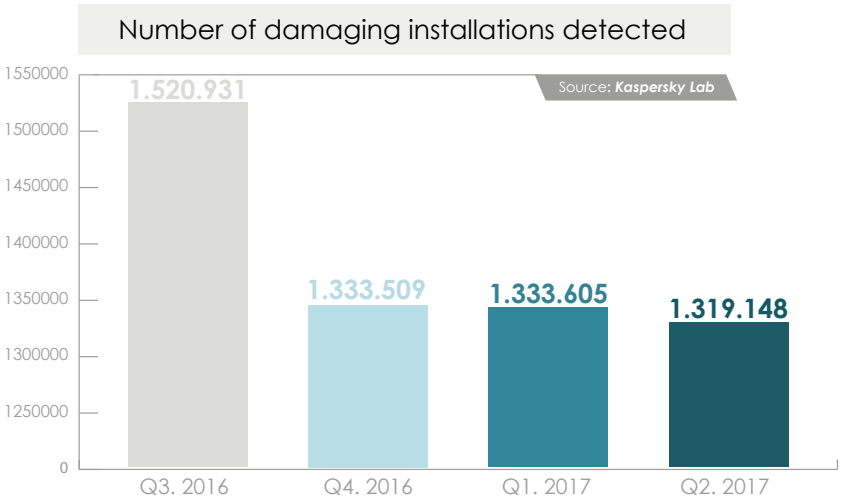
18. DNS (Domain Name System): is a system that names all connected computers, services or resources by giving them an IP address.

MALWARE

In 2017, malware continued to evolve in terms of sophistication and diversity, although a slight decrease in terms of frequency can be seen.

Mobile devices

Despite having declined in absolute numbers, malware for mobile devices has become more sophisticated.



FINANCIAL SECTOR

Attacks on these entities ranged from ***spear-phishing* emails or ATM malware** to ***watering hole*** attacks (attacks of this type attempted to infect more than 100 organisations in 31 different countries in 2017).

EXPLOIT-KITS

Although the number of exploit-kits[19] fell significantly in 2017, some of the most significant malware campaigns used this type of attack to compromise their objectives.

Leaks of tools and exploits have also shaped 2017. Leaking certain malware (the original development of which was attributed to state actors) led to the ***WannaCry* and NotPetya attacks.**

19. Exploit- kits: a set of automatic attack tools that exploit one or more vulnerabilities.

6 PROTECTION MEASURES

This section describes the most significant cyber incidents in 2017, grouped by the threat actors motivation.

MEASURES TARGETED AT INDIVIDUALS

Internet browsers are implementing measures to keep users better informed. For example, Google Chrome and Mozilla Firefox have announced that **all websites that do not use HTTPS protocol have been marked as insecure**; this could encourage website owners to implement the protocol for their own security.

In this sense, the **CCN-CERT has run a campaign to promote implementation of the HTTPS** protocol in public sector virtual branch, providing these organisations with a customised report on the HTTPS analysis and a document of recommendations for own implementation.

Another measure to protect individuals from being misled involves using **domain-validated certificates.**

MEASURES TARGETED AT ORGANISATIONS

Supplier security

Even though big organisations are generally capable of organising and managing your safety by following specific policies, procedures and measures; they often use suppliers with lower maturity levels.

In the Netherlands, in February 2017, digital transfer of results was banned due to the potential vulnerability in the software supporting the final count at the polling stations.

Attacks by Ransomware and DDoS

Large organisations often succeed in ransomware or DDoS attacks by investing in mitigation processes and tools. However, protection against large-scale attacks, such as the Miraies botnet, is always difficult.

When such actions affect smaller organisations, they often lack the expertise and financial means to invest in mitigating DDoS attacks or ransomware infections.

MEASURES TARGETING TECHNOLOGY

SMS MESSAGES

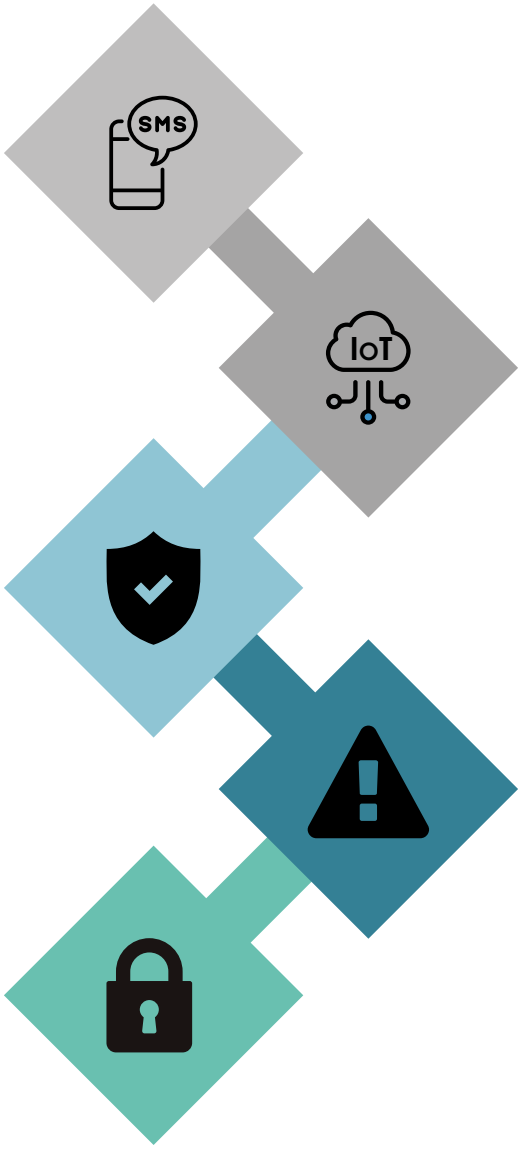
Android and iOS devices are susceptible to cyber attacks that allow access to text messages received from the recipient's computer. Therefore, using text messages represents a threat to two-factor authentication.

