CYBER-THREATS AND TENDENCIES

2017 EDITION

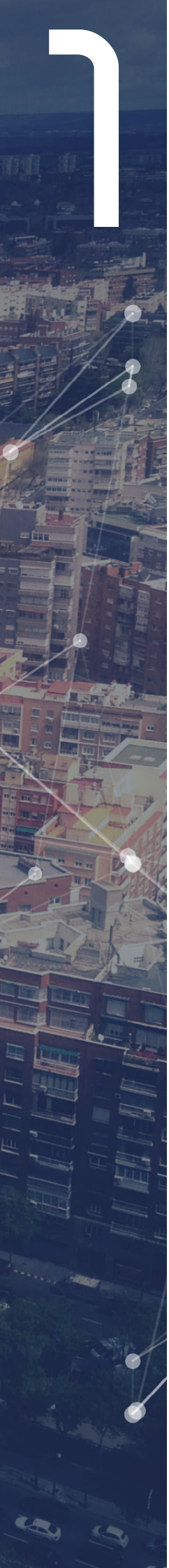
CCN-CERT IA-16/17

EXECUTIVE SUMMARY

con-tents

CCN Centro Criptológico Nacional

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
2017.06.23 11:24:19 +02'00'



1 PROLOGUE

The major threat for the Western world is cyber-espionage, usually carried out by foreign intelligence services

The National Cryptology Centre Cyber-incident Response Capacity (CCN-CERT) managed a total of 20,940 **cyber incidents** in 2016, mainly detected in the public sector and in companies considered to be of strategic interest for Spain, representing 14.5% more than in 2015. Out of them, 3.6% were considered by the National Governmental CERT team of experts as very high or critical, depending on the degree of danger determined by the type of threat, origin of the attacker, victim profile, number or type of systems being affected, impact, possible inclusion in a wider reaching campaign, etc.

Behind these figures, ever-increasing year after year in our country and throughout the world, information has been compromised at the very highest level; servers blocked whilst awaiting a ransom to be paid, defacing or denials of service on different websites; attacks on financial entities or shutoffs in energy services.

The attacks are made by different **Threat Agents**, using different **Attack Methods**, making the most of multiple **Vulnerabilities** for which **Measures** should be considered to improve protection.

Working from different sources and daily work at the National Cryptology Centre (CCN), it can be seen that the major threat for the Western world is cyber-espionage, usually carried out by **foreign intelligence services**.

Cyber-delinquency, **data-jacking** (such as the recent WannaCry campaign), **cyber-activisim**[1], **cyber-crime as a service or adware** are other aspects analysed by the Cyber-threat and Tendencies Report. *Edición 2017*[2] that has been drawn up by the CCN-CERT for the ninth year running. You are currently reading its executive summary. We hope this document will provide interesting reading on existing cyber-threats, helping to tackle the difficult task of cyber-security more effectively.

[1] Hacktivism or cyber-activism. Anti-social digital activism. Activists aim to take control of computers or websites to promote their cause, defend their political position or interrupt services, preventing or making it difficult to use them legitimately.
[2] The complete report (CCN-CERT IA-16/17 Cyber-threats and Tendencies. 2017 Edition) is available on the website https://www.ccn-cert.cni.es

2 CYBERINCIDENTS
What's going on?

The following sections discuss the most significant cyber incidents of 2016, grouped by the motivation behind the threats

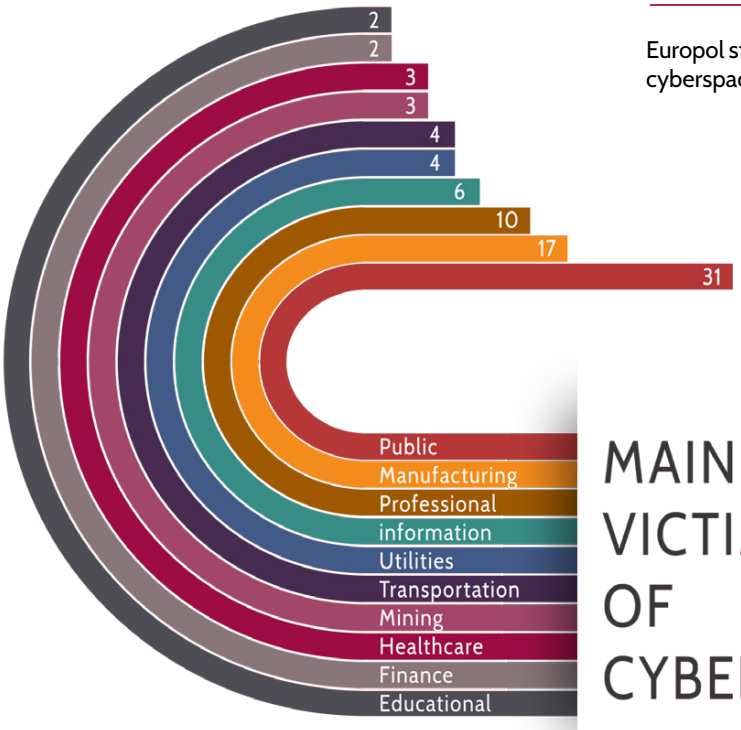
CYBER-ESPIONAGE

For Spain, like the other countries around us, cyber-espionage remains the greatest threat to national security. During 2016, western intelligence services saw significant growth in economic cyber-espionage particularly targeting industries in the **defence**, **advanced technology**, **chemical**, **energy** and **health** sectors, seeking access to advanced developments held by Countries and companies.

Political cyber-espionage is equally important, originating in Intelligence Services that seek political, economic or strategic information and development plans and national positions around debates or open negotiations.

CYBER-CRIME

Europol states that 2016 saw a substantial increase in criminal actions in cyberspace, even exceeding traditional crime in some countries.



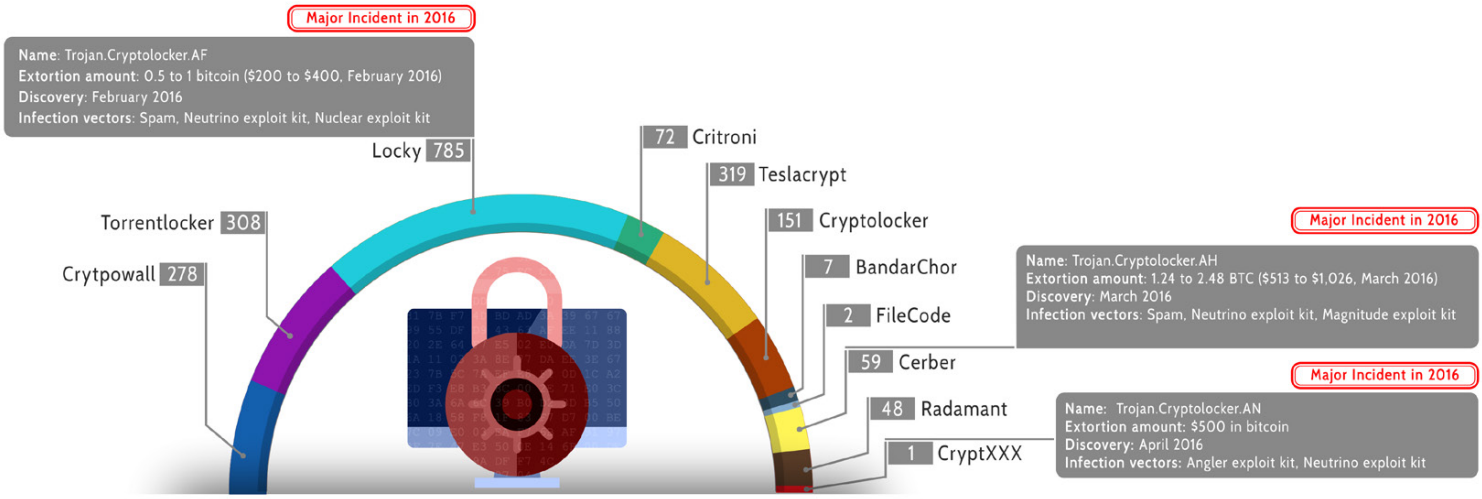
MAIN VICTIMS OF CYBER-ESPIONAGE

RANSOMWARE AND CRYPTOWARE

Ransomware[3] was the line of attack with the **greatest increase during 2016**, with almost 150,000 cases per month. It grew exponentially throughout the world, particularly in energy sectors (seeking to shut down services), and also governmental, health and telecommunications sectors.

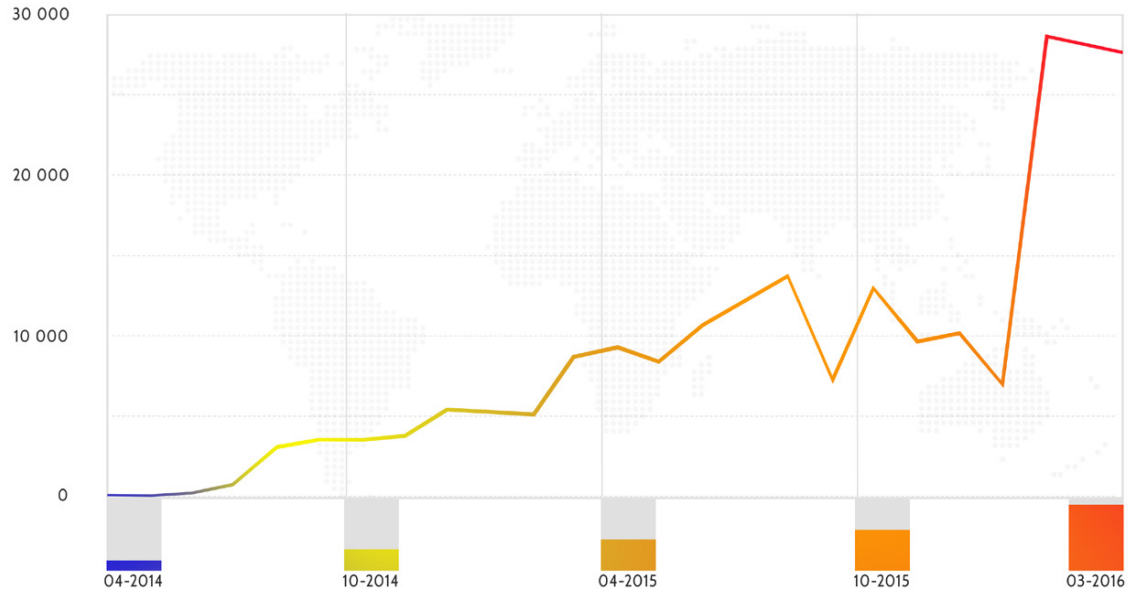
Attacks are **becoming increasingly focussed**, using **social engineering techniques**, affecting security copy systems and often making it impossible to recover the information.

