CCN-CERT IA-09/15

CYBER–THREATS 2014 TRENDS 2015

Executive Summary

xx de xxxxxx de 2015

CCN-CERT
centro criptológico nacional

CONTENTS

1 | INTRODUCTION

If anything might sum up 2014, it would be the particular virulence of attacks on Information Communication Technology (ICT) system security among governments, local authorities and companies with high strategic value. Wide-reaching incidents have been occurring, month by month, in a continuous attempt by attackers to get hold of valuable or sensitive information from a political, strategic, security or economic point of view. This is what we have come to call cyber-espionage.

What's more, cyber-crimes, with new business models such as Service Crime; hacktivism, with more modest intentions, although also potentially endangering an organisation's service provision and normal operation; or cyber-terrorism and cyber-wars, as potential threats, have all made themselves known in a year in which Spain has far from escaped this wide range of cyber-attacks. On the contrary, our country has been one of the most severely punished by cyber-threats, particularly cyber-espionage and organised cyber-crime.

This Report on Cyber-threats 2014 and Trends 2015 (CCN-CERT IA-9/15) aims to take a closer look at this panorama, its origins, development and consequences and even catch a glimpse of trends we might expect over the next few months in terms of cyber-security. For the seventh year in a row, it has been drawn up by CCN-CERT, at the National Cryptology Centre (CCN), depending on the National Intelligence Centre (CNI).

It is the result of experience from the National Governmental CERT, in charge of managing cyber-incidents that affect classified systems, Public Administration and companies and organisations with strategic national interest. It has also used other national and international, public and private, documentary sources.

Spain has been severely punished by cyber-threats, particularly cyber-espionage and organised cyber-crime

This document contains a national and international analysis of cyber-threats and how they are changing, as well as five very interesting appendices:

- CCN-CERT activity
- Mobile devices: cyber-threats and trends
- Hacktivism
- Cyber-espionage campaigns (Independent report: CCN-CERT IA-10/2015.

  Classification: Limited distribution)
- Compiling the most significant security news and incidents from 2014.

The abundance of data (threat agents, tools used to carry out cyber-attacks,
vulnerabilities, measures, cyber-incident types and outstanding campaigns or cyber-threats in mobile devices and communications) gives a report covering over 160 pages (available in the private zone of the www.ccn-cert.cni.es website), and its Executive Summary is presented here in this document.

2 | THREAT AGENTS

Who?

The CCN-CERT IA-09/15 report exhaustively analyses threat agents, their origin, motivation, plus the techniques and skills they have demonstrated.

2.1 States: Cyber-spying

During 2014, the threat of cyber-espionage originating from actual countries or companies reached maximum intensity seen so far and doubtlessly represented the greatest cyber-security threat to national interests. We have witnessed an increase in the number of cases recorded and the complexity and impact of their actions, bringing about the need to strengthen competent public services' detection, analysis and response capabilities throughout the world, particularly Intelligence Services.

Cyber-espionage revolves around the use of APT techniques (Advanced Persistent Threat), working against different targets. In the case of Spain, this has focussed on different Spanish public administration departments, defence, aerospace, energy, pharmaceutical, chemical and ICT industries plus mobile devices for these sectors.

In fact, this type of attack is behind the most dangerous incidents managed by the CCN-CERT. In total, in 2014, the National Governmental CERT tackled 12,916 incidents of which 132 were classified as critical; meaning any that might downgrade services for a large number of users, implying a serious information security violation, any that might affect people's physical integrity, cause important economic losses, inflict irreversible damage on the organisation's resources, lead to crimes and/or regulatory sanctions or very seriously damage an organisation's image.

Without mentioning the specific origin of this type of threat (the CCN-CERT IA-10/15 Limited Distribution Report compiles a summary of the main cyber-espionage campaigns), we should not forget that states can also develop attacks by contracting services from other players (consequently operating under another flag) or by making attacks look like hacktivist movements.

2.2 Cyber-crime

The CCN-CERT managed 12.916 incidents, of which, 132 were classified as critical

2014 demonstrated that crime is being organised more professionally in cyberspace, using the Internet to commit many different types of crime and for the ultimate purpose of economic gain. Some of the most outstanding pursuits are:

- Distributed denial-of-service (DDoS) type cyber-attacks or introducing malware into the victims' information systems as a form of blackmail. ***Ransomware***[1] (more innovative and aggressive than ever during 2014) and, specifically, the appearance of what is known as ***cryptoware,*** has been on the rise and increasingly sophisticated in terms of methods for paying ransoms (using digital tickets or currency, such as Bitcoin).
  The CCN-CERT has detected over 200 incidents of this type in Public Administrations.
- ***Crime-as-a-Service*** where third parties develop cyber-attacks. This model has grown in size, complexity and professionalism. It has also been seen that the cost of deploying botnets and DDoS is dropping thanks to the appearance of other options. On the other hand, the price of new vulnerabilities has gone up significantly.
- Trading services or stolen information using **botnets**[2] or malware.
- Use of cyberspace to develop other forms of crime and reveal that drug trafficking organisations have been contracting services from certain hackers.

