CCN-CERT IA-09/16

CYBER-THREATS 2015 / TRENDS 2016

EXECUTIVE SUMMARY

ccn-cert
centro criptológico nacional

TABLE OF CONTENTS

1. PROLOGUE

As in previous years, 2015 has seen an increase in the number, type and severity of attacks on information systems in Public Administrations and Governments, companies and institutions of strategic interest or any organisation important intellectual and industrial property assets and in general, against all types of entities and citizens.

Generalised use of electronic resources increases the attack surface area and consequently, its derived potential benefits, doubtlessly providing major motivation for attackers.

This has been shown, another year on, by the **National Cryptology Centre** when drawing up its now traditional Report on Cyber-threats and Trends[1]. This document includes an extract of this report and its main conclusions. This examines the impact, in Spain and outside its borders, of the most significant **threats and cyber-incidents** in 2015: cyber-espionage (by states and companies), **cyber-crime**, hacktivism[2] and, as a particular feature, what we have called the **cyber-jihad** (actions that can be attributed to groups with violent and radical tendencies within political Islam), Insiders or cyber-researchers.

The main document and this Executive Summary also look at the tools used by attackers (particularly referring to exploits[3], exploit-kits and malware) and **resilience** (the way in which the information systems have been able to deal with cyber-attacks and their **vulnerabilities** and the **measures** taken to strengthen them).

In addition, the complete Report compiles the main **trends for 2016** in terms of cyber-security and three major appendices that complete this overview: (Appendix A) most outstanding activity from the **National Cryptology Centre**; (Appendix B) **Mobile devices and communications** and (Appendix C) **Hacktivism in 2015**.

Most of the information in this report is the result of CCN-CERT's experience developing their responsibilities over 2015. In addition, other national and international, public and private documentary sources have been taken into account, working jointly with external organisations, professionals and members of academia.

[1] The complete Report (CCN-CERT IA-09/16 Cyber-threats 2015/Trends 2016) is available on https://www.ccn-cert.cni.es.

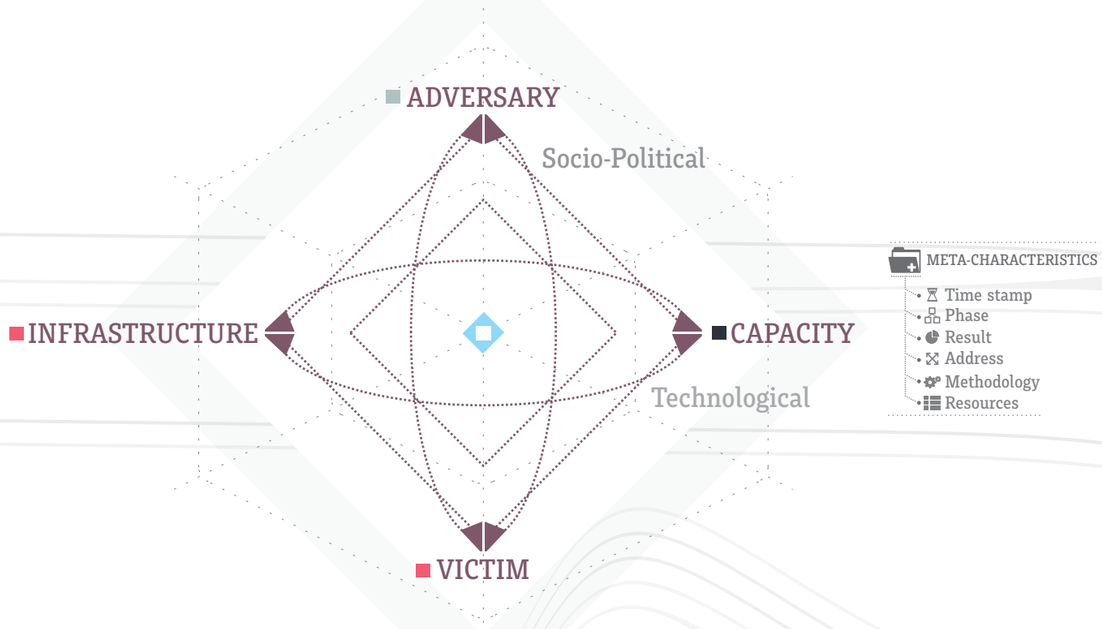
[2] Anti-social digital activism. Activists aim to take control of computers or websites to promote their cause, defend their political position or disrupt services, preventing or making it difficult to use them legitimately.

[3] An exploit is a program that exploits or makes the most of a 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.

2. THREAT FACTORS

1. Inappropriate **management of security updates (patches)** and use of **out of date software** in computers, mobile devices or central servers.
2. Lack of knowledge of the methods followed by **Social Engineering attacks**.
3. The occasionally long period in which manufacturers and service providers resolve **detected vulnerabilities**.
4. Attacks through **Advanced Persistent Threats (APT[4])** currently represent the most significant threat for companies and public organisations all over the world and they will remain as such in the future.
5. **Inter-connection of industrial environment systems**, particularly in the area of Critical Infrastructures[5], poses a problem for measures to be taken, especially as malware distribution periods (both fixed and mobile) are becoming increasingly short.
6. Attackers have become more professional making **threats more sophisticated**.
7. Availability of **attack tools** making it possible for new figures to appear on the scene.
8. **Business model** for the attackers, making it difficult to attribute the crime

One security scheme is compiled in the CCN-STIC 425 Guide Intelligence Cycle and Analysis of Intrusions, including two new meta-characteristics: **Socio-Political**, binding the Opponent to its Victim and **Technological**, that binds the Infrastructure with its Capacity, as represented in the following diagram:



2.1 TECHNOLOGICAL EVOLUTION AND CYBER-SECURITY

The most significant elements from 2015 stand out as:

- Software penetration (conflict between functional features and security)
- Mobile devices versus protecting information
- Compatibility versus information security
- Loss of trust in electronic services
- New areas of application for the IoT (Internet of Things[6])
- Separate networks requirement
- Medical equipment security
- Analogue alternatives do not exist
- Technological dependency on critical infrastructures (cyber-sabotage, financial sector, the media, other states, networks that manage critical infrastructures and others)

[4] Advanced Persistent Threat.
[5] See IA-04/16 Threats and Risk Analysis in Industrial Control Systems (ICS) by the CCN-CERT (https://www.ccn-cert.cni.es/informes/informes- ccn-cert-publicos/1381-ccn-cert-ia-04-16-amenazas-y-analisis-de-riesgos-en-sistemas-de-control-industrial-ics/file.html).
[6] Internet of Things (IoT).

3. CYBER-THREATS AND THEIR ACTORS

3.1 CYBER-ESPIONAGE / STATE FIGURES / PRIVATE ORGANISATIONS

As in previous years, during 2015 **cyber-espionage** (political or industrial) has been the greatest threat for countries, particularly focussing on information systems in industrial corporations, defence companies, high technology, the automotive sector, transport, research institutions and Public Administration.
The complexity, volume and impact of these attacks, usually via APTs, were similar to 2014. Evidence from 2015 helps us state that, on significant occasions, such actions have been carried out by **foreign Intelligence Services or Defence Departments** that continue to invest significant resources in defence and also attack. In addition, the States, to a varying extent, are the target for cyber-attacks originating in other States, interested in obtaining economic, geo-strategic or military information.
In addition, countries continue to make the most of international conflicts to carry out attacks (as seen in the crisis in the Ukraine).
In the case of industrial cyber-espionage, it is private organisations that act as attackers (occasionally also states). The profit derived from obtaining information illicitly and the intended damage to competitors' systems are good reasons for the private sector organisations to develop cyber-attacks.

- **MOST OUTSTANDING ATTACKS IN 2015.**

- In **Spain**, during 2015, the main information theft figures were the following groups: APT28, Snake, APT29 and Emissary Panda.
- Attack on German Bundestag building: the central systems in the Federal Parliament's internal network were compromised.

THIS TYPE OF ATTACK WILL CONTINUE TO RISE OVER THE NEXT FEW YEARS, ALSO BECOMING MORE SOPHSITICATED AND DANGEROUS.

3.2 CYBER-CRIME / CYBER-CRIMINALS

As **cyber-crime** becomes more professional and its main figures' internal organisation expands, it has reached the following level of attention in 2015. It is a steadily growing concern that techniques are becoming more sophisticated, new or renewed tools are more available (including providing criminal services on demand) and it is increasingly easy to complete these crimes 'cleanly'.
In 2015, as in 2014, it was demonstrated that cyber-criminal organisations are prepared to invest large amounts of money in organising their actions. In this way, what is known as "CaaS Cybercrime-As-A-Service" has penetrated further and become more professional, and it is possible to see some "competition" among actual cyber-criminals, leading them to provide their "customers" with an increasingly reliable "service".