In Spain alone, and from CCN-CERT, a total of 2030 incidents involving different types of ransomware were managed in 2016, 375% more than in 2015



Nº OF INCIDENTS RANSOMWARE (CCN-CERT)

COMPROMISED MOBILE DEVICES[4]



[3] Hijacking the computer (making it impossible to use it) or encrypting its files (Cryptoware), promising to release them after a certain amount of money has been paid as a ransom
[4] Source: Kaspersky Lb

WANNACRY CAMPAIGN

A special mention should be given to the WannaCry ransomware campaign, detected on 12th May 2017, that achieved as yet unseen media repercussions all over the world. This campaign used the exploit[5] that made the most of a Microsoft vulnerability (MS17-010) for which a patch had been published by the company on 14th March.

In our country, the CCN-CERT, that launched the first vaccine for this malware within 24 hours (NoMoreCry Tool), detected 239 IP addresses that had tried to contact one of the identified malware domains.

In the same way, and despite prevention and mitigation resources published by the actual National Governmental CERT on the same day as the attack,[6] five days later there were still 2774 IP addresses originating in Spain that were still vulnerable to the exploit.

ADWARE

2016 was particularly significant for cyber incidents caused by the presence of malvertisments on very well-known websites. On many occasions, the methodology followed by the attackers suggests the presence of cyber-criminals.

ATTACKS ON FINANCIAL ENTITIES

There were fewer attacks on end users, but ransomware and RAT *(Remote Access Tools)* targeting the actual banks[7] have increased.

In addition, phishing[8] campaigns are still going strong in an attempt to obtain credentials that are then sold on the Deep Web with a high success rate due to the careful construction of the hoax mail.

[5] Program that exploits or makes the most of vulnerability in a computer system for its own benefit. Zero day exploit. Making use of a vulnerability immediately after it has been discovered. It makes the most of the time required by the manufacturers to repair reported vulnerabilities.
[6] https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
[7] As seen in the case of Carnabak, when transactions in the international Swift network were the target of attacks.
[8] Attack method that seeks to obtain personal or confidential information from users by means of trickery or subterfuge, stealing the digital identity of an entity that is trusted in cyberspace.
[9] Source: TrendMicro.

INFORMATION THEFT

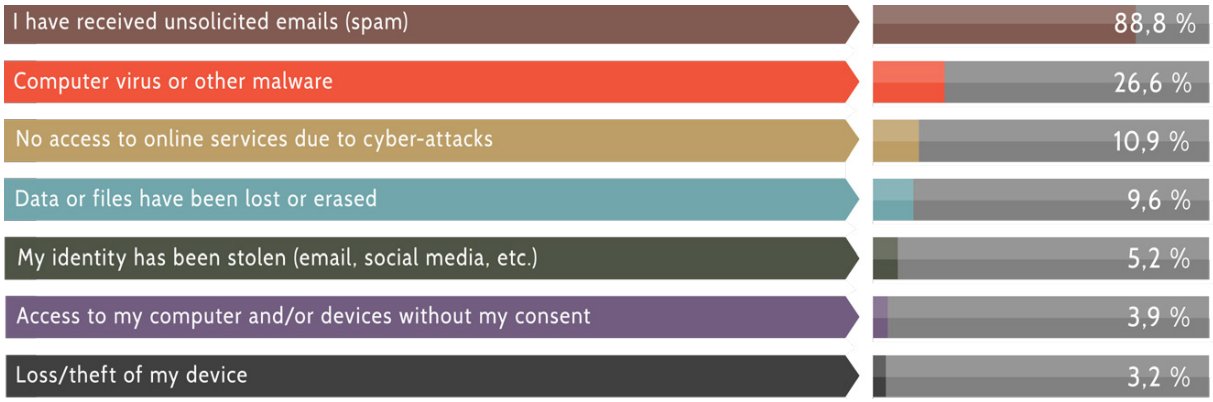
There were many cases during 2016 for economic purposes, obtaining credentials or to develop counterespionage or blackmailing actions[10]: **hospitals**, **political parties**[11] and governments of Western countries, **hospitality** and **trade** or **virtual currency exchanges**. Europol states that up to 89% of data theft is for financial or espionage purposes.

DATA BREACH IN 2016[12]

Organisation	Industry	Country	Source of breach	Records compromised	Data Compromised
Fling	Adult		Malicious outsider	40 000 000	Email, IP, passwords & birth data
T Mobile	Telecoms		Malicious insider	1 500 000	Undisclosed
Kiddicare	Retail		Malicious outsider	794 000	Name, email, telephone & address
Nulled.io	Criminal		Unknown	474 000	User name, email, IP, messages & hashed passwords
Kinoptic	Technology		Accidental loss	198 000	Username, email & hashed passwords
Rosebutt Board	Adult		Malicious outsider	107 000	Username, IP & hashed passwords
Landesbank Berlin & others	Finance		Malicious outsider	85 000	Credit card data
Swiss People's Party (SVP)	Government		Malicious outsider	50 000	Name & email
Islamic State	Military		Malicious insider	22 000	Name, address, phone number, place of birth & sponsor
Greenwich University	Education		Malicious outsider	21 000	Name, email, date of birth, phone number & signature
Engitel	Technology		Hacktivist	20 000+	Username & email
Faithless	Entertainment		Malicious outsider	18 000	Email
National Childbirth Trust	Other		Malicious outsider	15 000	Email & username
ShOping.su	Criminal		Malicious outsider	16 500	Username, email & cards details
Liverpool University	Education		Malicious outsider	6 500	Name & email

[10] Attacks on the U.S. Office Personnel Management (OPM), in June 2015, where data was stolen on four million public employees or the theft of personal data from the Ashley Madison dating website, where thirty million items of data were stolen.
[11] Such as the American Democrat Party.
[12] Breach Level Index, Data Breach Statistics, (véase: http://www.breachlevelindex.com/#!breach-database).

INDIVIDUAL USERS WHO HAVE BEEN VICTIM TO A CYBER-INCIDENT IN 2016[13]



system failure

DENIAL OF SERVICE ATTACKS (DoS)

During 2016, many organisations from all over the world fell victim to denial of service attacks (DoS), that increasingly hide extortion: the victims are urged to pay a ransom to ward off this type of attack[14].

DIGITAL SABOTAGE

The greatest danger is when the attack is led by a State[15], although to date the majority have originated among disgruntled former employees with their own access credentials. The most common actions involve erasing information and destruction/damage to storage supports.

DEFACEMENT

Website defacement is still usual. These are actions that generally stem from ideological reasons or as a means to publicly demonstrate the attackers' skills.

CRITICAL INFRASTRUCTURES

Attacks on industrial control systems are considered to be a potential threat due to the processes that they manage. Confirmed incidents on these systems are still scarce but many facilities have been detected with insecure configurations or Internet connections lacking the right surveillance.

Many facilities have been detected with insecure configurations or Internet connections lacking the right surveillance

[13] Source: ONTSI: Study on Cyber-security and Trust in Spanish homes (Nov. 2016).
[14] One example of organisation for extortion based on DDoS threats is the group called DD4BC *(DDoS for bitcoin)*.
[15] Such as attacks on electricity companies in the Ukraine, leaving between 700,000 and 1.4 million people without power.

Cost of cyber-incidents and their management

Security incidents have an overall cost, derived from several partial costs such as direct economics, service, image and reputation, due to sanctions, etc. In the United States alone in 2015, the *Internet Crime Complaint Center* (IC3) at the FBI managed 288,012 individual complaints about cyber incidents on the Internet with an estimated loss of 1,070 million dollars. The figure for losses around the world stands at around 400,000 million dollars[16].

As far as **ransomware** is concerned, the average ransom demanded by the attackers increased up to 679 dollars in 2016 compared to 294 dollars in 2015. In 2016, a new record was also set with the **Cryptolocker** family, by asking for a ransom of 13 bitcoin[17] per infected computer (around 5,083 dollars)[18].

[16] Source: Khoo Boon Hui (Ex president of INTERPOL). "Cyber-criminals make their fortune on the Internet." Bankinter Innovation Foundation – Future Trends Forum Foundation.
[17] Digital currency or crypto-currency with an approximate value of 39 dollars per unit.
[18] Source: Symantec: Special Report: Ransomware and Businesses, 2016.