[1] *This consists of hijacking the computer (making it impossible to use it) or encrypting its files (Cryptoware), promising to release them after payment of a quantity of money as a ransom.*

[2] *A botnet is a network of infected computers that are used for illegal activities, such as launching distributed denial-of-service (DDoS) attacks against a specific system.*

2.3 Hacktivists

Ransomware and, specifically, its more aggressive version, cryptoware, has become more widespread and sophisticated

Hacktivists: Persons or groups, some more organised than others, attempting to control networks or systems to promote their cause or defend their political or social positions, based on ideological reasons. Over the last few years, their cyber-attacks (defacing websites, DDoS attacks, etc.) claim to be in response to determined measures adopted by governments. Knowledge and skills vary widely from one group to another.

Internationally, outstanding hacktivist focus spots have appeared in parallel to social or political conflicts (Israel, Ukraine, Hong Kong, Turkey, Pakistan) as well as individual activity by several hacktivist organisations such as Syrian Electronic Army', 'Anonymous Italia' or 'Lizard Squad'.

Hacktivist presence in local organisations has fallen in Spain, where *'La 9ª Compañía'* is the only operative benchmark. On the other hand, a slight increase has been seen in Moroccan hacktivist organisation attacks against low level websites in our country.

Appendix C for the complete CCN-CERT IA-09/15 Threat Report contains a study focus on the ***«Hacktivist threat in 2014»***.

2.4 Terrorism

Terrorist groups have still not achieved the precise skills or have not had access to the resources to develop complex attacks. In any case, jihadist groups have carried out small scale cyber-attacks (essentially defacing websites and DDoS attacks) in different places, generally in response to claims of hostility to Islamic interests.

More frequently, the Internet is used for financing, coordination, propaganda, recruitment and radicalisation purposes.

In any case, knowledge being acquired by terrorist groups could be enormously important in the future which is why these extremes require constant surveillance.

2.5 Other players

2.5.1 *Cyber-vandals and script kiddies*

Cyber-vandals: individuals with significant technical knowledge that carry out actions just prove to the world that they can do it.

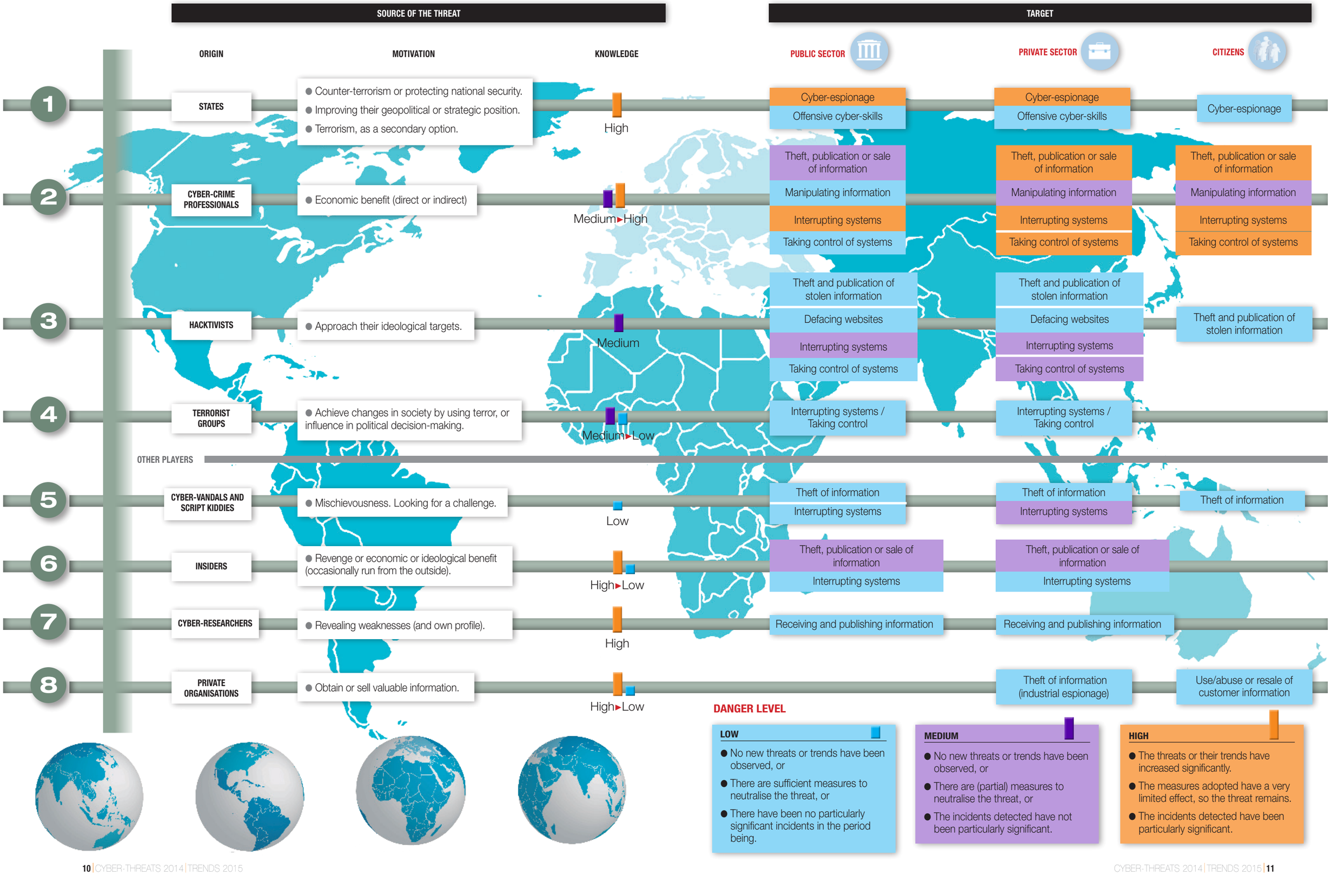
Script kiddies: someone with limited knowledge, making use of tools built by third parties, who performs actions as a challenge, often without being fully aware of the consequences.