- **ATAQUES MÁS DESTACADOS DE 2015:**

-**Carbanak Campaign** led against Eastern European financial entities where they managed to infect several banks via spearphishing. It has been estimated that the criminals were able to steal between 250 and 1,000 million dollars.
-**Corcow**: a targeted attack using intelligence techniques on financial entities (and their customers), particularly affecting Russia and the Ukraine.
-Attack on **Hacking Team**: extraction and publication of reports by this Italian company specialised in selling attack and monitoring tools and technology.
-**Home Depot** sustained a theft of 56 million credit and debit card numbers as well as 53 million customer email addresses.
- Theft of personal data from **Community Health Systems** (4.5 million patients), Anthem (80 million policyholders) and Premera (11 million policyholders in the United States).

THE BENEFITS OBTAINED AND EVER-EASIER ACCESS TO THE TOOLS TO PERFORM THIS TYPE OF ATTACK WILL LEAD TO AN INCREASE IN THE NUMBER OF CYBER-CRIMINALS AND CONSEQUENTLY ALSO THEIR CRIMES.

Category	Target	Type of Organization	Economic Impact
Non professional Hackers[7]	Security breaches	Individuals / Non-professional	Low
Crackers	Security software, copyright pirating	Individuals / Non-professional	Low
Piratas	Security, pirating of copyright	Individuals / Organised	Low
Attackers	IP theft, extortion	Criminal / Non-professional	High
"Black Hat" vulnerability explorers	ICT vulnerabilities	Individuals / Non-professional	Low in execution; high in consequences if the vulnerabilities are sold or relinquished to third parties
Malware professionals and script kiddies[8]	ICT vulnerabilities and ways of exploiting them	Individuals / Non-professional	Low in execution; high in consequences if the vulnerabilities are sold or relinquished to third parties
Carders[9] and money mules	Data theft	Organised	High
Extortioners	Botnets and malware as extortion tools	Individuals / Non-professionals / Organised	Medium
Phishing[10] and social engineering	Spam	Organised	High
"Black hat" fraud	Script attacks	Organised	High
Cheats	Online gaming	Individuals / Organised	Medium
"Click fraud"	Traps and access	Individuals / Organised	High
Hacktivists	Political attacks	Individuals / Organised	Low

[7] Hacker is someone that discovers the weaknesses in a computer or an information network or also someone with advanced knowledge. The term is contested by programmers who argue that anyone breaking into computers is called a "cracker" without differentiating between "Black hat" cyber-criminals and "White hat" IT security experts; finally there are "Grey hats" referring to a talented hacker that sometimes acts illegally although with good intentions. However some controversy still surrounds these terms. https://wikipedia.org/wiki/Hacker_seguridad_informatica.

[8] These are people with limited knowledge using third party tools to perform their actions as a challenge often without being fully aware of the consequences.

[9] Carders. Type of hacker who traffics credit cards.

[10] Phishing. Identity theft. This consists of sending emails that seem to be reliable but usually lead to false websites collecting confidential data from the victims.

3.3 CYBER-TERRORISM / TERRORIST GROUPS

Although the potential danger of actions that can be attributed to cyber-terrorism continue to grow, it cannot be stated that they currently represent a serious threat, particularly due to the limited technical abilities demonstrated in their deployment.

3.4 HACKTIVISM / HACKTIVISTS[11]

Persons or groups, organised to a varying extent, working in cyberspace, generally for ideological reasons. Over the last few years, their cyber-attacks (defacing websites, DDoS attacks[12] or removal of confidential data from their targets) claimed to be a response to measures adopted by governments that they considered an afront to Internet freedom. In general, the year was characterised by a smaller number of hacktivist operations compared to previous years.

- **MOST OUTSTANDING ATTACKS IN 2015:**

  -Confrontation between groups revolving around **'Anonymous'**, on the one hand, against hacktivist identities that support or show sympathy for the jihadist group **'Daesh'**[13].
  -After the attack on the French magazine **Charlie Hebdo**, there were several defacement incidents on French websites. The Anonymous operation called #OpCharlieHebdo led to the reaction known as #OpFrance in which tens of French websites displayed Islamic texts.
  -In **Latin America**, an offensive was maintained against Nicolás Maduro's government (Venezuela) and several anti-governmental operations in Mexico.
  -En España se caracteriza por una baja densidad con la excepción de 'La 9ª Compañía de Anonymous'.

[11] Appendix C of the complete CCN-CERT IA-09/16 Threat report contains a study on Hacktivism in 2015.

[12] Distributed Denial of Service (DDoS) Attack that denies service, by using multiple points of attack simultaneously.

[13] Dulat Aslamiyah Eraq wa Sham (Daesh) Islamic State of Iraq and Sham (ISIS). Sham is a zone including all of Syria and part of the Lebanon.

3.5 CYBER-JIHAD / JIHADIST GROUPS

A new threat appeared in 2015: cyber-jihad, using terrorism methods, procedures and tools, hactivism and cyber-war, is up and coming and represents one of the greatest threats that Western society will face over the next few years.
The significant lines of funding for these groups (under the protection of Daesh) make it possible to acquire exact knowledge and tools to develop cyber-attacks or counter-act them.
For the time being, its attacks have been limited to defacing websites, small-scale DDoS attacks or, more commonly, use of Internet and social networks to broadcast propaganda or for recruitment and radicalisation, activities that do not require great knowledge or infrastructure.

- **MOST OUTSTANDING ATTACKS IN 2015.**

  - Use of malware (for example in Syria, cyber-attacks were detected to get data on the positions of local targets).
  - Attack on websites
  - Instructions for using a remote access tool (RAT[14]) to control equipment.
  - Attacks on social networks to obtain information

  Phishing attacks to get credit card data and obtain information.
  -The **CyberCaliphate** group affiliated to Daesh attacked and took over US Central Command Twitter and Youtube accounts.

WE HAVE ONLY SEEN THE BEGINNING OF WHAT THE CYBER-JIHAD IS CAPABLE. WE CAN EXPECT MORE NUMEROUS, MORE SOPHISTICATED AND MORE DESTRUCTIVE ATTACKS IN THE NEXT FEW YEARS IF THE CURRENT SITUATION WITH ISIS GOES ON.

3.6 CIBER-VANDALISM/VANDALS AND SCRIPT KIDDIES

Cybervandal is the name given to individuals with significant technical knowledge, who carry out their actions simply to show the public that they can do it.
In turn, script kiddies are people with limited knowledge using third party-constructed tools to perform their actions as a challenge often without being fully aware of their consequences. Despite media coverage of cyber-vandalism actions during 2015, this is not a serious threat to the interests of organisations.

- **MOST OUTSTANDING ATTACKS IN 2015.**

  - Defacing the Malaysian Airlines website

LOOKING AHEAD, NO SUBSTANTIAL CHANGES CAN BE ENVISAGED IN HOW THESE FIGURES BEHAVE.

[14] **RAT.** *Remote Access Tools.*

3.7 INSIDERS

Insiders are people who are or who have been working for an organisation (employees or ex-employees, co-workers and suppliers) who cause important security breaches. In some cases, information extraction is detected for economic or political reasons; in other cases, it comes down to certain people's negligence or spite.
In several of the cyber-incidents that took place in 2015, it could be seen that some employees had planted sensitive information in private servers, without taking the right security measures.

- **MOST OUTSTANDING ATTACKS IN 2015**

  - An employee at an **insurance company** put data regarding claims by 27,000 policyholders on to a private server to test a piece of software.
  - Case of AMS-IX (Dutch Internet exchange company): an error during maintenance work crashed the platform and web services were not available for ten minutes which, although short, had international repercussions, given the size of the system that was affected.

INSIDERS HAVE ONLY REPRESENTED A SMALL PERCENTAGE OF THE THREAT ACTORS (LESS THAN 15%).

3.8 CYBER-RESEARCHERS

They seek out vulnerabilities in ICT environments in order to verify protection in the systems they are investigating. In order to inform companies, the results of their investigations are frequently published in the media with a dual positive and negative effect. Negatively, it is clear that publicising any vulnerability means that the identified systems are more vulnerable to external attacks, making life easier for attackers as they can benefit from the results of the investigations. There have even been cases of cyber-researchers accused of running extortion rackets on the entities being investigated.