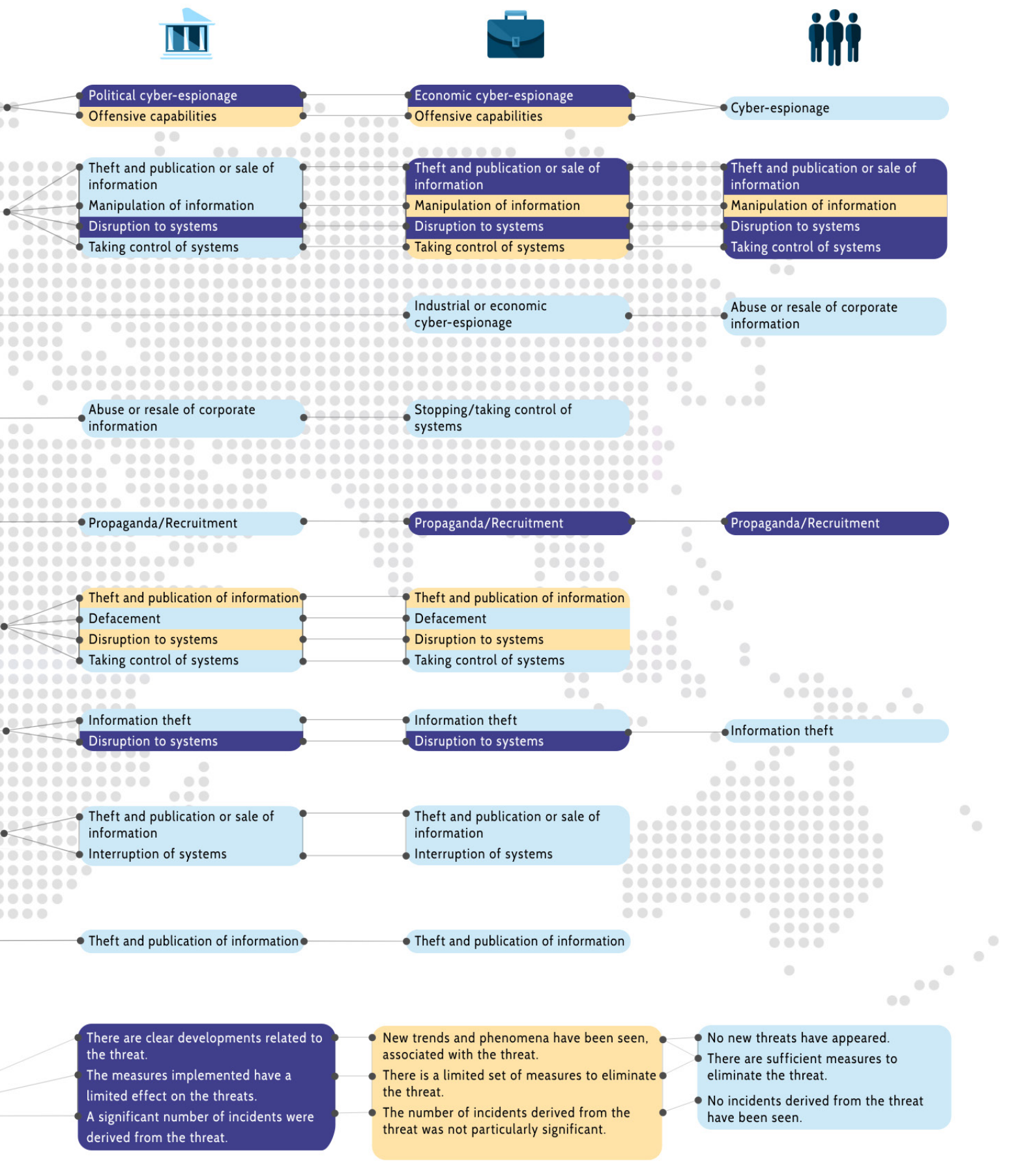
THREAT AGENTS

	ORIGIN	MOTIVATION
1	STATES	Improve your geopolitical or strategic position
2	CRIMINAL ORGANIZATIONS	Economic benefit (direct and indirect)
3	PRIVATE ORGANIZATIONS	Cyberspace: obtaining valuable information
4	CYBERTERRORISTS	Alter the normal social development, frighten the population or influence political decisions.
5	CIBERYIHADISTAS	Advertising, recruitment
6	CYBERACTIVISM	Ideology
7	CYBERBULLYING AND SCRIPT KIDDIES[19]	Demonstrate vulnerabilities, piracy, fun, challenges.
8	INTERNAL ACTORS	Revenge, economic benefit, ideological motives.
9	CYBERINVESTIGATORS	Evidence of weaknesses, self-assertion

LEVEL OF DANGER

[19] They are those who, with limited knowledge and using tools built by third parties, perpetrate their actions as a challenge, without being, on many occasions, fully aware of its consequences.

VICTIMS


PUBLIC SECTOR
PRIVATE ORGANISATIONS
CITIZENS
Political cyber-espionage
Offensive capabilities
Economic cyber-espionage
Offensive capabilities
Cyber-espionage
Theft and publication or sale of information
Manipulation of information
Disruption to systems
Taking control of systems
Theft and publication or sale of information
Manipulation of information
Disruption to systems
Taking control of systems
Theft and publication or sale of information
Manipulation of information
Disruption to systems
Taking control of systems
Industrial or economic cyber-espionage
Abuse or resale of corporate information
Abuse or resale of corporate information
Stopping/taking control of systems
Propaganda/Recruitment
Propaganda/Recruitment
Propaganda/Recruitment
Theft and publication of information
Defacement
Disruption to systems
Taking control of systems
Theft and publication of information
Defacement
Disruption to systems
Taking control of systems
Information theft
Disruption to systems
Information theft
Disruption to systems
Information theft
Theft and publication or sale of information
Interruption of systems
Theft and publication or sale of information
Interruption of systems
Theft and publication of information
Theft and publication of information
There are clear developments related to the threat.
The measures implemented have a limited effect on the threats.
A significant number of incidents were derived from the threat.
New trends and phenomena have been seen, associated with the threat.
There is a limited set of measures to eliminate the threat.
The number of incidents derived from the threat was not particularly significant.
No new threats have appeared.
There are sufficient measures to eliminate the threat.
No incidents derived from the threat have been seen.

3 THREAT AGENTS

Who is attacking us?

States

The greatest threat for national cyber-security comes from actions run by States, particularly any originating among Intelligence Services. They are a real alternative to espionage, due to their low cost, the difficulty of proving who is behind them and the significant volume of information that can be obtained this way.

Reasons why States use these tactics:

- To obtain information from the victim on national security and defence, intellectual property and intelligence on military capabilities (exploiting this subsequently, after vulnerabilities have been revealed).
- To prevent their rival from using communication channels in cyberspace.
- To carry out subversive activities in crisis or conflict situations, or influence actions.

Spain has received attacks specifically aimed at the Defence industries, technology companies and entities representing the public sector.

On the other hand, States continue to invest in developing **cyber-offensive** capabilities, generally carried out via Intelligence Services and specific cyber defence units in the Armed Forces.

During 2016, the concept of hybrid war[20] was consolidated, one of the most relevant emerging threats. Groups such as APT28, associated with the Russian military intelligence agency (GRU), carried out different actions included in this concept.

The last few years have shown that threats to information systems continue to rise in terms of type, volume, sophistication and danger

Criminal organisations

They seek to gain direct (stealing credentials) or indirect (through extortion) economic profit from both organisations and individuals. In the latter case, **ransomware** and threats related to **DoS** attacks[21] were the most-used methods.

The level of knowledge varies widely and covers the whole spectrum from the specialists (with a high level of professionalism and innovation) to low level groups. Consequently, use of ***Cybercrime as a service*** is still on the up, using the deep web to exchange tools and plan attacks.

Services are seen such as sale of ready to use malware (including ransomware), information stolen from credit cards, emails and social media, tools to develop denial of service attacks or remote access tools (RAT) designed to commission criminal actions.

The use of techniques to remain **anonymous** (intermediaries or proxies, virtual private networks and TOR[22]) in conjunction with **bitcoins** make investigation work extraordinarily difficult.

Significant growth has been seen in cooperation, even involving physical presence, between different groups of cyber-criminals[23].

[20] Operation run by a State that uses open and covert tactics with the aim of destabilising other States and polarising the civil population. It includes a wide variety of tools such as diplomacy and traditional intelligence actions, subversive acts and sabotage, political and economic influence, instrumentation of organised crime, psychological operations and propaganda.
[21] The best known attackers have been DD4BC and Armada Collective.
[22] TOR (abbreviation of The Onion Router) is software designed to allow anonymous access to the Internet. Although for many years it was mainly used by experts and fans, use of the TOR network has really taken off lately, due to Internet privacy issues. TOR has become a very useful tool for anyone that, for any reason, legal or illegal, does not wish to be monitored or does not wish to reveal confidential information.
[23] Dyre malware campaign where several groups of cybercriminals got together in an office building in Russia. http://tweakers.net/nieuws/108009/verspreiding- financiele-dyre-malware-gestopt-door-russische-autoriteiten.html

cyber-activism[24]

These groups justify their actions with ideological reasons and their idea is to raise awareness on a cause. It is considered to be a form of insurgent activism.

Their actions have focussed on denial of service (DoS) attacks on governmental targets, the media and private organisations and revealing certain behaviour or personal information from governmental institutions. Their skills vary widely, often becoming highly sophisticated.

In Spain, this has been going on without becoming a stable collective since 2012, when the police broke up the **Anonymous infrastructure** (#OpSpain). The cyber-activist ecosystem is characterised by low density of propaganda identities with barely operative skills, with the exception of the "**9th Company of Anonymous**" that has compromised websites belonging to town councils, the media, companies and Chambers of Commerce.

cyber-terrorism

Jihadist terrorism also uses cyberspace for tasks that do not imply direct commissioning of attacks, but rather radicalising, recruitment and logistics work.

The **use of the Internet** represents an operation procedure that is used intensely by Jihadist groups, mainly by **Daesh**[25], but also by **Al Qaeda, Boko Haram** or **Al Shabaab** to the extent that newly created groups such as **Harakat Sawa'd Misr** that appeared in Egypt in 2016 come with their own website [https:// hasam. org]. However, whilst terrorist actions have not been seen in cyberspace, there has been activity from terrorist groups or organisations in it.

The majority of so-called Cyber-jihadists[26] in addition to defacing websites[27], small DDoS attacks or against social media accounts, have concentrated on hiding the information being exchanged through encrypted communication channels.

[24] There is an appendix to the General report focussing on Hacktivism or Cyber-Jihadism CCN-CERT IA-04/17 Hacktivism and Cyber-Jihadism 2016.
[25] Al-Dawla al –islamiya fil Iraq wa al Sham (or ISIS in English). Islamic State of Iraq and the "sham" that includes Iraq, Syria and part of the Lebanon.
[26] The potentially most significant players in cyber-jihadism are: Al Qaeda, Al Shabaab, Boko Haram and ISIS (or Daesh). See: "The Anatomy of Cyber-Jihad". J. Scott and D. Spaniel (2016).
[27] As could be seen after the Paris attacks.

THESE PLAYERS DEVELOP THEIR ACTIONS AS A CHALLENGE, TO DEMONSTRATE THEIR OWN SKILLS OR AS A SIMPLE JOKE

THIS USUALLY REFERS TO DISGRUNTLED EMPLOYEES OR FORMER EMPLOYEES WHO, FOR ECONOMIC, POLITICAL OR PERSONAL REASONS, DELIBERATELY MANIPULATE SYSTEMS TO CAUSE SEVERE DISTURBANCES

THE AIM CAN BE TO PUT RIVAL INFORMATION SYSTEMS OUT OF ACTION

CYBER-VANDALS AND SCRIPT KIDDIES

During 2016, significant growth was seen in actions by these agents, caused by the increase in tools to perpetrate attacks. These players develop their actions as a challenge, to demonstrate their own skills or as a simple joke.

So-called **Booter-Services**[28] (**DDoS-As-A- Service**) have been used as mechanisms to perpetrate DDoS attacks.

One example is the group known as "Crackas with attitude", that acted against executives from certain North American intelligence units.

INTERNAL PLAYERS AND CYBER-INVESTIGATORS

This usually refers to disgruntled employees or former employees who, for economic, political or personal reasons, deliberately manipulate systems to cause severe disturbances, damage storage systems or steal sensitive information.