PRODUCT SAFETY

In 2017, the CCN published a Catalogue of ICT Security Products listing products that have been awarded certificates recommended for systems requiring high security levels.

THE NEED FOR ENCRYPTION

European states, such as the Netherlands, have made the use of HTTPS mandatory on government websites. In addition, this need has been extended to instant messaging applications, such as Telegram or WhatsApp, which already use end-to-end encryption.



THE INTERNET OF THINGS

There is still no clear solution for the Internet of Things's side effects. Lack of ICT sustainability will remain a problem if the sector can regulate itself.

KEY VULNERABILITIES

In 2017, different studies have been published related to exploitation of vulnerabilities linked to the software, such as Dedup Est Machina, that exploits memory duplication to take control of a browser.

STRATEGIC AND LEGAL FRAMEWORK

In 2018, two new **Technical Safety Instructions** were published in **Spain**:

- Resolution of 27 March 2018, from the Secretary of State for the Civil Service, approving the Technical Instruction on **Security Audits** for of the Security of Information Systems.

- Resolution of April 13, 2018, from the State Secretariat of Public Function, approving the Technical Instruction on Security for the **Notification of Security Incidents.**

Both come in **addition to the ITS in accordance with the National Security Framework (ENS)** and the previously published **Security Status Report**.

On the other hand, the transposition process is being completed for Directive (EU) 2016/1148, of 6 July, the NIS Directive, which will also affect the public sector, and which, among other issues:

- Will identify the Essential Service Operators.
- The security measures to be applied.
- The competent authorities.
- Will identify the reference CSIRTs.
- Will assign the CCN-CERT the coordination and technical response in particularly severe cases.

In addition, and as a result of fully applying Regulation (EU) 2016/679 of 27 April on processing and free movement of personal data (General Data Protection Regulation), **a new draft Organic Law on Data Protection** has been drawn up which, repealing the current law, will regulate any issues which the General Data Protection Regulation leaves to the Commission.

EUROPEAN ACTIVITY

- **European Commission proposal to replace the e-Privacy Directive** with a regulation covering other communication services in the top layers of the system, in addition to the traditional telecommunications providers.

- Establishing the **EU Cybersecurity Strategy.**

- **Adoption of the NIS Directive** on network and information system security.

- **Proposal for a Regulation of the European Parliament and of the Council** on ICT cybersecurity certification.

- Announcement by the Commission regarding the **evaluation and review of Regulation (EU) No 526/2013** of the European Parliament and Council, which could lead to a possible reform of the Agency and strengthening of its powers and authorities to support Member States sustainably.

CCN-CERT ACTIVITY OF THE NATIONAL CRYPTOLOGY CENTRE

SOLUTION DEVELOPMENT

ATHENEA is the new **cybersecurity challenge training instrument which aims** to raise awareness on the importance of this field.

GLORIA is the platform **for managing cybersecurity incidents and threats,** which has also been interoperable with into the Carmen, Lucía and Reyes tools to make it easier to detect, analyse and exchange incidents.

The **main function of the Early Warning System for Industrial Control Systems** is early **detection of security incidents**. It also allows access to a greater number of detection rules and the correlation of events, favouring support for incident resolution.

LEARNING

In 2017, the National Cryptology Centre has produced more than 146 guides and reports and has also given training courses, both in person and remotely.

RESPONSE TO CYBER ATTACKS

Saguaro
Mexican player focused on credential theft. More than 60,000 different IP affected addresses and more than 36 countries involved.

STRUTS
Vulnerability that affected millions of web servers connected to the Internet. In Spain, 75 organisms were affected, six of them critically.

NotPetya
Attack on the supply chain in the Ukraine with credential theft. Use of the Eternalblue exploit for its propagation.

January 2017 | *February 2017* | *March 2017* | *May 2017* | *June 2017* | *October 2017*

Owncloud
Suite that gave a server in a private cloud. Exploitation of various vulnerabilities, file access and code execution. Ten entities concerned. Some of them remain vulnerable.

Wannacry
The CCN developed the NoMoreCryv0.1 vaccine and also published a malware report, Ransom. WannaCry. To this day, the tool is still being updated.

#OpCatalunya
Four-phase campaign against Public Administrations and companies. DDoS attacks on more than 70 pages. In addition, social networks were used to increase visibility and coordination.