THREAT ACTORS

	ORIGIN OF THE THREAT	REASON	KNOWLEDGE LEVEL
1	States	Improve their geopolitical or strategic position. Cyber-terrorism as a false flag. Counter-terrorism or national security protection.	HIGH
2	Cyber-criminals	Economic benefit (direct or indirect).	HIGH>MEDIUM
3	Hacktivists	Move closer to their ideological targets.	MEDIUM
4	Jihadist groups	Broadcast their ideology.	LOW > MEDIUM
5	Terrorist Groups	Make changes in society by using terror, or influence political decision-making. High impact targets.	MEDIUM > LOW
6	Cyber-vandals	Pranks. Looking for a challenge.	LOW
7	Insiders	Revenge or economic or ideological benefits (occasionally run from the outside).	HIGH > LOW
8	Cyber-researchers	Revealing weaknesses (and their own profile)	MEDIUM
9	Private organisations	Obtain or sell valuable information.	HIGH > LOW

OBJECTIVES

PUBLIC SECTOR	PRIVATE SECTOR	CITIZENS
Political cyber-espionage	Economic cyber-espionage	Instrumental cyber-espionage
Offensive cyber-skills	Offensive cyber-skills	
Theft, publication or sale of information	Theft, publication or sale of information	Theft, publication or sale of information
Manipulating information	Manipulating information	Manipulating information
Disrupting systems	Disrupting systems	Disrupting systems
Taking control of systems	Taking control of systems	Taking control of systems
Theft and publication of stolen information	Theft and publication of stolen information	
Defacing	Defacing	
Disrupting systems	Disrupting systems	
Taking control of systems	Taking control of systems	
Disrupting systems / Taking control	Disrupting systems / Taking control	Propaganda and recruitment
Desfiguraciones	Desfiguraciones	
Disrupting systems / Taking control	Disrupting systems / Taking control	
Information theft	Information theft	Information theft
Disrupting systems	Disrupting systems	
Theft, publication or sale of information	Theft, publication or sale of information	
Disrupting systems	Disrupting systems	
Reception and publication of information	Reception and publication of information	
	Information theft (industrial espionage)	Use/abuse or resale of customer or general public information

LOW

- No new threats or trends have been observed, or
- There are sufficient measures to neutralise the threat, or
- There have been no particularly significant incidents in the period being analysed.

MEDIUM

- New threats or trends have been noted, or
- There are (partial) measures to neutralise the threat, or
- The incidents detected have not been particularly significant.

HIGH

- The threats or their tendency have significantly increased.
- The measures taken have a very limited effect, so the threat remains.
- The detected incidents have been particularly significant.

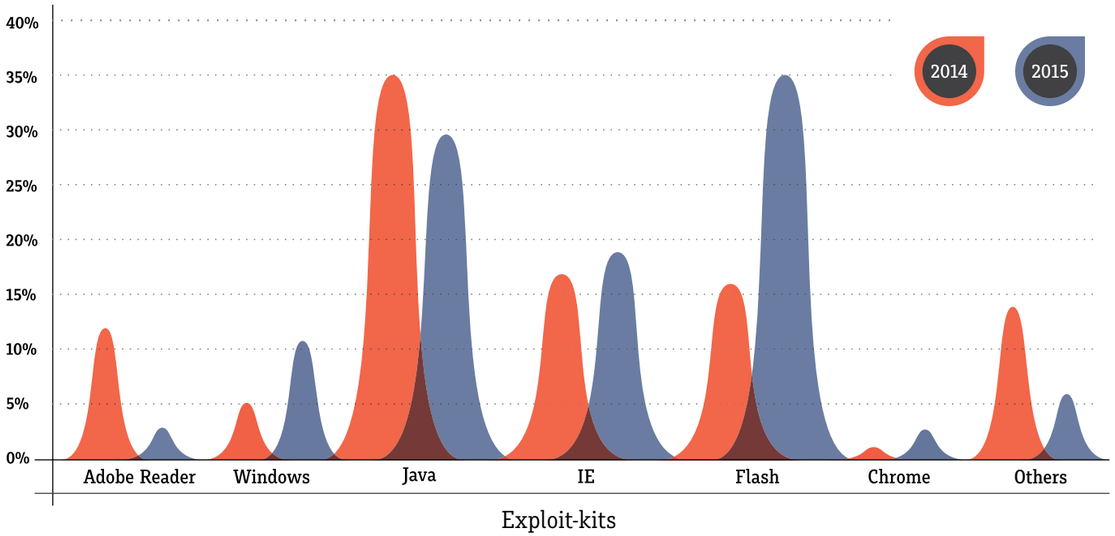
4. TOOLS USED BY ATTACKERS

4.1 TOOLS BUILT FOR OTHER PURPOSES

Attackers are making massive use of tools developed for other purposes, such as monitoring systems or carrying out penetration tests. Some examples of this are SaaS services (Software as a Service or booter services) that allow attackers to run Distributed Denial of Service attacks (DDoS) through a website.
As another example, the people behind the attack campaigns known as Cleaver, Hurricane Panda and Anunak/Carbanak used the MimiKatz tool (originally designed to recover passwords, Kerberos tickets and summary functions (hashes[15]) for a Windows system memory) to obtain login data for a Windows network and manage to access the systems in the network.

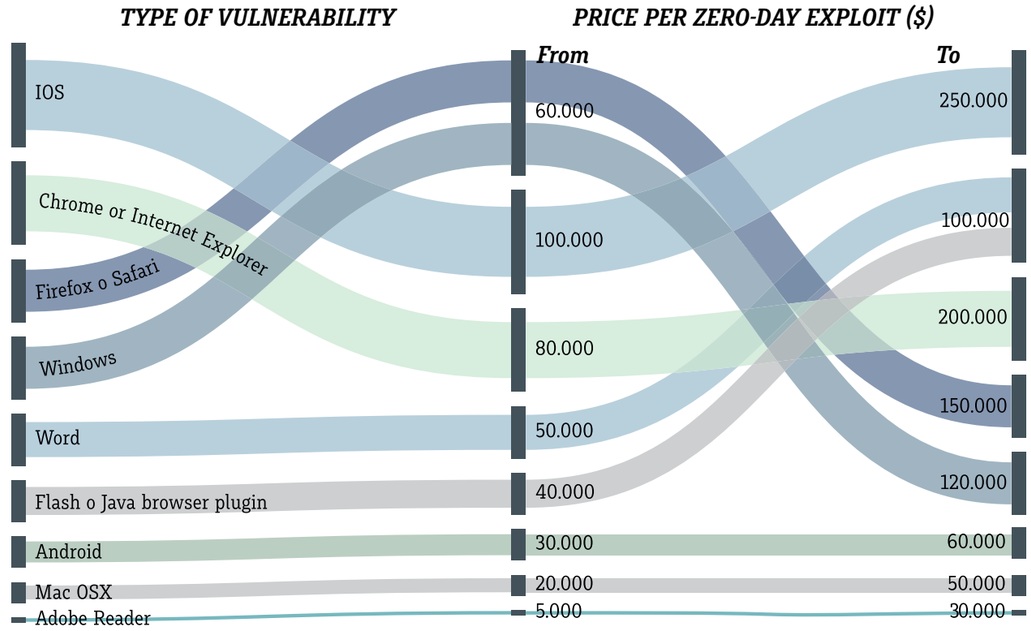
4.2 EXPLOITS, EXPLOIT-KITS AND EXPLOIT DRIVE-BY

The tools most used to run attacks (as over the last few years) are exploits, exploit-kits and Drive-By exploits (this means that the victim's system is infected with malware when they enter a particularly website, usually distributed via advertising banners). Windows and the PHP[16] applications (plug-ins[17] for Wordpress[18] and Joomla, above all) continue to be the focus for exploits, although substantially less were brought out in 2015. However, the most usual exploit-kits focus on Adobe Flash, as shown on the graph below[19]. In the first term of 2015, eight new exploits - packaged as exploit-kits - were sent out to exploit vulnerabilities in this program. five of them were zero-day.



[15] *The cryptographic hashing function is a (mathematical) function in which a known algorithm takes a message of an arbitrary length as an input and produces a result with a fixed length (generally known as "hash code" or "message summary"). CCN-STIC 401 Glossary of Terms.*
[16] *PHP Hypertext Preprocessor is an open code language that is highly appropriate for web content development.*
[17] *A plugin or complement is an application that is related to another to give it a new and generally very specific function. This additional application is run by the main application and they interact via the API (Application Programming Interface. Programming interface for applications). http://es.wikipedia.org/wiki/Complemento_(informática).*
18 Wordpress and Joomla are content creation systems for websites or Content Management Systems (CMS).
19 http://exploit-db.com/.

These tools are not only used on suspicious websites but also on other absolutely legitimate, non suspect sites.
Watering Hole[20] attacks are also very common; this is the usual mechanism to started targeted attacks particularly when the infected websites are frequently visited by people from the victim-organisation.
The following diagram shows the price of the different types of exploits-kit, depending on the vulnerabilities being attacked[21].



THE LEVEL OF THREATS HAS GROWN CONSIDERABLY COMPARED TO 2014 AND DUE TO MASSIVE USE OF DRIVE-BY EXPLOITS AND EXPLOIT-KITS. MOST RECENT INVESTIGATIONS SHOW THAT CYBER-ATTACKERS ARE INVESTING IN DEVELOPMENT OF NEW EXPLOITS AND SEARCHING FOR NEW VULNERABILITIES.