Cyber investigators, by seeking out vulnerabilities and not respecting responsible broadcasting by publically showing an inappropriate level of security often make the systems temporarily vulnerable.

PRIVATE ORGANISATIONS

Occasionally, the aim can be to put rival information systems out of action, although it is more usual for these attacks to seek information from the competition to use it for their own profit, or even sell it to third parties. This is what is usually known as industrial cyber-espionage[29].

[28] This is a service offered by cyber-criminals who run distributed denial of service (DDoS) attacks against targets requested by their customers who pay an economic amount for the commission.
[29] In the United States the employees of a company that supplied textile products attacked one of their competitors (see https://www.security.nl/posting/453200/IT-directeur+Amerikaans+be- drijf+hackte+server+concurrent

4 VULNERABILITIES

Why am I being attacked?

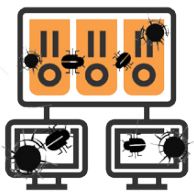
Software

The software industry seems more and more like an assembly line where the product obtained is the result of reusing existing components. If some of the components contain a vulnerability, the final result will also be vulnerable[30].

The number of vulnerabilities continues to grow steadily

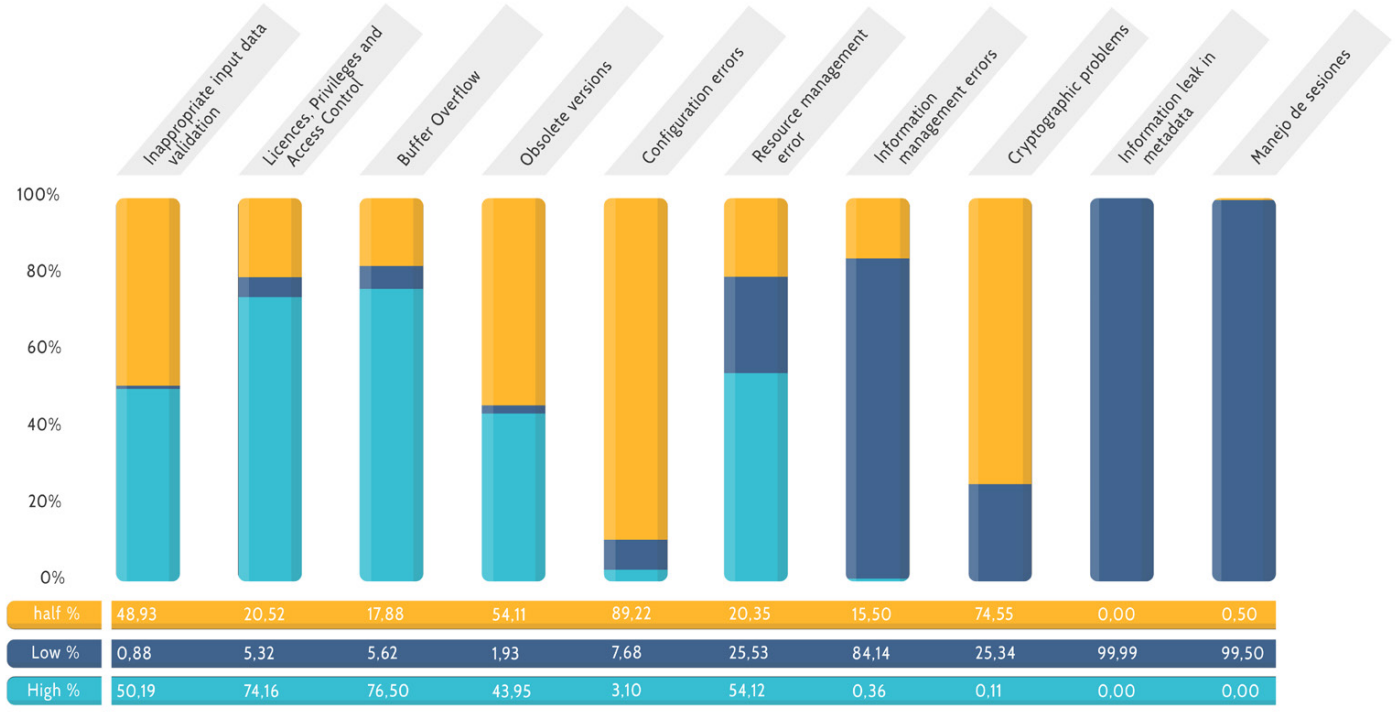
Other aspects to bear in mind:

- Official teaching on programming still pays little attention to cyber-security. It prioritises functional features of software and calculation speed over secure behaviour.
- Software insecurity is particularly delicate in **Industrial Control Systems** that operate for a long time without receiving the necessary updates.
- Many security breaches are due to vulnerabilities that have been around for a while but the organisations in charge do not update them so tools (exploits) can be brought out to exploit them (the case of WannaCry is living proof of this).
- In many organisations, the only security measure is still just antivirus software, often hopelessly out of date.
- The public exhibition of certain vulnerabilities puts the affected systems in grave danger and occasionally, exaggerated publicity lets other more critical vulnerabilities go unnoticed.



[30] The Taiwanese company D-Link accidentally filtered one of its software signature passwords to certain attackers using legitimate D-Link signatures to deploy malware (http://www.theregister.co.uk/2015/09/18/d_link_code_signing_key_leak/).

VULNERABILITY SEVERITY (ACCORDING TO CRITERION CVSS[31])



half %	48,93	20,52	17,88	54,11	89,22	20,35	15,50	74,55	0,00	0,50
Low %	0,88	5,32	5,62	1,93	7,68	25,53	84,14	25,34	99,99	99,50
High %	50,19	74,16	76,50	43,95	3,10	54,12	0,36	0,11	0,00	0,00

THE CCN-CERT WEBSITE[32] PUBLISHED A TOTAL OF 3,773 VULNERABILITIES IN 2016 DECLARED BY THE FOLLOWING MANUFACTURERS:

Developer	1st semester	2nd semester	Total 2016
Adobe	29	10	39
Apple	21	17	38
Cisco	259	82	341
Debian	365	269	634
IBM	1.203	330	1.533
Microsoft	145	125	270
Oracle	5	2	7
Red Hat	229	206	435
Symantec	204	272	476
Total:	2.460	1.313	3.773

[31] *Common Vulnerability Scoring Systems*. Scoring system to estimate the impact derived from vulnerabilities identified in information systems.
[32] https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades.html

USER

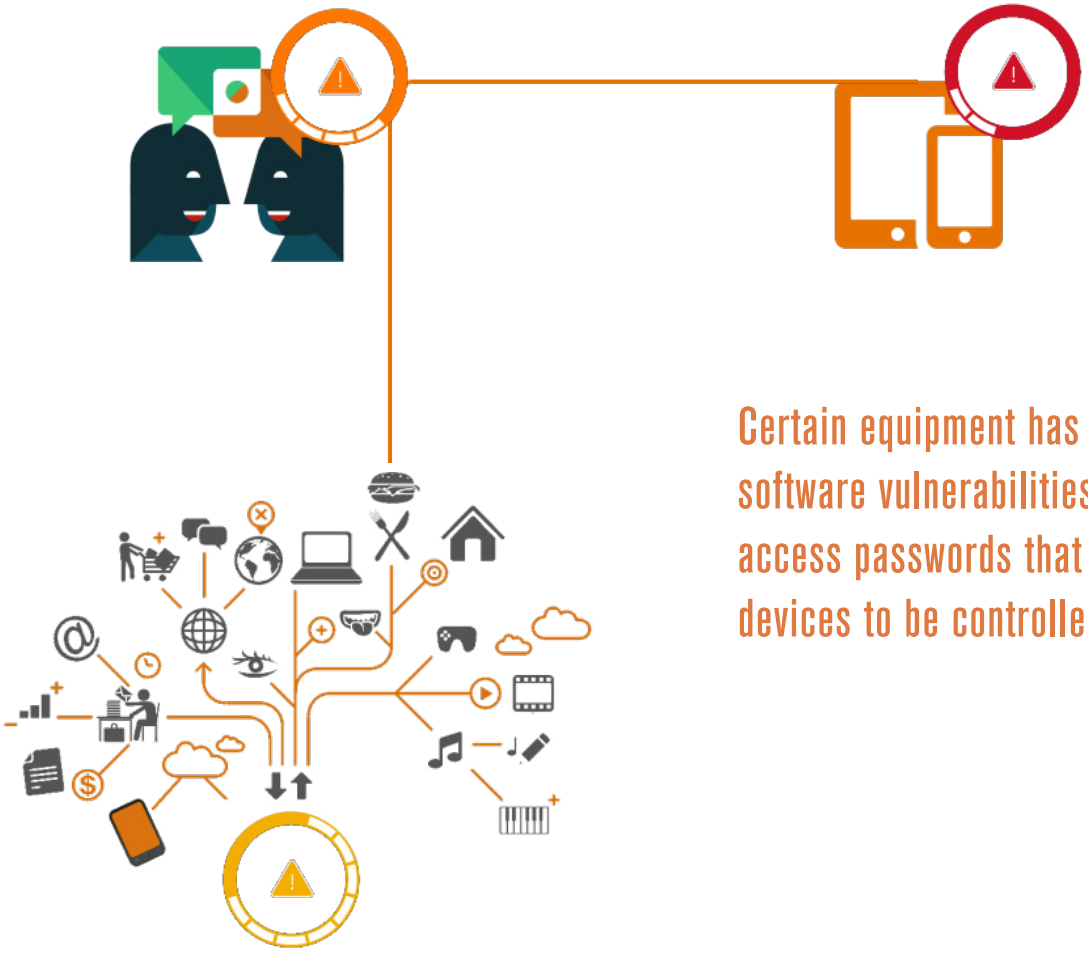
Regarding users, it is advisable to focus on three points: **mobile devices**, social engineering and Internet of Things.

Mobile devices, the pace of their sales and useful life (two years is the norm) mean that many manufacturers no longer publish security updates for the older products, making them easy victims for cyber-attacks.

Social engineering where attackers continually intensify their efforts to trick their victims. Many users have fallen into the spear phishing trap or even phone calls (which increased spectacularly in 2016). When social engineering specifically targets individualised sectors, its success rate grows exponentially.

When social engineering specifically targets individualised sectors, its success rate grows exponentially

The Internet of Things (IoT) where many manufacturers do not seem to be aware of the risks involved in connecting to the Internet and do not implement secure communications protocols, even certain equipment has severe software vulnerabilities or weak access passwords that allow these devices to be controlled remotely.