There did not seem to be a significant change in actions that could be attributed to either of these types of cyber-criminal in 2014 compared to previous years. use of tools built by third parties, who performs actions as a challenge, often without being fully aware of the consequences.

There did not seem to be a significant change in actions that could be attributed to either of these types of cyber-criminal in 2014 compared to previous years.

2.5.2 Insiders

Someone that has or has had any type of relationship with the organisation, including former employees, temporary staff or suppliers.



DANGER LEVEL

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.

MEDIUM

- No new threats or trends have been observed, or
- There are (partial) measures to neutralise the threat, or
- The incidents detected have not been particularly significant.

HIGH

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

They can be one of the greatest threats, usually with similar motivation: revenge, financial or political reasons, etc.

We should also bear in mind that these insiders might be employed by any of the former (particularly for cyber-espionage) for preliminary infection of the target network or to extract information from it.

2.5.3 *Cyber-researchers*

People who track down vulnerabilities that might affect systems (hardware or software). Publishing the results of their investigations might mean that their findings are used by malicious third parties.

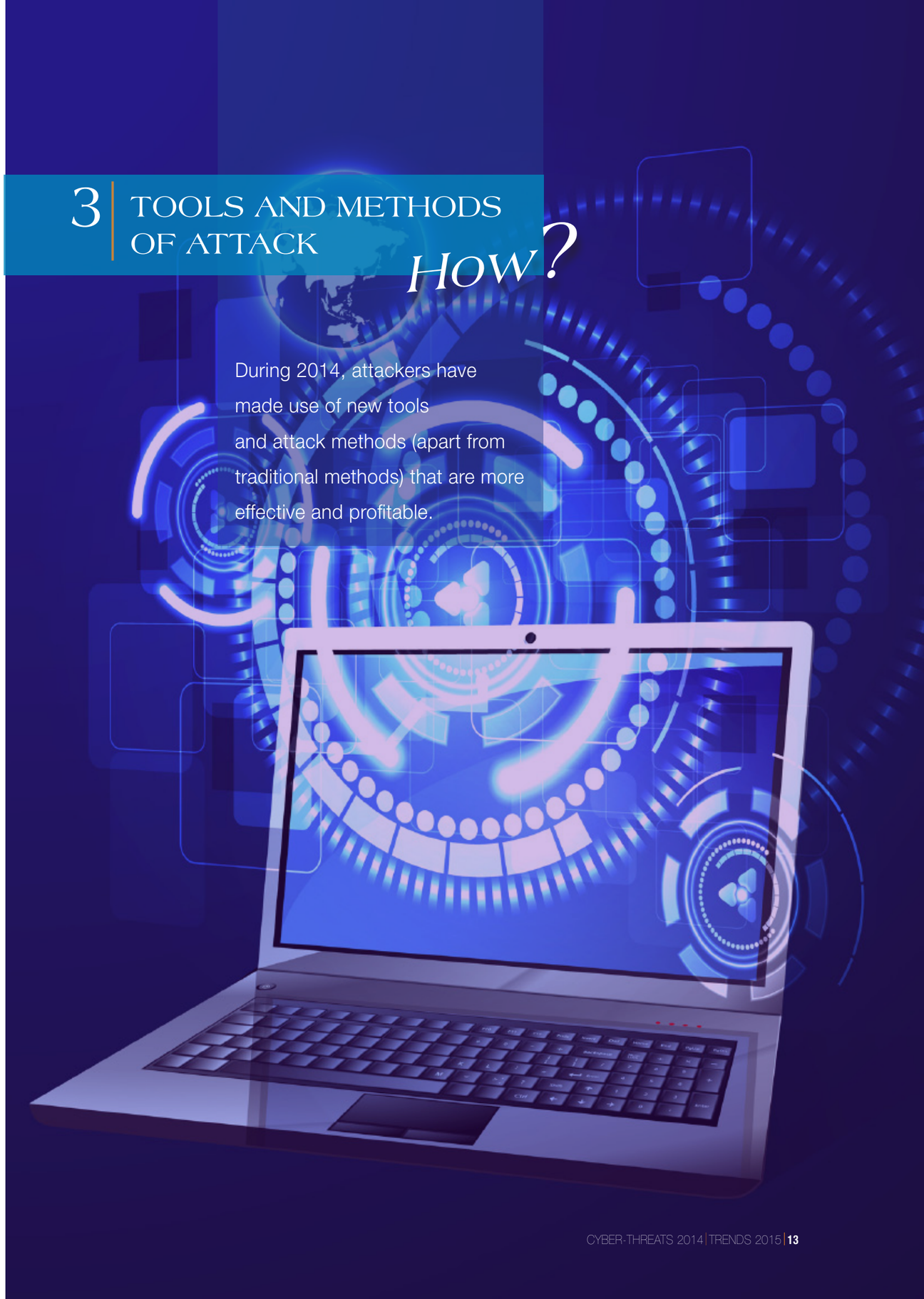
2.5.4 Private organisations

The reasons behind cyber-attacks also lie in Private Organisations that get involved with industrial cyber-espionage to get hold of the competition's knowledge for economic gain.