[20] *Water hole. Strategy where a particular group is attacked (organisation, sector or region) in three phases:*
1. Guess/observe the websites that the group often uses.
2. Infect one or more of them with malware.
3. One of the members is infected. Its efficacy is based on users trusting websites that they often visit. It is even effective with aware groups that tend to be resistant to spear phishing and other forms of phishing. CCN-STIC 401 Glossary of Terms.
[21] *McAfee Labs: Threats Report (Aug., 2015).*

4.3 MALWARE[22] / RANSOMWARE[23] / CRYPTOWARE

This represents one of the most frequently used tools to carry out the infections preceding attacks. The total number of malware versions for PC currently stands over **439 million** (affecting **Windows the most**), whilst the amount of malware on mobile platforms continues to grow incessantly (**96% of this malware affects the Android operating system**).

The variety of samples of Ransomware or Cryptoware (Critroni, CryptoFortress, CTB-Locker, Cryptolocker and Cryptowall) has not stopped growing and its distribution methods vary: drive-by[24] exploits, emails with links to malware programs, hosting in Microsoft Office product macros, etc. During 2015 Cryptoware infections have been seen in a whole host of public and private organisations, of all sizes, including health institutions and SMEs.

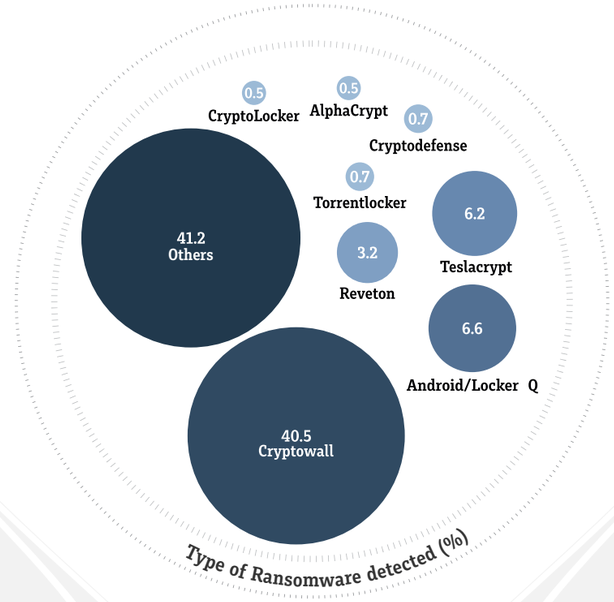
In fact, the Dell SecureWorks company has reported that the Cryptowall variant alone infected over 625,000 computer systems all over the world in just five months.

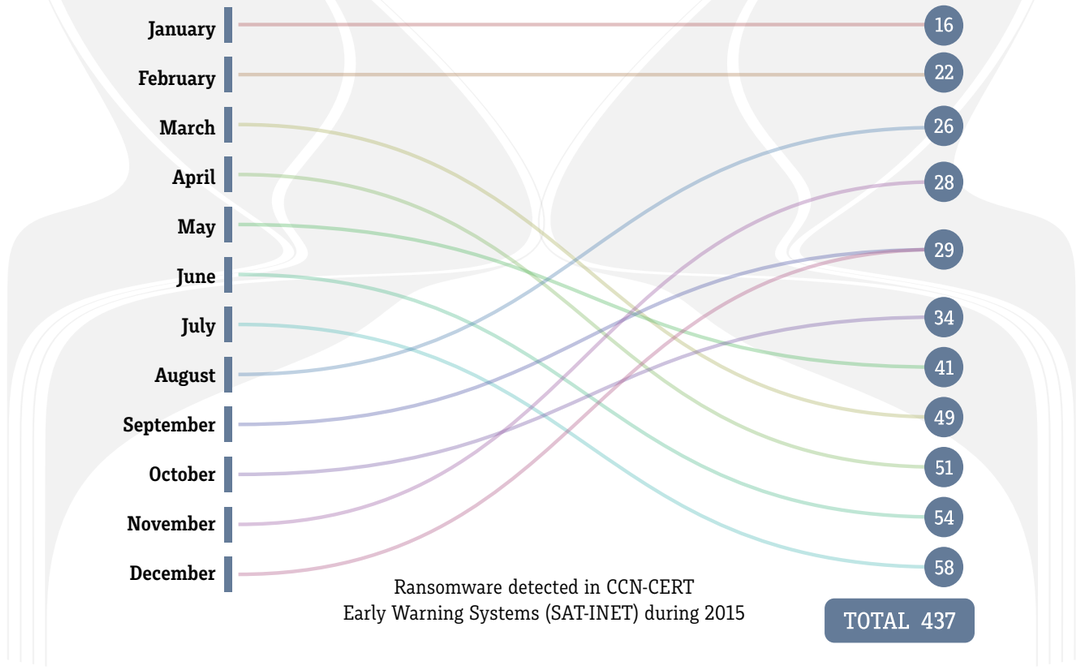
As an example, we can quote the Coinvault case, an infection investigated jointly by the Dutch Police and Kaspersky Lab where it was determined that approximately 1.5% of victims paid the ransom.

It is logical that new variants will appear, given that it has been calculated that a certain percentage of the victims pay the ransom, therefore encouraging criminals to continuously improve their tools and their targets: major companies, SMEs and end users; new operating systems and new devices (including mobile devices).

Código dañino	Nivel de amenaza	Función primaria	Vector de infección primario	Nominaciones/ Variantes	
Cryptolocker	High	Ransomware	Email Attachment		▲
DarkComet	High	RAT	Exploit Kit	Fynlaski, Fynlos, Kradernok, DarkKornet	▲
Dridex	High	Data Stealer	Email Attachment (Word macros)	Bugat, Feodo, Cridex	▲
Zeus	High	Data Stealer	Exploit Kit	Zbot, Garneover (GOZ)	◆
Blackshades	High	RAT	Exploit Kit		▲
Citadel	High	Data Stealer	Exploit Kit		▲
SpyEye	High	Data Stealer	Droper		▲
CTB-Locker	Medium	Ransomware	Email Attachment (.zip)	Critroni	▲
Dyre	Medium	Data Stealer	Dropper (Upatre)	Dyreza	▲
Tinba	Medium	Data Stealer	Exploit Kit	Tyrrybanker, Zusy	▲
Carberp	Medium	Data Stealer	Exploit Kit		◆
Shylock	Medium	Data Stealer	Exploit Kit	Caphaw	◆
Ice IX	Medium	Data Stealer	Exploit Kit		▼
Torpig	Medium	Data Stealer	Exploit Kit	Sinowal, Anserin	▼

Malware's trend in terms of risk level (Europol)





[22] *Software that carries out undesirable, unwanted or damaging functions in an infected system.*

[23] *This consists of hijacking the computer (making it impossible to use it) or encrypting its files (Cryptoware) promising to release them after a certin amount of money has been paid as a ransom.*

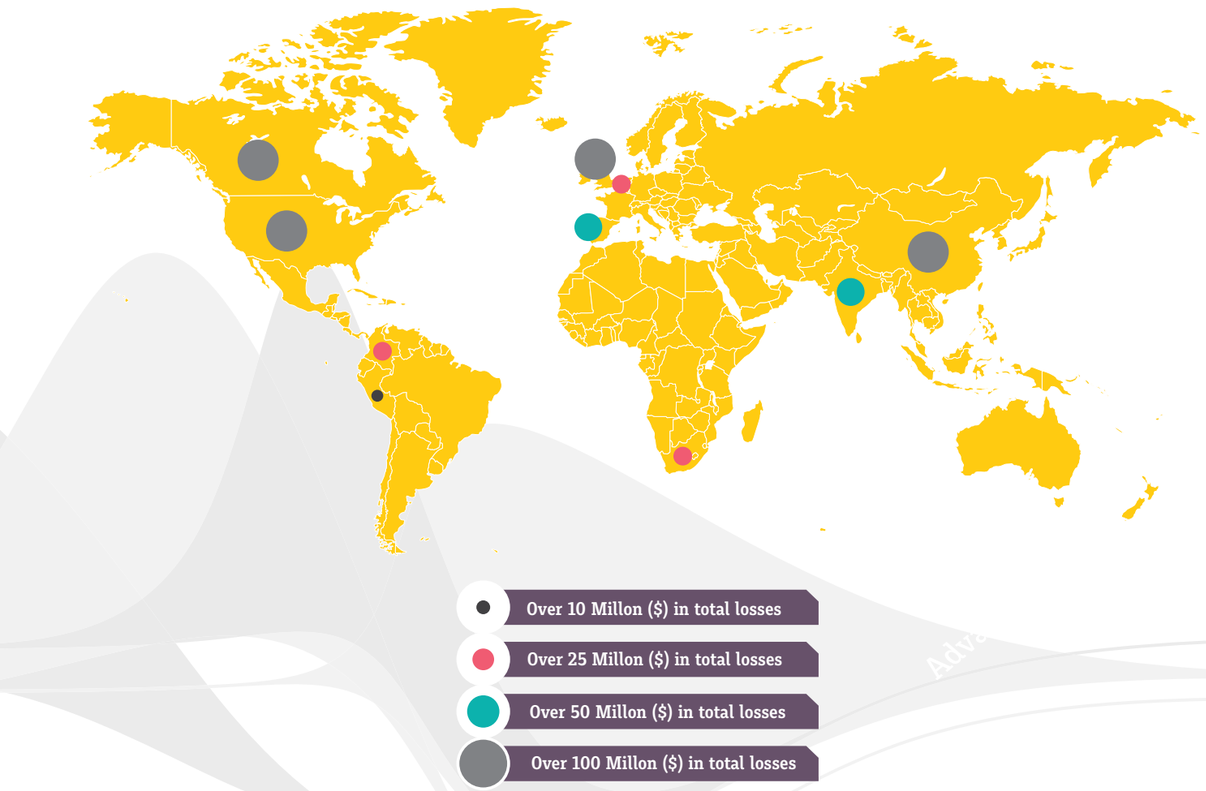
[24] *Attack mechanisms that can infect the victim's system with malware when they access a certain website that has been previously infected. The code exploits vulnerabilities in the Web browsers, their complements or the actual operating system.*