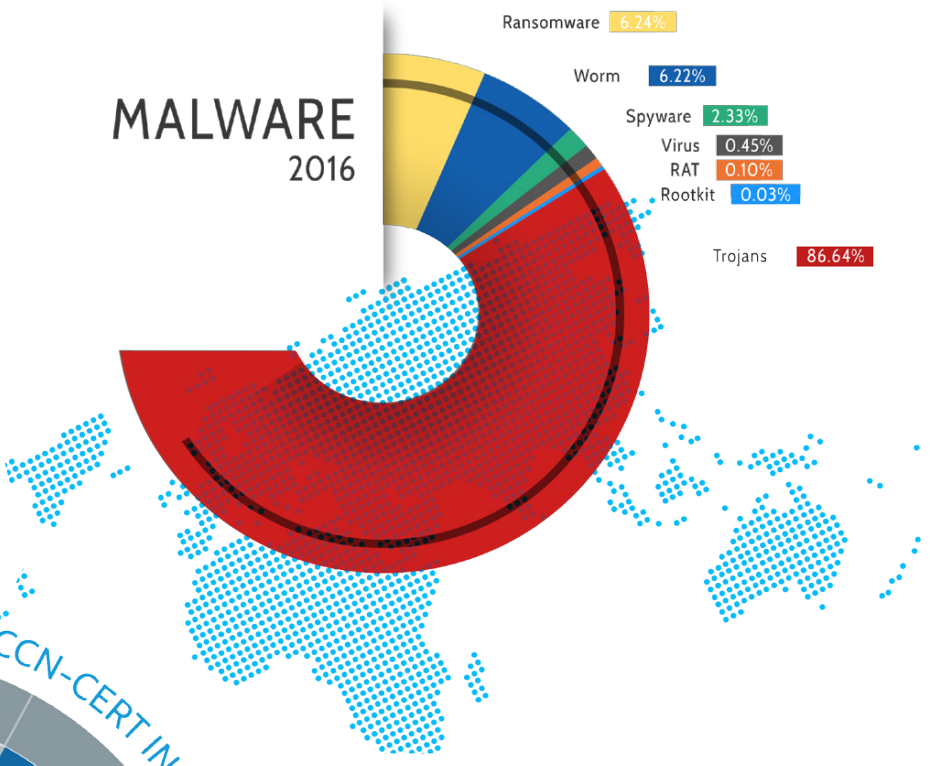
Certain equipment has severe software vulnerabilities or weak access passwords that allow these devices to be controlled remotely

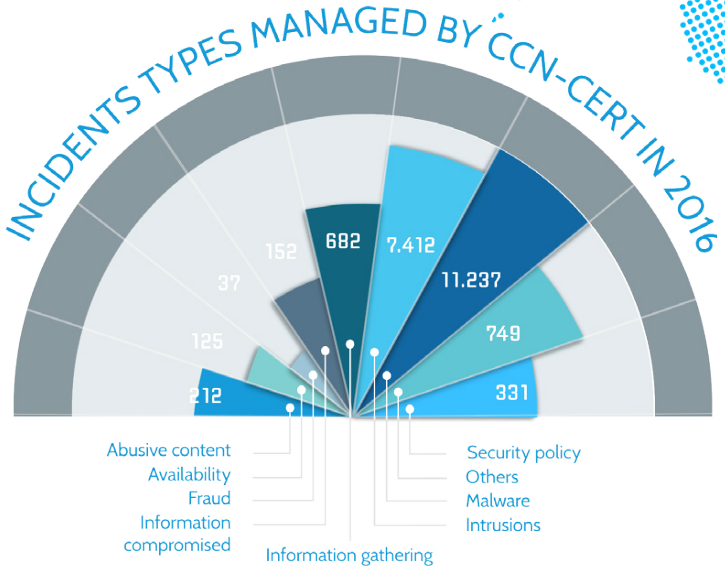
5 ATTACK METHODS

HOW AM I BEING ATTACKED?

Malware

Its importance and presence in many cyber incidents, is clear from CCN-CERT figures. Consequently, in 2016, from the 20,940 cyber incidents managed in the public sector and in companies of strategic interest, 53.6% (11,237) referred to malware (including Trojans[33]).





[33] Trojan Horse or trojan is malware that looks like an inoffensive program but, when run, gives the attacker remote access to the infected computer, normally by installing a backdoor.

In general, there are three main ways to install malware: email with attachments, websites that download this type of software or a hybrid of the two (emails with linked to malware sites).

Most used type:

- **Ransomware**: they started to affect the Apple operating system (mac OS) and other servers such as the KeRanger code, with which, in addition to obtaining a ransom, the attackers entered their victims' networks and threatened to give away their personal information.
- **Infection of trusted websites for users**, such as official stores for applications for mobile devices or infecting development environments, both from the actual software manufacturers and resellers.
- **Mobile devices** continue to be an increasingly frequent target for attackers. Although Android remains the main target, there has been an increase in attacks on iOS

Attack tools (exploit-kits)

Sales of automatic attack tools or exploit kits continue to be one of the most significant threats[34], currently affecting conventional computers, mobile phones and communications devices (routers[35]). However, 86% of exploits in exploit-kits make the most of vulnerabilities in the multimedia Flash Player.

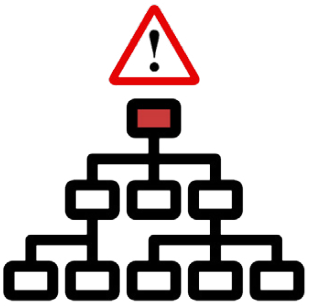
On the other hand, **remote access tools** (RAT) on different operating systems continue to be an effective attacking procedure. Their low cost (around 5 dollars in clandestine forums) boosts their use, even including tech support.

[34] Examples include Angler and Black Energy exploit-kits (associated with the electrical power outages in the Ukraine).
[35] Router.

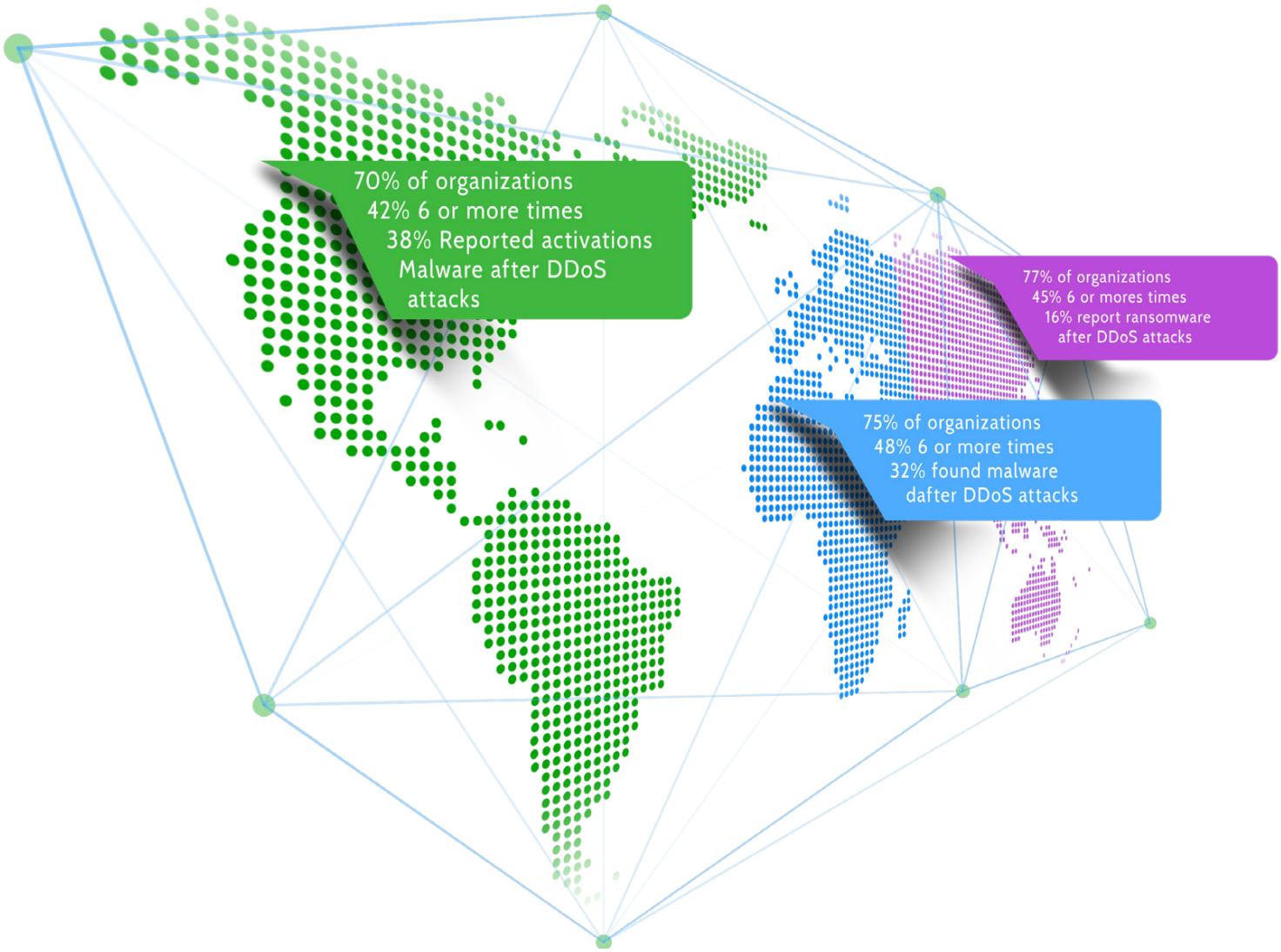
Denial of service attacks (DoS) and web applications

Denial of service attacks registered in just the second quarter of 2016 had increased 129% on the same quarter in 2015[36].

According to a poll carried out by the company Neustar, 73% of all participating organisations suffered a DoS attack, 49 % lost, at least 100,000 dollars per hour during peak periods and 53% had data stolen as a result of a DoS attack.