3 | TOOLS AND METHODS OF ATTACK

How?

During 2014, attackers have made use of new tools and attack methods (apart from traditional methods) that are more effective and profitable.



In general they have been more effective and profitable as demonstrated by the existence of new botnets that have been used for the most relevant DDoS attacks.

Spear-phishing[3] has continued to be the most used element to spread this type of infection.

On the other hand, what is known as ransomware has become more innovative and aggressive.

Perhaps, the most significant example can be found in cryptoware infections that have represented a new and lucrative business model for criminal organisations.

This has led to the development of what is known as *Crime-as-a-service,* capable of making large-scale attacks possible by users with low technical knowledge.

3.1 *Exploits*[4]

Their number dropped in 2014 (standing at around a thousand a year), although the market price of these tools (particularly so-called zero-day exploits) has grown at the same pace. These circumstances have caused the development of a black market for exploits that is capable of moving enormous sums of money every year.

PLATFORM	PRICE*
Adobe	5.000 – 30.000 $
Reader Mac	20.000 – 50.000 $
Os X Android	30.000 – 60.000 $
Plug-ins browsers Flash or Java	40.000 – 100.000 $
Microsoft Word	50.000 – 100.000 $
Microsoft	60.000 – 120.000 $
Windows Firefox	60.000 – 150.000 $
or Safari Chrome or Internet	80.000 – 200.000 $
Explorer Apple iOS	100.000 – 250.000 $

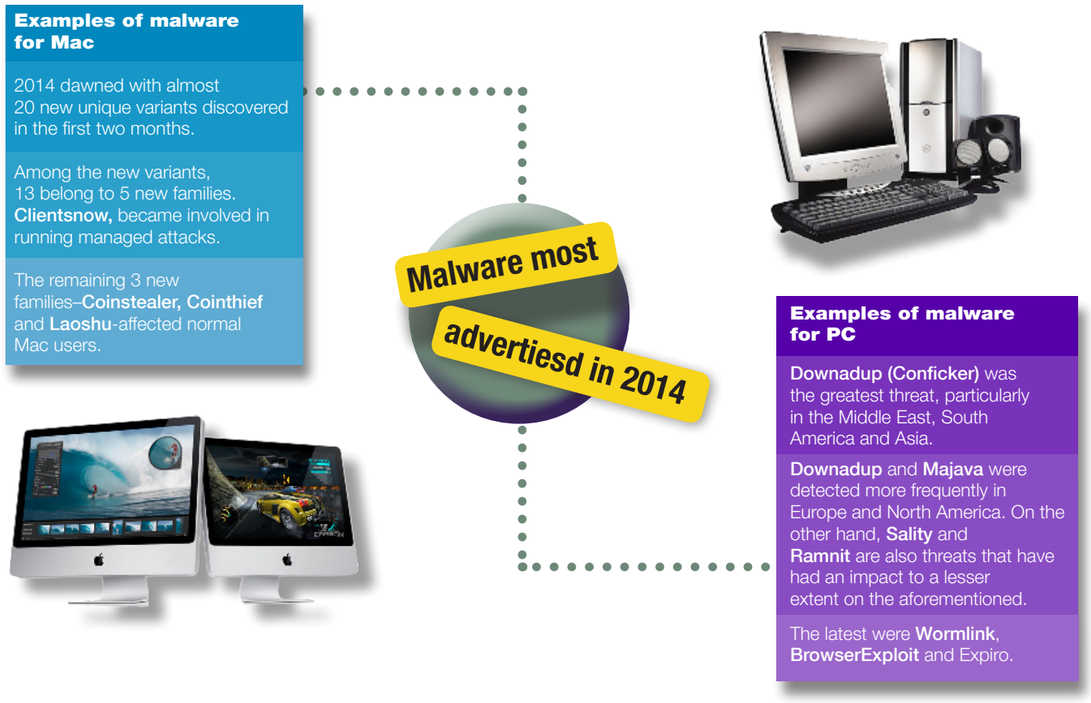
Zero-day exploit Source: FORBES

3.2 Malware

It has four main features:

- Complexity: from the 1997 virus up to current ransomware, APT tools or the use of web infrastructures (DNS[5]).
- Constant rise in number (up to 25 million examples).
- Capability to adapt over time (malware is often a variation on previous samples).
- The highest quantity of malware corresponds to trojans[6].

The complete Threat Report compiles a vast amount of data on malware: its volume, type, distribution geographically and by business sector or methods of infection.



Also, detection of ransomware increased in 2014, with increasingly innovative and aggressive examples of malware whilst also making the method for paying the ransoms more sophisticated, using digital tickets or currency (cryptocurrencies) such as Bitcoin. **Spain appears among the list of countries particularly targeted by this type of malware.**

[3] *This consists of a scam in the form of an email sent specifically to the target to get personal information that can be used subsequently to benefit the attacker.*

[4] *An* exploit *is a program that exploits or makes the most of a vulnerability in a computer system for its own benefit. On the other hand,what are known as zero-day exploits are any that have not yet been published and therefore do not have security solutions for their vulnerabilities.*

[5] *DNS (Domain Name System). Domain Name System is a system that names all the connected equipment, services or resources giving them an address.*

[6] *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).