4.4 SPAM AND PHISHING / SPEARPHISHING

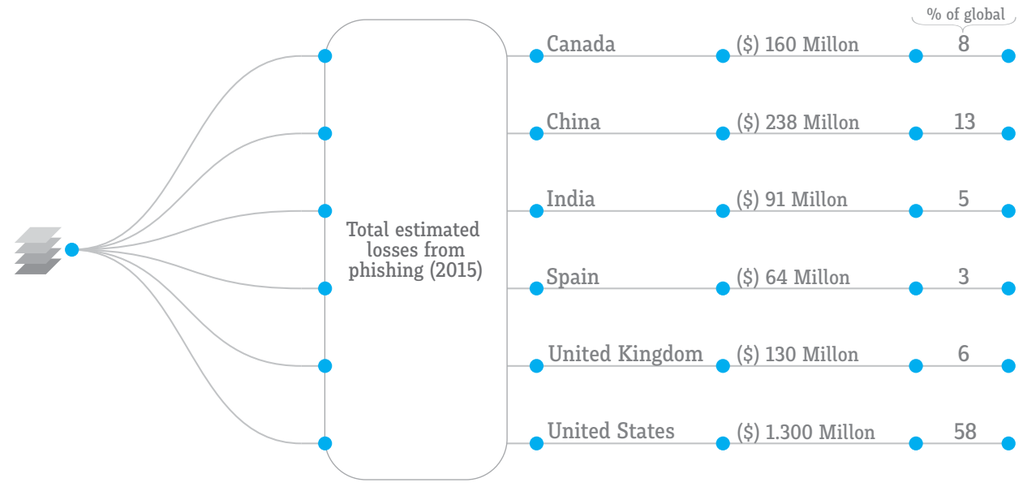
This term can be subdivided into several types: traditional spam, malware spam and phishing messages. After a rise in 2014, spam dropped in 2015 to approximately 30% of the volume in the previous year. However, it was the more traditional type that increased significantly as it holds malware, using email addresses obtained in other infected systems that in turn become the main source of infections. Many samples of malware were found in the **Geodo family.** It was also seen **that they are being distributed increasingly professionally**. Use of fraud and identity theft techniques, the use of individual versions of the malware and the time schedule control of downloading, are tools intended to infect the user's system without the anti-virus software being able to detect it.

Regarding phishing and spearphishing (mail sent from someone you know), these are the most-used tools to start personalised attacks (and also the most feared) and for cyber-espionage

The following diagram shows countries where the greatest losses have taken place due to phishing[25].



[25] *Source: EMC-RSA http://spain.emc.com/microsites/rsa/phishing/index.htm*



4.5 BOTNETS[26]

Botnets are used massively by cyber-criminals in order to steal information, commit online bank fraud, attack computer system availability or send spam. As cyber-crimes become more professional, it is relatively easy and cheap for non specialists to run a botnet. Consequently, the current danger level remains critical and the trend is rising.

- In February 2015, a particularly significant botnet, Ramnit, was deactivated. It had caused approximately 3.2 million infections throughout the world.

- Thanks to its market share, **the systems mainly compromised by botnets are Windows**, although attackers are bearing down hard on Mac OS X and Android systems.

- There is still a persistent trend towards damaging use of **compromised web servers** to operate **C&C servers**[27] (Command and Control).

4.6 DDOS ATTACKS

Although DDoS attacks are still occurring, the damage that they have been able to cause is quantitatively less than in 2014 and their duration has dropped as well (the majority last between 30 minutes and one hour). However, the maximum volume of the attacks is increasing and closing in on 400 Gbps, where the average bandwidth for a DDoS attack is between 8 and 12 Gbps. So, for example, an Indian network provider was hit by an attack of this type with a peak of 334 Gbps. In 2015, sectors reporting new attacks of this type included education institutions or public transport services. However, their favourite targets are the games industry (35.3% of attacks) and the software/technology industry (25.2% of attacks).

There is also evidence that **Booter** services are being used that allow an attack to be made without any great technical knowledge (DDoS-as-a-Service) and what are known as **reflection attacks** using public access servers to reinforce it. This means that operators of this type of server have become (involuntary) co-perpetrators of the damaging actions.

[26] *Robot Network"(network of robots or zombies) Network of equipment infected by a remote attacker. The equipment is at its mercy when it wishes to launch a massive attack such as sending spam or [distributed] denial of service. CCN-STIC 401 Glossary of Terms.*

[27] *Command and Control.*

4.7 OBFUSCATION

Obfuscation refers to any activity carried out by attackers to leave the least possible trace of their actions in order to make it difficult to identify them or the methodology they follow, etc. One example of this is the use of legitimate services to distribute malware (there are examples in Dropbox, Pinterest, Reddit, Google Docs. Gmail, etc.).

4.8 SOCIAL ENGINEERING

This is one of the favourite lines of a attack from threat actors, tricking victims so that they install malware programs, all to be able to access information from the system under attack.

In this case, attackers have the chance to quickly and anonymously obtain personal information from their victims over the social networks; this is usually the first phase of the directed attacks (attempting to guess the victim's password, generating trust, personalised spearphishing emails).

The "False President" attack was very lucrative in the business world in 2015 (the attacker pretends to be a director from the organisation, asking an employee to urgently transfer some money for a secret project).

4.9 WATERING HOLE

This is usually the second option for attackers when a spearphishing attack is not successful. Attackers make the most of a known vulnerability and by prior-infecting a website frequently visited by the victims with malware.

The use of malware advertising messages has also increased (known as **malvertising**).

4.10 JAVASCRIPT LIBRARIES

Including Javascript and other libraries in a website led to a significant series of incidents in 2015. Frequently, the website developers involve a library directly instead of copying it to its own website. If an attacker manages to manipulate a library, they will be able to attack all the websites that contain a dynamic call to it.

4.11 MACROS AS AN ATTACK VECTOR

Several recent families of malware, such as **Dridex, Vawtrak and Cryptodefense** are clear examples of malware that is installed in end user systems through macros.

4.12 WIRELESS ROUTERS

A compromised individual or SME router can, for example, be used to adjust the DNS (Domain Name System) configuration and redirect to infected websites, form part of a botnet, propagate malware, penetrate a network or manipulate traffic without being detected

4.13 IDENTITY THEFT

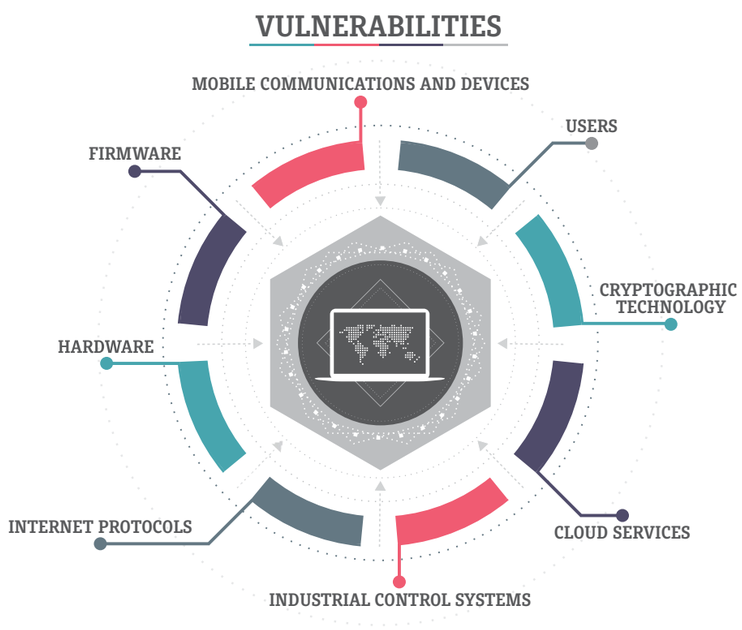
Usually, identity theft (user, password or other data) is carried out using social engineering mechanisms, installing malware in the victim's systems (there are even programs designed just for this type of theft) or through prior attacks on websites.