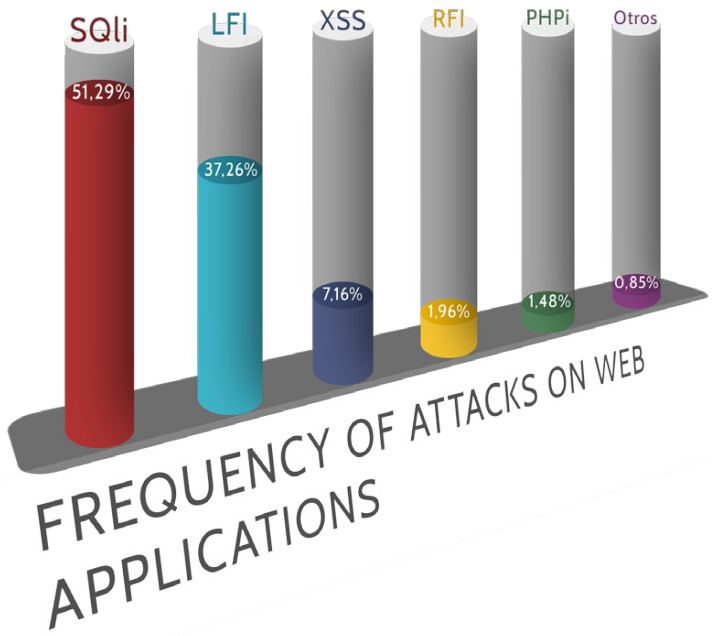


DoS ATTACK INCIDENTS PER CONTINENT



[36] Source: Akamai's State of the Internet/Security. Q2-Q4 2016 Security Report.

During 2016, attackers continued looking for new ways of expanding, abusing the facilities of legitimate applications and services such as: NetBIOS, RPC, Sentinel, RPC Portmapper, DNSSEC, TFTP or Bittorrent. In addition, some types of devices connected to the Internet, such as network electronics (routers, switches, etc.), digital cameras with Internet Protocol (IP), network hard disks and, even, network printers, have also been used to develop DoS attacks.



Regarding **attacks on Web Application**, the most significant attack vectors were **SQL injection**[37] and **Local File inclusion**[38], compared to all the rest. Between the two, they account for almost 90% of all attacks.

The most significant aggressive vectors for attacks on Web applications were SQL injection and Local File inclusion, compared to all the rest. Between the two, they account for almost 90% of all attacks

[37] Structured Query Language: this is a language for managing relational databases.
[38] Local file inclusion means files that are in the same web server with this type of fault as opposed to Remote File Inclusion that includes files hosted in other servers.

Hiding the attacker and abuse of services

Attackers are interested in hiding their identity, erasing evidence that they might have left in the infected systems using concepts such as a **USBthief** where the malware that they contain can only be run from the original USB memory, without leaving any trace in the compromised system.

Abuse of very popular services has also been confirmed such as Dropbox, Pinterest and Google Docs, making the most of the fact that the traffic is usually encrypted by default[39]. The attackers also abused legitimate certification authorities to obtain digital certificates to give them a legal image as well as satellite communications to hide the location of the attack command and control servers (C&C)[40].

We can also predict a rise in the volume of advanced malware and cases of data theft using SSL/TLS[41]. All this means that encrypted traffic management is called on to play an increasingly important role in protecting infrastructures.

WE CAN ALSO PREDICT A RISE IN THE VOLUME OF ADVANCED MALWARE AND CASES OF DATA THEFT USING SSL/TLS

Adware

Advertising that is used to infect the victim's computer continues to be widely used. So-called "adware"[42] continues to increase and has been evolving into **Malvertising-as-a-service** (MaaS)[43].

If some websites receive hundreds of thousands of visits every day, we see that we are up against a major threat as it even allows the infections to be directed towards a specific sector or it might be specifically interested in a certain type of product.

Despite all this, it is not easy to protect against adware. The business model upheld in web advertising would, in many cases, prevent the use of ad-blockers.

[39] For example, Hamertoss, the backdoor for the group known as APT29, used Twitter to communicate with its C&C systems.
[40] Command and control.
[41] Secure Sockets Layer. Encryption protocol that allows secure information exchange between two ends, predecessor of TLS (Transport Layer Security).
[42] Advertising software. Applications that display advertising during use on popup windows or tool bars in exchange for free use. Advertising normally allows you to visit the advertiser's website so it requires an Internet connection to work. It differs from freeware that includes advertising. The majority of advertising programmes are trustworthy but occasionally, some of them are used for unethical purposes, even acting as real spy programs to control user movements.
[43] Malware inserted in adware as a service.

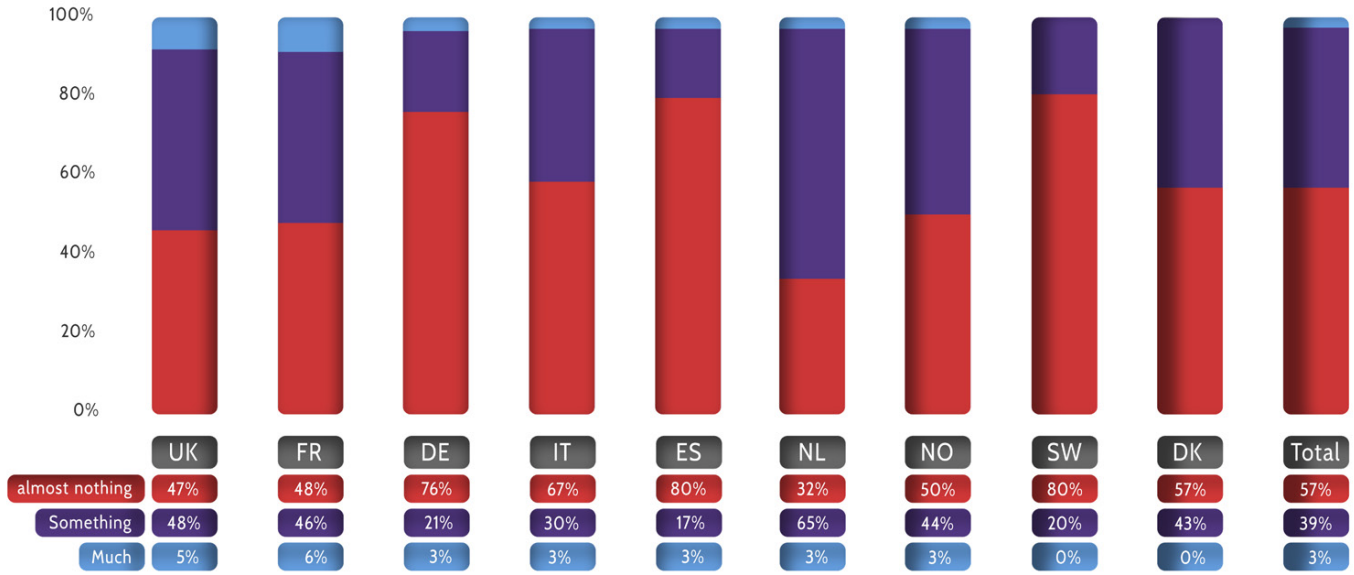
6 MEASURES

HOW CAN I PROTECT MYSELF?

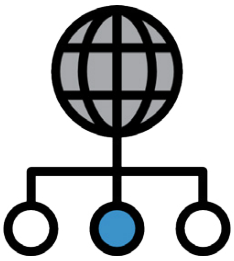
Human factor

Awareness-raising regarding cyber-security still leaves a lot to be desired in many countries. The following diagram (survey by Lloyd's) shows the degree of awareness among businessmen from certain European countries on such extremes.

DEGREE OF AWARENESS IN COMPANIES



	UK	FR	DE	IT	ES	NL	NO	SW	DK	Total
almost nothing	47%	48%	76%	67%	80%	32%	50%	80%	57%	57%
Something	48%	46%	21%	30%	17%	65%	44%	20%	43%	39%
Much	5%	6%	3%	3%	3%	3%	3%	0%	0%	3%



Awareness-raising alone is not enough. According to a Verizon report, users open 30% of suspicious emails (phishing) and click on 12% of attachments.

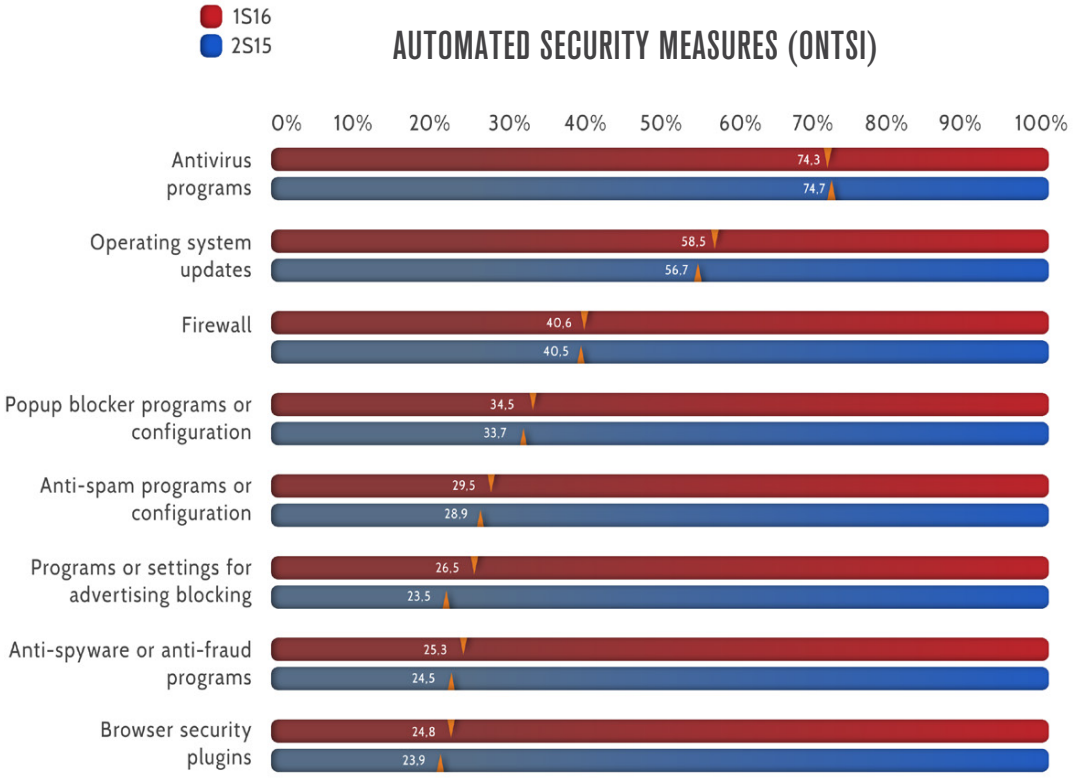
In addition, the current scarcity of professionals working in cyber-security is an issue. Consequently, organisations must make an additional effort to train their staff. There is a significant absence of staff with the profile for monitoring systems, investigating incidents, forensic analysis or implementation of security configurations.