3.3 Malware for mobile devices

It has the same objectives that caused malware to be developed for PCs (**Appendix B** of the complete CCN-CERT 09/15 report, compiles an in-depth study of **«Mobile Devices: Cyber-threats and Trends»**), although with a few differences:

- Manufacturers of the operating systems for this equipment (Apple, Google or Microsoft) control their official stores where the applications are sold. For this reason, the malware usually spreads more slowly, although a large quantity is distributed via unofficial stores, forums or webs. The so-called «jailbreak» or «rooting»7 of the device significantly increases the risk.
- Many services, particularly banking, usually employ a second factor (channel) for authentication, so there are types of malware that attempt to infect the PC and mobile device over time.
- There is malware that causes calls or text messages to be sent to special tariff numbers that can cost victims a lot of money.

As in previous years, Android continues to be the most used and attacked mobile operating system, followed by iOS (Apple) and Windows Phone. On the other hand, although some manufacturers consider it unnecessary, many anti-virus software companies are developing products for this type of device.

3.4 *Botnets* and *Spam*

It is increasingly difficult to detect and erase robot networks (botnets) that are still being used to spread spam[8], to run DDoS attacks, *spear-phishing*, *click-fraud*[9], *keylogging*[10], and the spread of ransomware or theft of digital money.

[7] Jailbreak *in Apple or* rooting *in* Android *(access to the root directory) gives complete access to this operating system, with administrator or superuser privileges, by removing some of the manufacturer-imposed limitations.*

[8] *Mails, generally advertising sent massively to thousands of users, also known as junk mail.*

[9] Click *fraud is the type of fraud that takes place when clicking on advertising in a website that imitates a legitimate user.*

[10] *Key logger. This is malware that captures confidential data such as user passwords.*

Data from 2014 shows a drop in the number of botnets detected, although not in their efficacy or danger. In fact, attackers now use the TOR[11] network to hide botnets and/or control and command servers (C&C), making it incredibly difficult to detect and remove them.

3.5 *DDoS* attacks

After a few relatively calm years, DDoS attacks returned with unusual intensity. The bandwidth used and the duration of the attacks (sometimes very long) demonstrate this exceptional virulence.

The reason behind all this lies in the increasing simplicity of developing DDoS attacks and how easy it is to access certain tools (bought on the *hidden-wiki*[12], black market, for example).

2014 saw the appearance of attacks by DDoS amplification by means of UDP[13] protocols and against the network infrastructure (volumetric attacks).

An increase has also been seen in attacks run against the application layer (layer 7), much more sophisticated and not necessarily focussed on the bandwidth that requires significant knowledge.

[11] *TOR (abbreviation for* 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, mainly due to Internet privacy issues. Correlatively, TOR has become a very useful tool for anyone that, for any reason, legal or illegal, does not wish to be watched or does not wish to reveal confidential information.*

[12] *This is an encyclopaedia that is hosted in the hidden web also called the invisible web or deep web) and it works as an index to access domain pages (.onion) that give an anonymous IP address that can be accessed by means of the TOR network (The Onion Route).*

[13] *UDP* (User Datagram Protocol) *is a type of transport level communications protocol that does not have the same reliability and security features as the TCP (Transmission Control Protocol) but in exchange it is much faster; ideal for short messages, such as the domain name system (DNS) or when losing packages is not relevant as in the case of audio or video streaming.*

3.6 Phishing[14]

As in previous years, email continues to be the preferred medium for cyber-attackers to collect information from victims or to get them to involuntarily download malware.

It has been seen that the quality of phishing messages has considerably improved, although attacks have begun to combine use of email and telephones (social engineering).

In the same way, and as previously mentioned, spear-phishing has been the most used element in this type of attack. The attacker writes an email using information from the victim's context (often obtain from social networks) to make it seem more believable and includes a link with exploits-kits[15] or RAT tools[16]. It is therefore more likely to succeed.

3.7 Use of digital certificates

Growing trend to use (apparently legitimate) digital certificates in application installation processes or as a means of authentication.

Using this procedure, attackers attempt to generate trust among their victims, making them believe that these are legitimate sources. Theft of certificates or compromising the Certification Authorities are usually the chosen means for this type of action that can even be spread using automatic content distribution networks (CDN[17]) that make malware programs look like legitimate software packages.

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

[15] *Exploits-kits: Packages with malware programs.*

[16] Remote Administration *Tools.*

[17] Content Delivery Network.

4 VULNERABILITIES

Where?

As in previous years, vulnerabilities that can be attributed to software remain at a high level, while any caused by human and organisational factors are stillone of the weakest links in the chain.

4.1 Technical vulnerabilities

The Heartbleed case, a vulnerability in OpenSSL[18], appeared in April 2014 and gave attackers access to the memory of the attacked computers; it demonstrated **the importance of promoting secure software development whilst accepting that it is impossible to guarantee building error-free programs and applications.** The following table shows the most outstanding vulnerabilities in 2014[19]

IntelliShield	Vulnerability	Urgency	Credibility	Severity
33695	OpenSSL TLS/DTLS HeartBeat Information Disclosure V.			
35880	GNU Bash Environment Variable Content Processing Arbitrary Code Execution V.			
35879	GNU Bash Environment Variable Function Definitions Processing Arbitrary Code Execution V.			
36121	Drupal Core SQL Injection V.			
32718	Adobe Flash Player Remote Code Execution V.			
33961	Microsoft Internet Explorer Deleted Memory Object Code Execution V.			
28462	Oracle Java SE Security Bypass Arbitrary Code Execution V.			
30128	Multiple Vendor Products Struts 2 Action: Parameter Processing Command Injection V.			