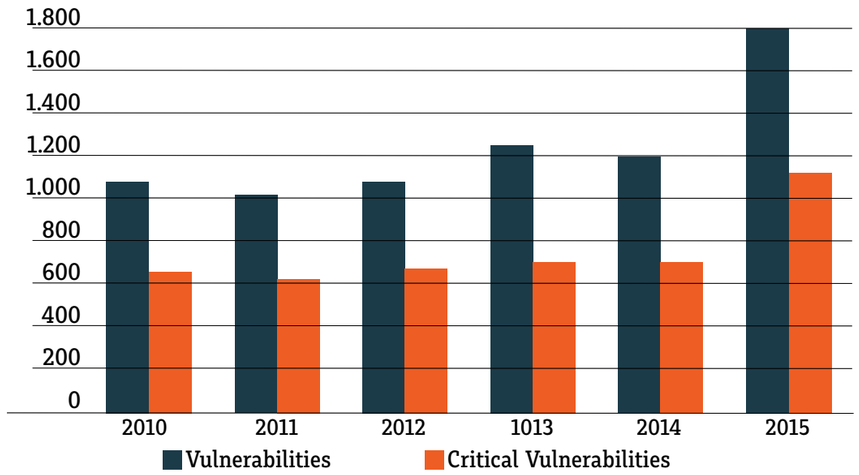
Consequently, attackers can obtain a direct and healthy profit by selling stolen identities so this activity will remain a permanent threat over the next few years.

5. RESILIENCE[28]

5.1 VULNERABILITIES

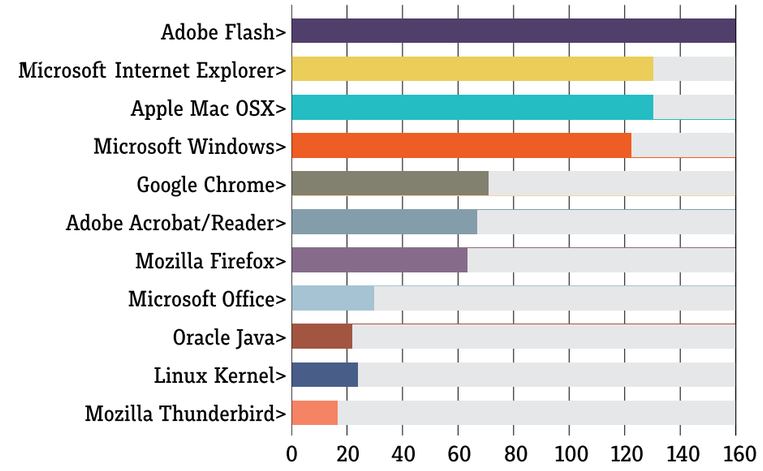
Although users are a source of vulnerabilities (the case of phishing is a good example), **software** continues to be the most problematic element. So, the **number of critical vulnerabilities** in 2015 in standard ICT products **has increased considerably** compared to figures from the previous year.





[28] Capacity of systems to continue operating despite under-going a cyber-attack, even in a downgraded or weakened state. In addition, it includes the capacity to promptly restore its essential functions after an attack. CCN-STIC 401 Glossary of Terms.

At the end of September 2015, **847 critical vulnerabilities had been identified from the 11 software products** shown in the diagram below



Alternately, on the **CCN-CERT website, in 2015 a total of 5,099 vulnerabilities were published corresponding to 10 manufacturers** (Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse Linux, Debian, IBM, Apple and Symantec), compared to 3,346 from 2014

Other types of vulnerabilities detected were:

- **Firmware**[29]: after infection, it is almost impossible to detect the attack in the actual device (USB memory sticks, hard disks, computers, etc.).
- **Hardware**: physical access to the equipment is required for this type of attack. They are very difficult to detect (if not impossible), as they might manipulate the chip, keyboard, USB, etc. The best protection can only be achieved by means of producing components in secure environments and distributing them by means of a secure supply chain.
- **User**: more than half all successful cyber-attacks are user-related (IBM study), with non authorised access as the main reason.
- **Cloud services**: owner awareness in terms of ICT security is still lacking. Suppliers have not made great investments in this respect.
- **Cryptographic technology**: Current cryptographic algorithms can be considered as secure - apart from RC4 whose use is not recommended in TLS[30]. Its prior requirement is reasonable lengths for parameters and passwords.
- **Internet protocols**: often the Internet architecture's structural vulnerabilities are based on design decisions made in the past that are difficult to undo. The use of HTTPS[31] offers advantages for all types of web services, preventing unwanted monitoring of the user's browsing behaviour.
- **Communications and mobile devices**: they represent certain risks due to fast software development (with no guarantees that vulnerabilities have been updated correctly), storing information in the cloud, connection to public access without encryption (**hotspots**), geo-location and the chance of interception.

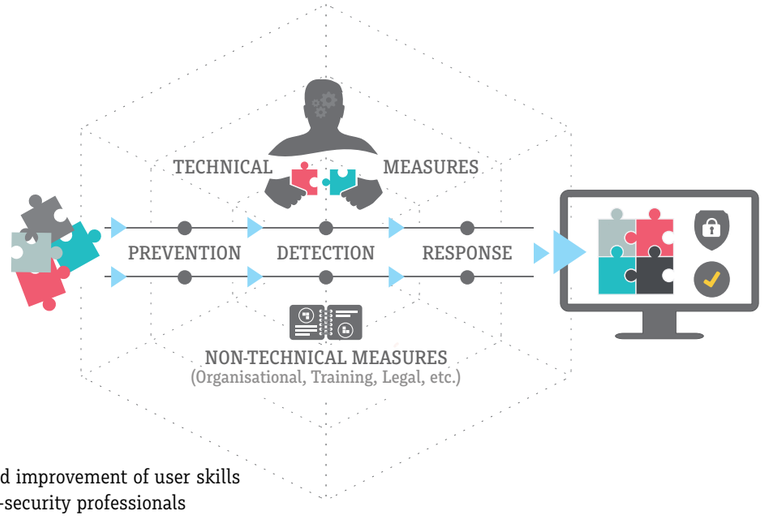
[29] Firmware works as the crossroads between the instructions (software) that enter the device from the outside and the different electronic parts (hardware).
[30] TLS. Transport Layer Security. Encryption protocol that allows secure exchange of information between two extremes.
[31] Secure Hyper Text Transfer Protocol. Secure hypertext transfer protocol, usually used in web browsing.

In the same way, there is an important risk in applications (Apps) and in the professional use of private devices (BYOD[32]).

- **Industrial Control Systems:** Growing use of standard ICT components means that they are exposed to the same risks as any other organisation. In 2015 there have been cases of generalised faults in complete production systems from Ransomware, spyware or spearphishing. Even North American researchers used the Internet for wireless penetration of an information system and maintenance of a 4×4 vehicle through a vulnerability.

5.2 MEASURES

This section examines the measures that have contributed most significantly in 2015 to increasing the resilience of the information systems on which they are applied and as a consequence, of the affected organisations.



PERSONAL

- Awareness-raising and improvement of user skills
- Qualification of cyber-security professionals
- Responsible dissemination
- Cooperation between different figures

TECHNOLOGIES

- Authentication of two factors
- Use of cryptography: TLS and DNSSEC protocols[33]
- Capacity for detection
- Adaptation of security measures contemplated in Appendix II of the National Security Scheme (ENS)[34] especially for Public Administrations.
- Efficient deployment of capacities, including cyber-threat exchange tools such as REYES developed by the CCN-CERT.
- Cyber-security exercises

ciberseguridad

REGULATORY

- Harmonisation of European legislation
- Legal instruments that allow online use of investigation methods.
- Application of the European Directive on attacks against information systems

[32] *BYOD. Bring your own device.*
[33] *DNSSEC. Domain Name System (DNS) Security Extensions. This constitutes a form of cryptographic security for the DNS protocol.*
[34] *RD 3/2010, dated 8th January, regulating the National Security Scheme (ENS), modified by the RD 951/2015 dated 23rd October.*

- TEN COMMANDMENTS OF CYBER-SECURITY -

01 **Increase network and system surveillance capability.**
Appropriate cyber-security staff.

02 **Monitoring and correlation of events**
Centralised record management tools (network traffic, remote users, administration passwords, etc.).

03 **Restrictive Corporate Security Policy.**
With more restrictive user grant, practical approximation of services in the cloud and use of devices and equipment owned by the user.

04 **Setting configurations.**
In all corporate network components, including mobile device and laptops.

05 **Use of certified and trusted products, equipment and services.**
Accredited networks and systems for handling sensitive or classified.

06 **Automate and increase the information exchange.**
Reciprocal work with other organisations and Information Security Incident Response Teams (CERT).

07 **Management should be committed to cyber-security.**
Management should be the first to accept the risk and promote these policies.