7 TRENDS

It is expected that future cyber attacks will become more sophisticated, virulent and bold. The following are some examples of developing trends in the immediate future.

EXPLOITS-KITS

The decrease in the number of attackable vulnerabilities will cause a decrease in the use of exploits-kits (although they will continue to be used in geographic regions where they cannot be monitored by researchers). Thus, "human kits" will be introduced where threat actors will change their business model to achieve their objectives by attacking **human weaknesses.**

DENIAL OF SERVICE ATTACKS

Everything points to an increase in this type of attack, with some variations:

- **Permanent Denial of Service (PDoS)** for the operations involving Data Centres and IoT devices.
- Greater importance and sophistication of DoS telephone attacks (TDoS).
- Increased segmentation (and even personal) of **denial of service attacks combined with e-rescue (Ransom-DoS).**
- Health systems could become a new target.

CYBER-ESPIONAGE

Experts expect **growth in cyber-espionage** due to geopolitical triggers, economic sanctions or nations' strategic objectives. For this purpose, although they **will continue to use APTs**, new techniques and tools are being created to steal intellectual property and their targets' secrets.

RANSOMWARE

In the immediate future, there will be an **increase in targeted attacks**, such as against healthcare devices.

MORE SECURITY VULNERABILITIES

Analysts, such as Tyler Moffitt of Webroot, agree that there will be significant security breaches in the coming months **that could affect at least 100 million accounts**, a threat that, according to Imperva, will extend to massive data breaches in the cloud.

ADOPTION OF BIOMETRICS

Webroot has indicated that, over the coming months, we will see the first exploits aimed at biometric access, based on facial recognition or fingerprints.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

The security industry will begin to use more automation, machine learning and artificial intelligence to combat cyber-attacks, as FireEye has pointed out.

MOBILE THREATS

In the coming months, according to Webroot, the first major malware infection will appear in the Android App Store. Other companies claim that 2018 and 2019 will see the first spread mobile ransomware, probably via SMS/MMS.

Internet of things regulation

This could be the most affected sector by the Meltdown and Spectre gaps, even though many specialists agree that the legislation will be the biggest change. It will come as no surprise when events such as the Mirai botnet are repeated, but this time with little capability to respond.

More sophisticated crime

In the coming years, cybercriminals will take advantage of hacking kits from tools filtered or stolen from state-sponsored intelligence agencies.

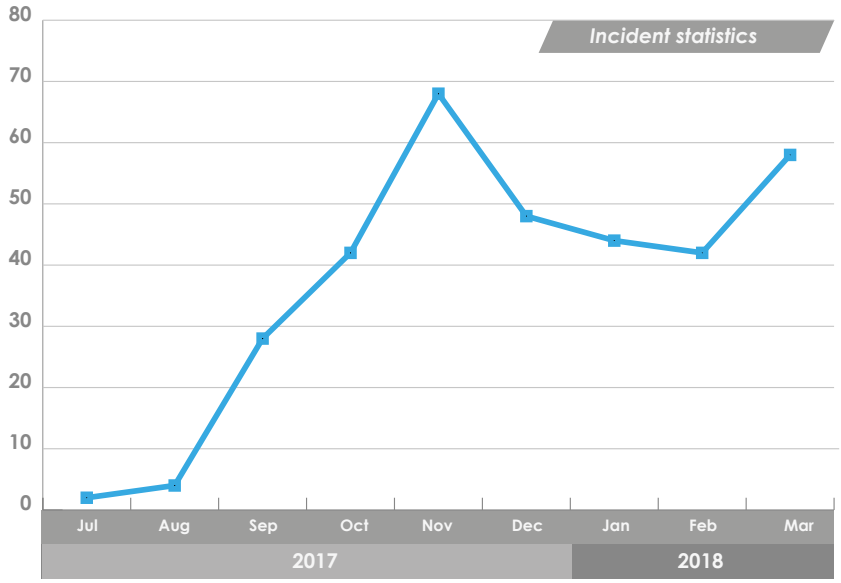
Attacks against social networks

It is likely that the next few months we will see the development of more affordable ways for attackers to access social networks, which can be used for sophisticated social engineering and reconnaissance activities.

As Airbus Cybersecurity points out, to protect themselves from these attacks, organisations must implement security policies, such as employee training programmes and setting up incident response plans that coordinate the activities of legal, human resources, marketing and IT departments.

CRYPTOMINING

The process of generating Cryptocurrency is expected to continue to grow throughout 2018, as more and more **malware families** include mining functionality in their attack arsenal. The current trend also points to **the use of browsers** for cryptomining, where **JavaScript** is the most widely-used technology.



FILELESS MALWARE

Digital Pathways has claimed that "fileless attacks" **will be taken more seriously and will be a threat as powerful as Trojans**; "this type of malicious code resides in the PC memory and remains there until it is rebooted. A normal antivirus will not detect these attacks".

INCREASED USE OF MSSP

Many of the security measures **will be provided by Managed Security Service Providers (MSSPs)**, which will be the focus of increased interest from organisations that recognise that the level of work and internal expertise required for a successful Cybersecurity Operations Center is beyond their capabilities. This has been covered by Resolve.

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es