Technological factor

Despite the fact that the user is often the weakest link in a cyber-attack chain, technology remains essential to guarantee security.

Particularly delicate elements are software **versions with no support** or a lack of consensus on which security configurations would be best to prevent attacks.

Using standards such as the National Security Framework (ENS)[44], can significantly help identify these measures. The configurations proposed in the different series of security guides by the National Cryptology Centre (CCN-STIC) are highly recommended.



It is appropriate to highlight in this respect that the National Cryptology Centre's functions include protection and promotion of secure technology. It coordinates promotion, development, obtaining, purchasing and putting into operation and use of security technologies; in addition to assessing and certifying encryption products and authorising systems to handle information securely; making up the **Certification Organisation**[45] for the National Framework for Security Assessment and Certification, to be applied to products and systems in its field.

In fact, publication of a **Catalogue of Recommended Products** has been envisaged, offering a list of ICT security products supervised by the CCN that will provide a minimum level of trust to the end user and the organisation using them.

[44] The ENS developed by RD 3/2010, dated 8th January, is applied to the Spanish public sector (Law 40/2015, dated 1st October).
[45] From which the Assessment and Certification Regulation is applied on Security of Information Technologies, approved by Order PRE/2740/2007, dated 19th September.

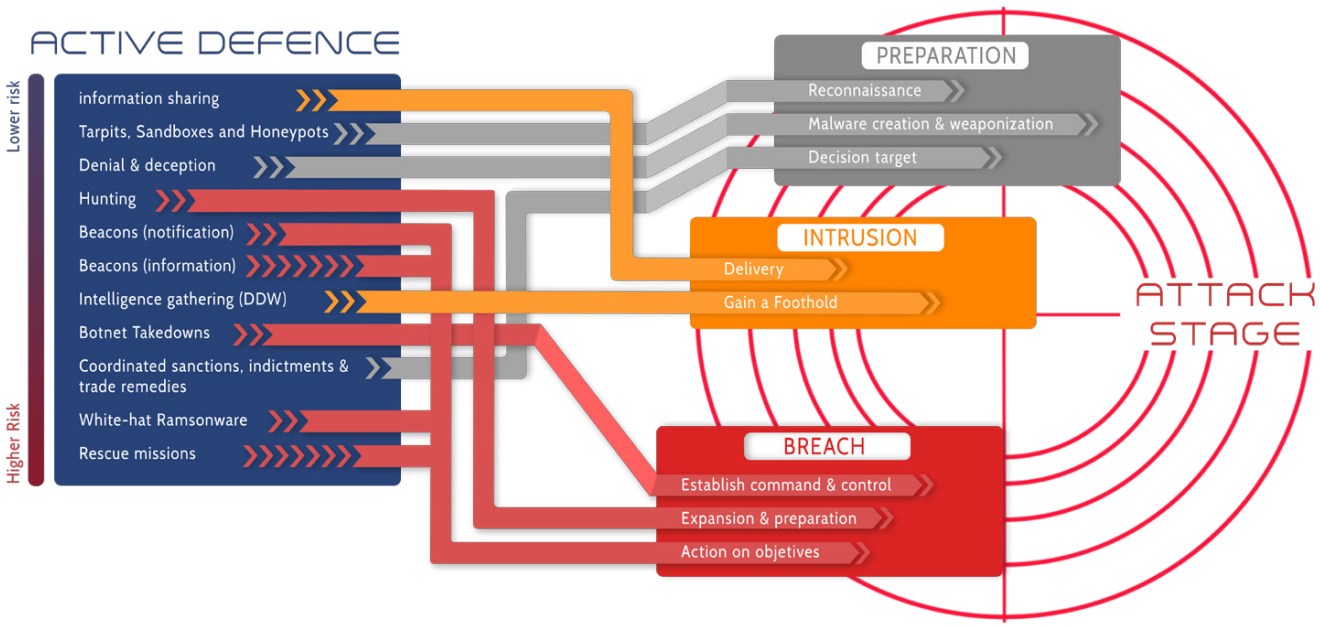
ECONOMIC AND METHODOLOGICAL FACTOR

Every day new dangers appear in cyberspace that are difficult to quantify. In this context, **cyber-risk policies** are drawn up as the first line of defence that will have beneficial effects on the national and international markets, along with awareness-raising among workers and an increase in corporate cyber-security.

Finally, 2016 put **Active Defence** on the world's stage. These activities can cross the threshold of the victim's network borders and produce (negative) effects on the other's network. The organisation's network limits can never been passed and for such actions, the responsible organisation's support must be requested.

2016 put Active Defence on the world's stage. These activities can cross the threshold of the victim's network borders and produce (negative) effects on the other's network

ACTIVE DEFENCE MEASURES TENDING TO BLOCK A CYBER-ATTACK[46]



[46] Source: Center for Cyber & Homeland Security

International initiatives

Some of the most significant initiatives developed internationally in late 2015 and 2016 are shown below.

- **NIS European Directive:** in July 2016, the European Parliament adapted the Directive on network and information system security that requires all Member States to have their own cyber-security capabilities, strengthening cooperation between states and establishing specific requirements for essential service operators. In Spain, a work group has been set up that is transposing the law for this Directive.

  Obligations will involve adopting a national strategy, requirements for security and notification, as well as designation of competent national authorities, single contact points and CSIRT[47] with functions related to cyber-security.

- **General Data Protection Regulation (RGPD):** on 4th May 2016, after several years of processing, standard instruments were published making up the new European framework for personal data protection.

  - **European Regulation 2016/679, dated 27 April**, relating to protecting physical persons in terms of processing personal data and freedom of movement.

  - **Directive 2016/680, dated 27 April**, relating to protecting physical persons in terms of processing personal data by the competent authorities for the purposes of prevention, investigation, detection or processing of criminal offences or executing criminal sanctions.

  - **Directive 2016/681, dated 27 April**, relating to the use of passenger number register (PNR) data for prevention, detection, investigation and processing of crimes of terrorism and serious delinquency.

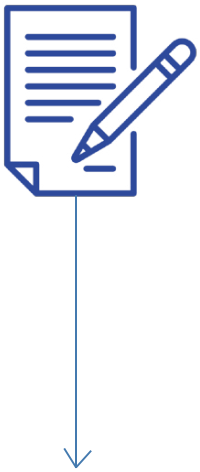
  This regulation bases the application of security measures on risk and impact analysis. They make it compulsory and recommended to apply measures based on codes of best practice and certification schemes and notification of incidents.

- **CSIRT deployment throughout the world** : development of response capacities has been enormously strengthened in many countries, with the mission of supporting the organisations in resolving detected cyber incidents. There are hundreds of CSIRT in the world, with different missions and scope. In 2016, there were 369 teams signed up to FIRST[48], from 80 different countries, including 14 from Spain.

- **Responsible revealing of security vulnerabilities**: as a mechanism to conciliate cyber-investigators' work with the need for discretion concerning their findings. In April 2016, the International Standardisation Organisation (ISO) published the ISO 29147 document on revealing vulnerabilities.

In the complete threat report (CCN-CERT IA-16/17), there is a list of other initiatives carried out by neighbouring countries.

We should highlight the **Global Cyber-security Index** to compare the level of cyber-security that has been implemented, working from the ***Global Cybersecurity Agenda*** initiative from the **International Telecommunications Union** ITU).



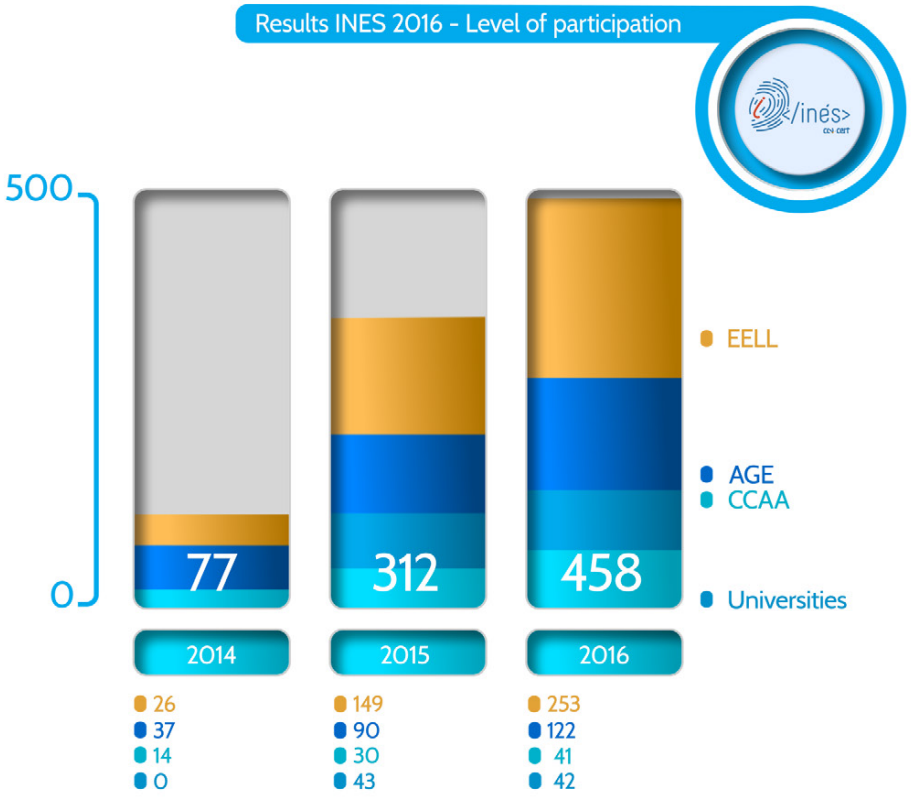
NIS European Directive requires all Member States to have their own cyber-security capabilities

[47] Computer Security Incident Report Team. Response team for cyber incidents.
[48] Main CSIRT organisation in the world https://www.first.org

National initiatives: the National Security Framework

2016 was particularly important for electronic development of work in the Spanish Public Sector.

- **Law 39/2015**, on the Common Administrative Procedure for Public Administrations and Law 40/2015, on the Public Sector Legal Regime, both dated 01 October 2015 (coming into force in November 2016).
- Technical Security Instruction from the State Security Report (Ruling of 7th October 2016). The **National State Security Report** (INES) for information and communication technology systems in 2016 has included data from 458 public sector organisations, with a total of 14,577 ICT declared systems that provide service to 3,467,434 users and from which an overall national score is given depending on how well the National Security Framework has been implemented.
- Technical Security Instruction in compliance with the National Security Framework (Ruling of 13 October 2016).