08 **Training and awareness raising at user level.**
Every level of the organization (management, employees and professionals) shoul be aware of the riskt and act acordingly.

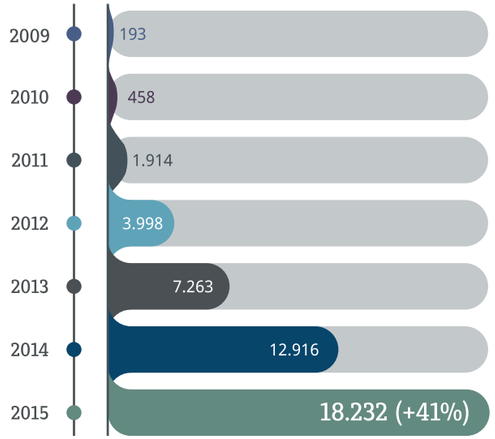
09 **Compliance with legislation.**
Adaptation to them and to the different cyber-security standards.

10 **WORKING AS IF YOU were COMPROMISED.**
Assume that the systems are already compromised or will be soon and protect critical assets.

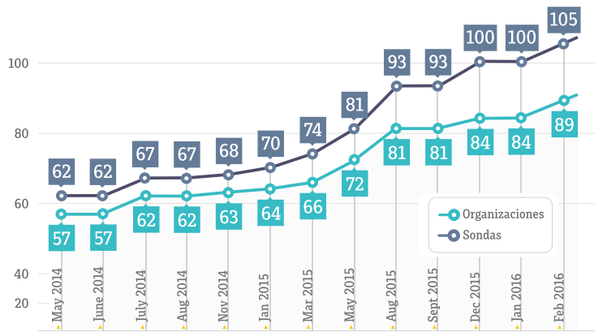
6. CCN ACTIVITY

6.1 INCIDENT MANAGEMENT IN 2015

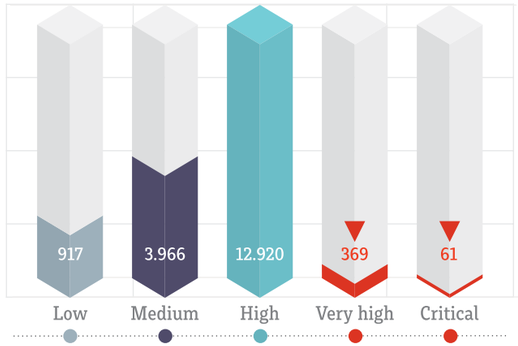
During 2015, the CCN-CERT managed a total of **18,232 incidents** detected in Public Administrations and in companies of strategic interest. This figure represents a **41.45% increase** on 2014.



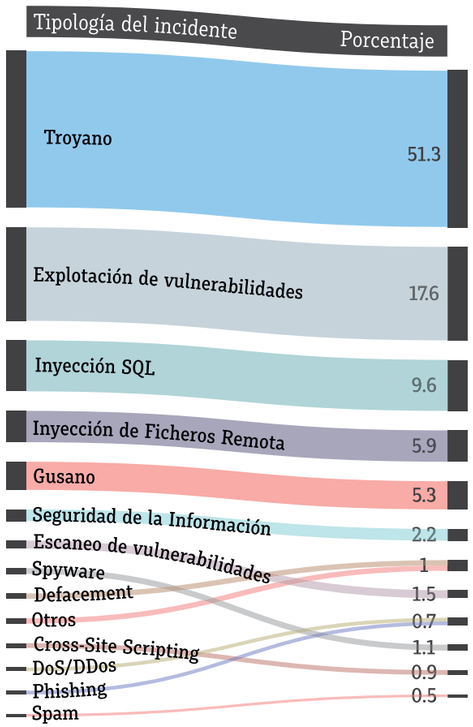
Evolution of Incidents managed by the CCN-CERT



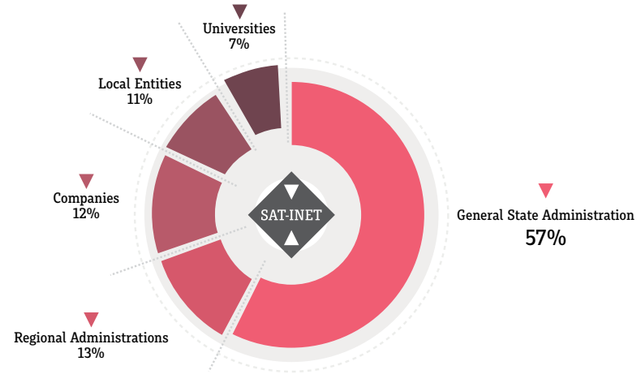
Organisations signed up to the CCN-CERT Internet Early Warning System (and the installed probes)

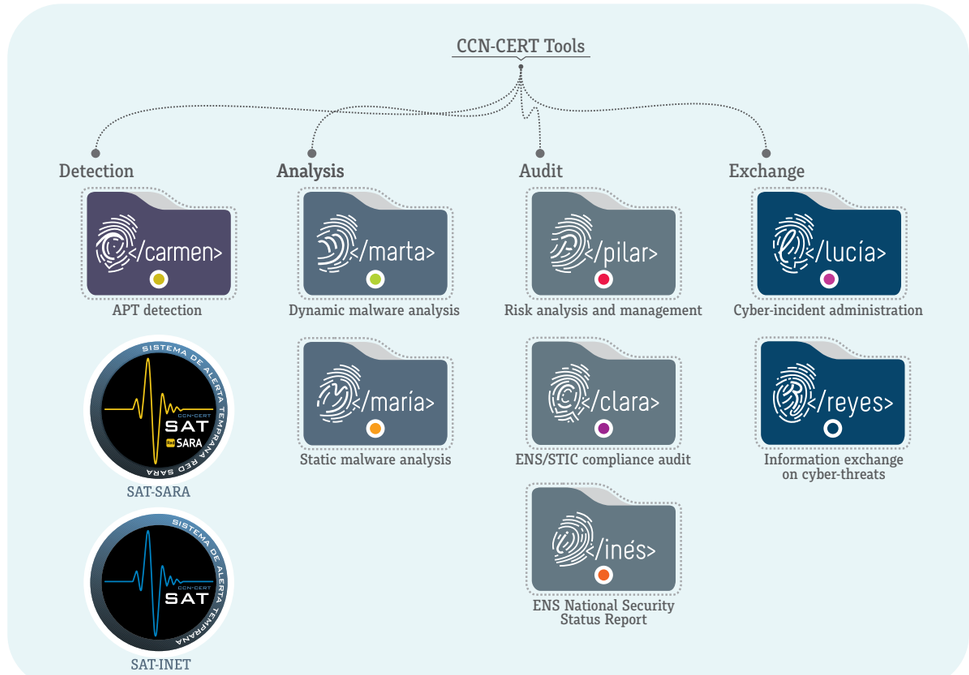


Out of the total incidents, **430** were classified by the National Governmental CERT team of experts as a **very high or critical** risk level; in other words, it was stated that the attacks affected the organisation systems and their sensitive information. The following diagram shows distribution of the managed attacks, according to their danger level..



Distribution of the 89 organisations signed up to the Internet Early Warning System (SAT-INET)





ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN

CRYPTOLOGICAL CERTIFICATION
Products capable of protecting information.
13 encrypting product files open.

FUNCTIONAL CERTIFICATION
Based on set, acknowledged criteria as an international standard
27 ICT product files open.
3 laboratory credential Files

TEMPEST CERTIFICATION
Equipment protected from emanations.
146 files open for TEMPEST certification for premies, equipment and mobile platforms

Certification projects in which the Certification Organisation worked in 2015

7. TRENDS

A summary of the trends is given below that can presumably be expected in 2016 and the years to come.

Regarding...	It should be expected that...	
The number of attackers (states or professional criminals)capable of developing cyber-attacks...	... is increasing.	↑↑
Due to the limited number of high quality software developers...	... what is known as “Cybercrime-As-A-Service” is increasing, reducing entry obstacles for cyber-criminals.	↑
The sophistication of opponents...	... is developing, making detection and response more difficult.	↑
Spear-phishing...	... continues to be widely used by attackers, as well as the increase in Watering Hole infections.	↔
Ransomware/Cryptoware...	... continues to be one of the most important threats.	↑
Opponents with high technical capacities...	... are increasing in number, in addition to a rise in the volume of incidents. A substantial increase in technical skills has not been envisaged.	↔
Website defacing and holding social communication media to ransom...	... is increasing.	↑

7.1 CYBER-ESPIONAGE

7.1.1 ATTACKS FROM STATES AND CYBER-WAR

The states will continue reinforcing their cyber-skills (defensive and offensive) by improving their capability to obtain information (cyber-espionage) and perfecting their processing methods by broadening the concept of cyber-war on a daily basis and the rules for participating in it.
In fact, cyber-war skills already form part of the international political arsenal, composed of offensive and defensive systems.