[18] *Library of programs that are usually used by a large number of systems (web servers, VPN, WiFi hotspots, etc.) to establish safe connections. In order to avoid being compromised again, the main technological companies announced wide-reaching economic support for OpenSSL and other open code software. The Heartbleed case left the possibility wide-open that a similar problem issue might occur with other common use software.*

[19] Source: *CVSS. Common Vulnerability Scoring System.*

«Mobile Devices and Communications: Cyber-threats, and Trends», Appendix B of the Report CCN-CERT IA-09/15

Outstanding aspects in the field of vulnerabilities:

- Increase in exploitation of vulnerabilities in Java, Internet Explorer, Adobe Flash and Adobe Reader.
- **Updating software and end of support:** updating software is not possible in some devices whilst only available for a limited time in others. For example, support ended for **Windows XP**[20], on 8th April 2014 despite the fact that a large number of users still have this operating system.
- **New trends:** Attacks on sales points or cloud services.
- Massive use of protocols with no security such as BGP, DNS and SMTP[21] with scarce verification authentication or encryption, despite their essential role in routing Internet traffic. A well-constructed attack that exploits **BGP vulnerabilities** could manage to monitor **Internet traffic** on a large scale, with the risks that this would incur.
- **Mobile devices:** As many as 80,000 million applications have been downloaded. Normally, they do not use the available security mechanisms appropriately; they make unauthorised connections and they compile private information without express authorisation from the user.

4.2 Human and organisational factor

New trends were directed towards better efficiency in business that implement BYOD[22] type solutions and use of cloud services, the possibilities brought about by Big Data increase organisations' exposure, requiring new security policies and measures to be implemented.

As far as users are concerned, we might highlight the use of weak passwords and the massive use of social networks providing personal and corporate information making attacks easier.

[20] *CCN-CERT IA-02/14 Risks of using Windows XP after the end of support.*

[21] *BGP* (Border Gateway Protocol), *DNS* (Domain Name System), *SMTP* (Simple Mail Transfer Protocol).

[22] *CCN-CERT IA-21/13 Risks and Threats from BYOD* (Bring Your Own Device) *allows employees, with their personal mobile devices, to access corporate services (mainly mail).*

5 CYBER-INCIDENTS *what?*

The number of cyber-incidents has not stopped growing during 2014 and, even more worryingly, they are becoming more dangerous.

Incidents can be classified differently (the CCN-CERT compiles the types used by Public Administrations in its ***CCN-STIC 817 Guide to Managing Cyber-incidents***) pero, en general, todas tienen en cuenta los ataques dirigidos a la información o a los sistemas.

5.1 Attacks on information

«Cyber-espionage Campaigns», Report CCN-CERT IA-10/2015. Classification: Limited distribution

- ***Cyber-espionage:*** the most important and dangerous attacks on institutions and companies in Western countries **–including Spain–** (such as several Ministers and Secretaries of State for the Government suffered a variety of campaigns attacking mobiles and personal computers belonging to senior staff in the Government, through a malware email).
- **Advanced Persistent Threats *(APTs)*:** The CCN-CERT IA-10/15 report compiles information on actions detected in 2014, their complexity and sophistication.
- **Theft of information,** in addition to being the main aim of APTs, represents a specific type of threat that the report studies in depth (*Pony*[23] *botnet*, stolen credentials, etc.)
- **Blackmail** such as threatening to publish certain information.

5.2 ICT attacks

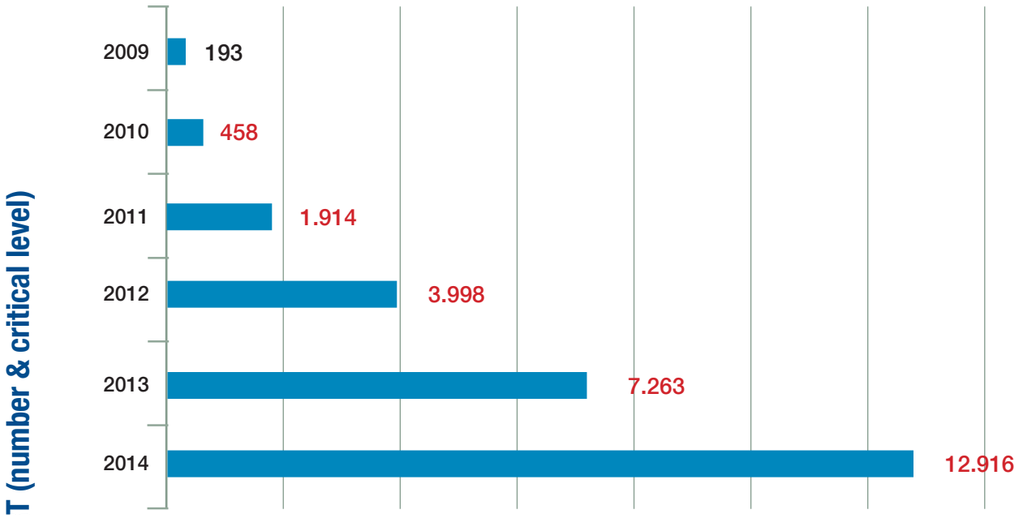
In addition to the information that they process or store, it is often the actual information systems and infrastructures that are targeted by cyber-attacks. This includes:

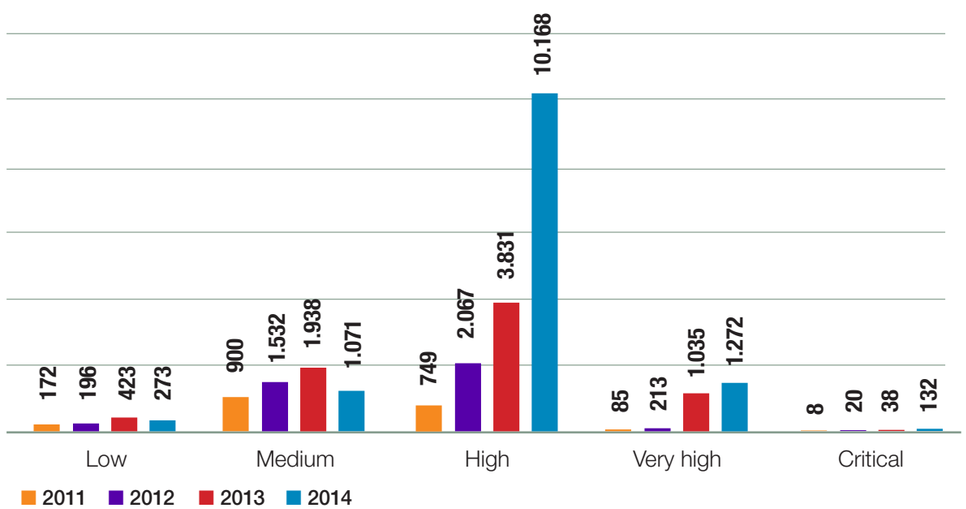
- **Defacement:** attackers change website content, such as attacks led by Anonymous and the Syrian Electronic Army (CCN-CERT IA-01/14, IA-04/14, IA-08/14, IA-12/14 and IA-18/14 reports among others).
- **Interrupting and taking control of systems:** massive use of legitimate web services by attackers to use them as command and control infrastructures and entry points to extract information from the target networks.
- **Cloud Services:** use of cloud services as an intermediate step in leaking information from the attacked networks.

[23] *This is a* botnet *that uses* keylogger *type malware (registering keyboard strokes) that captures all types of confidential information and access data for many applications. It is given this name because it uses the* pony *logo from the famous* «Farmville» *game.*

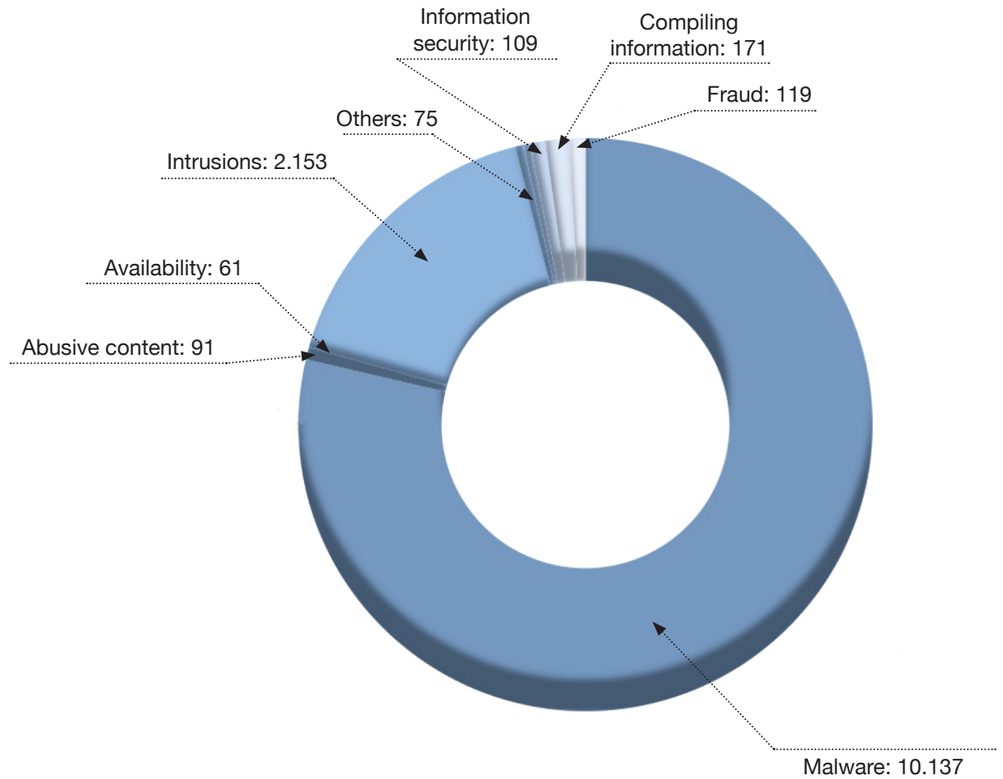
5.3 *Cyber-incidents* in Spain

Looking at the data compiled by CCN-CERT, 2014 was a particularly significant year in terms of cyber-threats, especially cyber-espionage and APTs, malware and ransomware (the National Governmental CERT published the CCN-CERT IA-21/14 report relating to this in December).