7 TRENDS FOR 2017

WHERE ARE WE HEADING?

CYBER-ESPIONAGE

It will remain very active in 2017 as part of a State's intelligence operations or run by organised groups that will provide services or will search for information of interest and will be able to sell it. More actions are envisaged regarding influence in decision-making processes and in cyber-sabotage within the framework of hybrid operations.

NEW TYPES OF COMPLEX ATTACKS

Some **infection mechanisms do not use malware**, nor have they written (almost) anything on disks for several years now. It is going to be increasingly usual to see malware in "**no file**" **mode** run in the memory and sticking around as a **task programmed** directly from the **register**.

ELEMENTS "CHARACTERISING" THE MOST "ADVANCED" CYBER-ESPIONAGE GROUPS

- Use of zero-day exploits[49].
- Unknown infection vectors, not previously identified.
- Commitment from several governmental organisations in several countries.
- Successful extraction of information for many years before being discovered.
- Capability to extract information from isolated networks.
- Have multiple exfiltration channels.
- Malware in the equipment memory, without using the disk.
- Advanced persistent threat techniques that use undocumented functions.

It will be necessary to increase and widen the surveillance capabilities based on faults and improve the exchange of detection patterns in any format (IoC[50], Yara rules, etc.)

[49] Zero Day exploit. Making use of a vulnerability immediately after it has been discovered.
[50] Indicator of compromise.

WHILST CRITICAL INFRASTRUCTURES AND THE INDUSTRIAL MANUFACTURING SYSTEMS REMAIN CONNECTED TO THE INTERNET WITHOUT REQUIRED UPDATES AND USING DEFAULT CONFIGURATIONS, WITH LITTLE OR NO PERIMETER PROTECTION, THEY WILL REMAIN A TARGET FOR ATTACKERS

SHORT-LIVED INFECTIONS

There will be increase in memory-resident malware, intended for general recognition and stealing credentials, **without remaining in the victim's system**. This requires new, more sophisticated detection tools.

THREATS TO HARDWARE AND FIRMWARE[51]

Hardware vulnerabilities can undermine operation and security for all software. So, hardware vulnerability exploitation can compromise the entire system and not require complete exploitation. In addition, systems whose hardware has been attacked are difficult to repair.

MOBILE DEVICES AS A TARGET FOR CYBER-ESPIONAGE

There is increasingly frequent use of mobile devices in professional circles so it is expected that during 2017, the cyber-espionage campaigns directed at this equipment will increase, specifically the growth of ransomware, banking trojans and monitoring and remote access tools.

ATTACKS ON FINANCIAL ENTITIES

Banks will be attacked more than users. It is probable that 2017 will see an increase in attacks directly against electronic payment system technological infrastructures as well as selling these attacks by means of services such as ***Crime-as-a-service***[52].

LOSS OF TRUST IN RANSOMWARE

These attacks are based on the principle that the attack will respect a tacit contract with the victim. However, it is highly possible that there are cases where, despite having paid the ransom, encrypted files are not released. This can cause a trust issue leading people to think that paying the ransom does not lead anywhere, which is actually exactly what the CCN-CERT recommends. Regardless, it will continue to be a highly significant threat in 2017, including *Ransomware-as-a-Service*.

CYBER-ATTACKS AGAINST INDUSTRIAL CONTROL SYSTEMS

Whilst Critical Infrastructures and the industrial manufacturing systems remain connected to the Internet without required updates and using default configurations, with little or no perimeter protection, they will remain a target for attackers.

[51] Firmware works as the meeting point between the instructions (software) that reach the device from the outside and the different electronic parts (hardware)
[52] Cyber-crime as a service

PHYSICAL AND LOGICAL SECURITY COOPERATION

It can be presumed that physical security and cyber-security industries will work together in 2017 to come up with complete security solutions. Cyber-security suppliers will start to provide service and give support to physical security providers by offering new software, platforms and architectures for integration.

POOR SECURITY FOR THE INTERNET OF THINGS

Whilst the manufacturers of IoT[53] devices continue producing devices without security functions, it is probable that these vulnerabilities will be exploited to control these devices. This situation could bring about the need to deactivate vulnerable devices.

DRONEJACKING

Examples have been seen of attacks using a drone fitted with a set of cyber-attack tools to access the target's wireless networks.

UNCONTROLLED VULNERABILITY REVEAL

A large quantity of exploits for multiple technologies (Shadowbrokers, Vault 7,...) have been published in open sources followed by multiple attacks, with an underlying paradox: devices created to prevent an attacker from entering, that make penetration possible.

PRIVACY

Persistent cookie monitoring will continue to be of great value and it is likely that this situation will spread further in 2017, combined with widgets[54] that allow companies to track users' browsing habits.

ADVERTISING AS AN ATTACK TOOL

Advertising networks provide very complete user profiles (IP address, browsing and session start patterns). This type of data allows an attacker to discriminate or redirect their malware to the chosen targets. It should therefore be expected that in 2017, advanced attackers will consider creating/using an advertising network to reach their targets.

REDEFINING ICT INVESTMENTS

More investments will be made in mobile applications, migration to the cloud and detection and response to incidents in the coming financial years.

WHILST THE MANUFACTURERS OF IOT53 DEVICES CONTINUE PRODUCING DEVICES WITHOUT SECURITY FUNCTIONS, IT IS PROBABLE THAT THESE VULNERABILITIES WILL BE EXPLOITED

[53] Internet of Things.
[54] Programme or application similar to direct access but in addition to accessing the determined programme quickly, it also provides access to frequently used functions and different visual information. For example, on the desktop they are usually applications for the time, clock, search engines, etc.

VULNERABILITIES IN TECHNOLOGIES

It is estimated that the cost of zero day vulnerabilities for Apple and Microsoft technologies will increase considerably. During 2017, reuse is expected of vulnerabilities and tools published in different open sources such as Wikileaks.

MACHINE LEARNING FOR SOCIAL ENGINEERING ATTACKS

With an increasingly greater impact on education, business and research, the availability of machine learning tools has shortened the learning period and accessibility for everyone, including cyber-criminals.

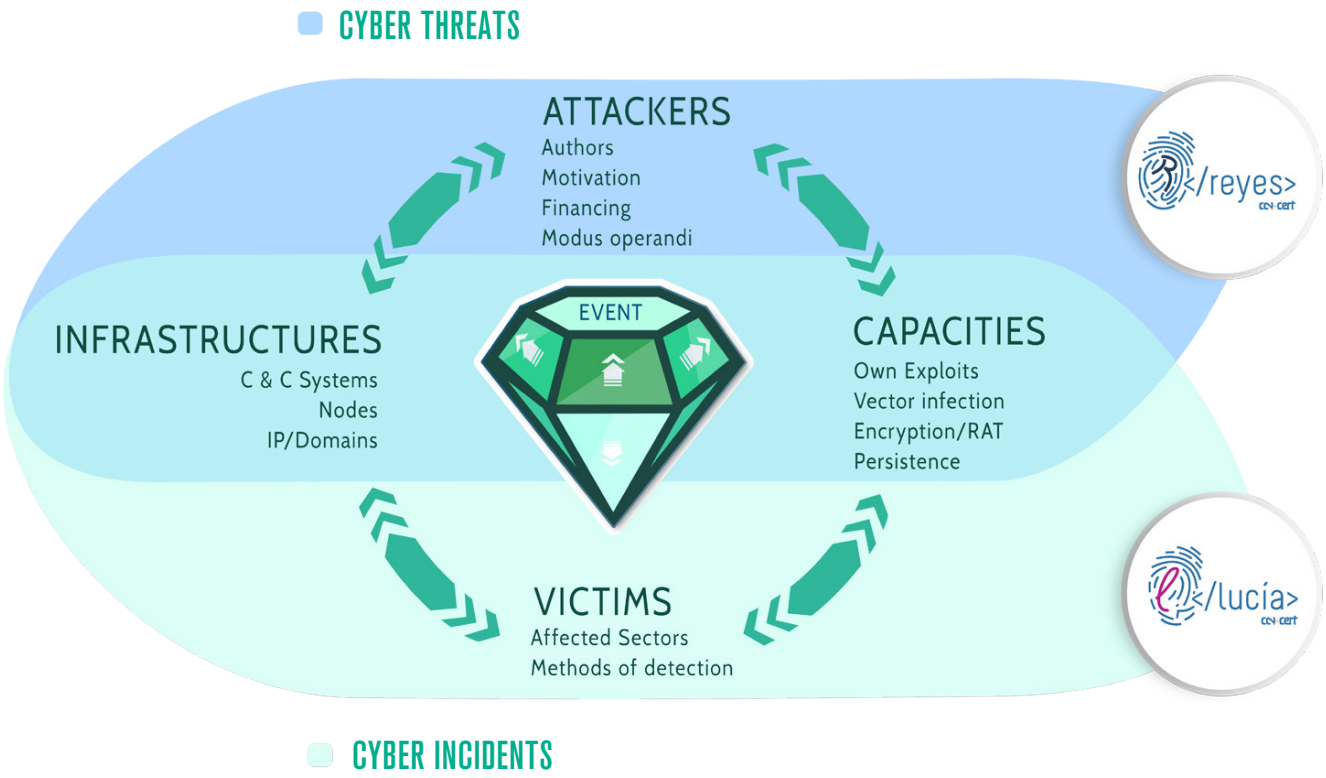
ATTACK ON PRIVACY AS A CYBER-ACTIVISM TOOL

In 2016, user awareness-raising grew on their "digital footprint" and the need to protect it with the same intensity as in real life and it will continue increasing in 2017. However, cyber-activists will continue to make the most of the volume of data that the user's equipment compiles such as personal information, searches, links, connections, page visits, use of products, etc. to then extract them, exhibiting this content publically for different purposes.

Sharing intelligence on threats shifts the balance of power from the opponents to the victims, whilst it interrupts the life cycle of an attack and it is more expensive for the threat agents

PROGRESS OF INTELLIGENCE EXCHANGE REGARDING THREATS

Sharing intelligence on threats shifts the balance of power from the opponents to the victims, whilst it interrupts the life cycle of an attack and it is more expensive for the threat agents.




CCN-CERT
centro criptológico nacional
WWW.CCN-CERT.CNI.ES
WWW.OC.CCN.CNI.ES
WWW.CCN.CNI.ES
You Tube