7.1.2 DETECTION DIFFICULTY

La Attackers will become more capable of working through security systems and avoiding detection. They will experiment with infections that do not require the use of a file. Thanks to vulnerabilities in BIOS[35], controllers and other firmware will escape defences by injecting commands in the memory or by manipulating functions to introduce an infection or filter data.
There will also be the seizure of remote control or remote shell protocols such as VNC[36] RDP (Remote Desktop Protocol), WMI (Windows Management Instrumentation) and PowerShell[37], where attackers will have direct control over the systems and install malware transparently in the security tools.

7.1.3 MORE PATIENT ATTACKS

Attacks will continue to be registered that are capable of remaining inactive for several months before managing to work through the isolated environments or infections that compile data stealthily without interfering with the user. Also, occult infiltration mechanisms in normally encrypted protocols such as HTTPS. Another technique that will remain present is the decoy: malware or botnet that attracts the attention of security equipment, whilst the real attack is infiltrated stealthily elsewhere, without being seen.

7.1.4 GHOSTWARE? GHOST MALWARE?

As attackers become the focus of attention for researchers, police forces and the justice system, they will develop a new variety of malware designed to complete their assignments and erase all trace before security measures can detect them.
It can be presumed that 2016 will bring us the first evidence of this **Ghostware**, developed to steal data... and disappear without leaving a trace.

7.1.5 TWO-SIDED MALWARE

As security measures have evolved (including sandboxes or test areas), we cannot rule out that we will see an upsurge over the next few years in new malware that, after running an innocent task, and passing the test filter, then runs a damaging process, once it has cleared the security protocols.

7.1.6 GREATER INTERVENTION FROM GOVERNMENTS

On the other hand, there is a current field of thought throughout the world revolving around further involvement in legislating the Internet which will have a greater impact on the security of organisations as well as the entire net.

7.2 CYBER-CRIME

7.2.1 EVOLUTION

The majority of cyber-crime actions aim to obtain money, going after anything of value. For this reason, the increase in value of personal information will be determining and will continue to grow.
In addition, cyber-attacks will be more accessible to users with great technical knowledge, permitting or encouraging the appearance of more personal targets such as discrediting or false testimony, attacks on integrity, bullying or vandalism.

7.2.2 DDOS EXTORTION WILL BE INCREASINGLY COMMON

Groups such as **DD4BC or Armada Collective**, specialising in sending mails asking for a ransom and threatening to bring down a website, have confirmed the success of this technique. This threat will continue (and get worse) in 2016, as more criminals see the potential benefits of DDoS extortion..

7.3 OTHER TECHNICAL TRENDS

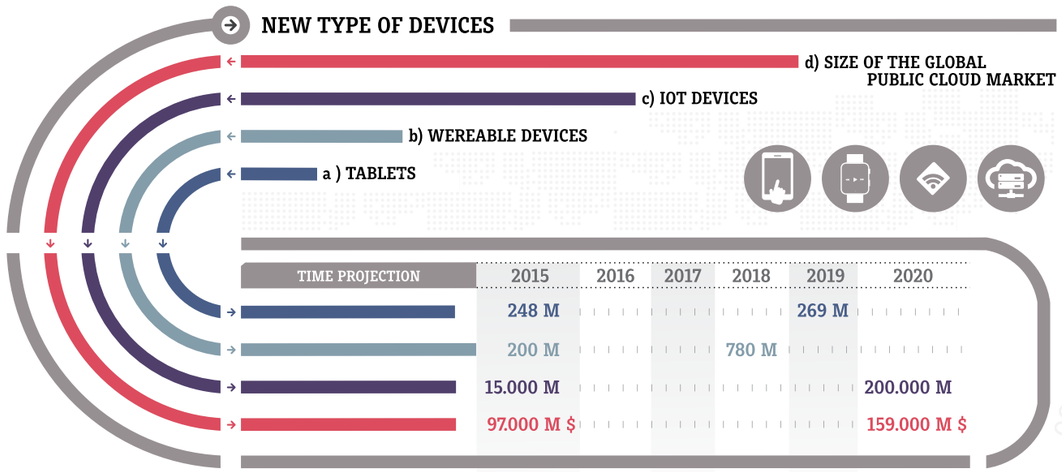
7.3.1 HARDWARE SECURITY

It has been envisaged that many groups will appear using new techniques to develop singularly effective attacks on hardware or firmware vulnerabilities. In parallel, protection mechanisms will emerge such as secure start-up, trusted environments, protection against manipulation, acceleration of cryptography, protection of active memory and device identity making life more difficult for attackers..

[35] Basic Input and Output System.
[36] VNC. (Virtual Network Computer) This is a free code program based on the client-server structure allowing someone to take control of the server computer remotely via a client computer https://wikipedia.org/wiki/VNC.
[37] Powershell. This is a console interface with the possibility of writing and joining commands by means of instructions (scripts). https://wikipedia.org/wiki/Powershell.

7.3.2 ATTACKS ON THE INTERNET OF THINGS

The rise of what is known as the Internet of Things (IoT) and its users will continue to attract interest from cyber-criminals. Not only devices (telephones, tablets, TV, wearables[38], lights, cars, electrical appliances) from which an enormous amount of information can be extracted, but also services behind them connected to a central hub in the cloud.



Evolution of the volume of new devices[39]

7.3.3 VIRTUALISATION AND ACCESS TO THE CLOUD

Virtualisation presents advantages and disadvantages: it isolates and protects virtual servers and applications but it makes it difficult to detect sideways movements. Over the next few years **SDN technology** (Software Defined Networking) will be generalised, not only in data centres and cloud environments. It will be used along with NFV40 technology to create a variety of services on demand, in adaptable and automated formats. The risk will be a greater attack surface area and single fault points.

7.3.4 SECURITY AND PRIVACY

Over the next few years, the sheer amount of personal data being compiled will cover all types of personal information: name, address, phone number, email, shopping record, most visited sites, daily behaviour (what we eat, watch and listen to), our weight, blood pressure, medication, sleep habits or the exercise that we do. Sensors will provide this information to organisations that in turn will send us advertising, recommendations and offers to match our interests. This "digital footprint" will have enormous economic value, imposing the need to protect it, control it and logically, there will be people who try to get hold of this information "legitimately" (consent agreements) or illicitly. By means of analytical techniques that are used in the world of Big Data, these criminals search for links and correlations in personal identities and sell the information to the highest bidder.

[38] Wearables (smart accessories). This is a device that can be worn under or even on clothing and that is always switched on allowing multi-tasking. https://wikipedia.org/wiki/Wearable.

[39] Source: McAfee Labs, 2015.

[40] NFV Network Functions Virtualisation. This consists of virtualising essential components in the network such as firewalls, routers, switchers, storage, load balancers, etc. so that it is not necessary to have physical equipment and the same functions can be performed by deploying software-based network services that can be hosted in centralised or distributed servers. NFV is basically "cloud" technology from the IT world applied to the world of telecommunications operators and service providers https://wikipedia.org/wiki/NFV.

APPENDIX B:

MOBILE DEVICES AND COMMUNICATIONS

The CCN-CERT IA-09-16 report includes three major appendices that complete the general Cyber-security panorama in 2015. The first (Appendix A) compiles the most outstanding work from the National Cryptology Centre (see central pages); the second (Appendix B), Mobile devices and communications and the third (Appendix C), Hacktivism in 2015.

In the case of mobile devices and communications, it weighs up the current situation, their relevant cyber-threats, malware for iOS, the licence model in Android and the most important outstanding vulnerabilities.

So, mobile technologies appear as one of the main areas in the emerging panorama of security threats, specifically due to their close relationship with the Internet of Things and the risks associated with the loss or theft of the devices. In the same way, it is calculated that there are more than **9 million samples** of malware for mobiles, with an **increase of 50% on the previous year** (95% directed at Android) and Ransomware was the most prevalent malware for Android. They include: **Locker** (tricks the user into thinking that they are installing a harmless software update), Porn Droid, or **Lockerpin**, distributed through adult websites, modifies the access code for the device to force the user to pay the ransom.

The **Hacking Team** incident (a company that deals in vulnerabilities and non public exploits and that works with governmental agencies) confirmed the capabilities of its developments, for both Android mobile devices and for iOS. In fact, 11 apps were used (WhatsApp, Twitter, Facebook, Facebook Messenger, WeChat, Google Chrome, Viber, Blackberry Messenger, Skype, Telegram and VK) to distribute malware.

We can expect an increase in what is known as **Potentially Unwanted Software** or **PUS**, meaning apps that spy on user's activities or data, or attack payment systems, increasingly used through mobile phones, and banking malware, that will continue to become more professional and whose main aim is to obtain the user's credentials to access online banking via their mobile such as through **SlemBunk**.

.

CCN-CERT
centro criptológico nacional

WWW.CCN-CERT.CNI.ES
WWW.CCN.CNI.ES
WWW.OC.CCN.CNI.ES