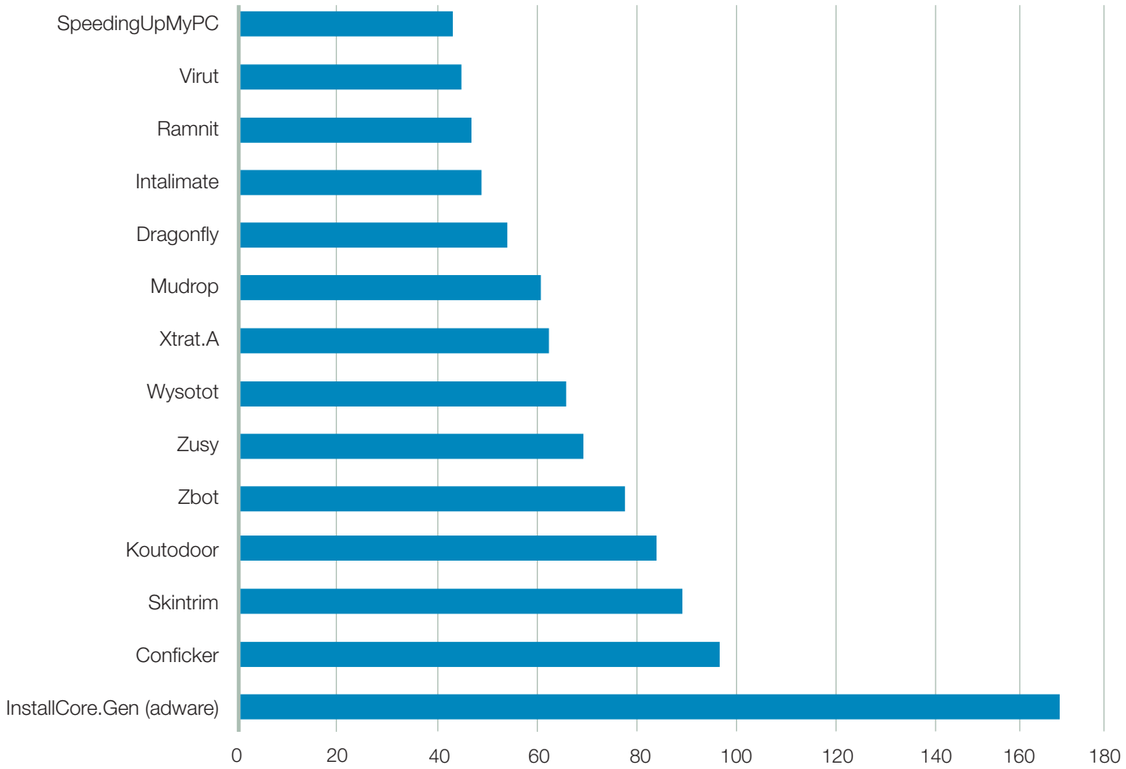
Main subcategories for incidents managed in 2014



Main subcategories for incidents managed in 2014

General sub-classification	Classification	Nº of incidents
Trojan	Malware	9.371
Exploitation of vulnerabilities	Intrusion	833
SQL injection	Intrusion	460
Remote File Injection	Intrusion	460
Worm	Malware	459
Spyware	Malware	258

Most-detected malware by the CCN-CERT



6 | MEASURES

What can we do?

Efforts should be focussed on increasing prevention, detection, analysis, response and coordination along with a policy involving investigation and changing how we think and act: working as if you have been compromised and therefore protecting fundamental assets in a compromised medium.

For Public Administration, the best guarantee is to apply measures considered in the National Security Plan

Necessary measures include:

1. **Necessary measures include:** deploy systems that strengthen capabilities to detect and investigate incidents in networks and systems, making it easier to contain and eliminate them. Deploy centralised management systems for early anomaly detection at security events.
2. **Exchange of information on cyber-threats:** deploy systems that allow detection rules and compromise indicators to be automatically exchanged so they can be included in the defence systems.
3. **Protection against DDoS cyber-attacks:** by means of applying security configurations[24] and connection filtering services.
4. **Secure implantation of IPv6**[25]. Support for migration to the new version.
5. **Use of cryptographic measures,** including the use of HTTPS[26], StartTLS[27] or encrypting connections between data centres. *(CCN-STIC 807 Guide to Cryptology used in the National Security Plan).*
6. **Protection and surveillance of essential services for the organisation.** As highlighted by the National Security Plan, mail and web services (or what are known as electronic headquarters for local authorities) are part of these essential services. In this respect, in 2014, DNSSEC[28] has been consolidated as a particularly useful method to make domain names secure. Using DNSSEC, visitors to a website can check whether they are really using that website or, on the contrary, they have been diverted to another page.
7. **Encourage RTD+i on cyber-security.** Improve security features for products by promoting their corresponding certification processes. Develop new projects that improve surveillance capabilities and streamlined information exchange for use in detection systems.
8. **Awareness-raising at all levels:** executive, employees, professional and citizens.
9. **Training on cyber-security.** Increase training and certification of cyber-security professionals.
10. **Adapting the legislation:** the report compiles a wide-ranging chapter on the standards that have appeared during 2014 throughout the world and the different cyber-security strategies (including from Spain).

[24] *CCN-STIC 812 Security in Web environments and applications and CCN-STIC 820 Guide to protect against denial of service.*

[25] *IPv6* (Internet Protocol Version 6). *This increases the limit of admissible network addresses, going from* 2^{32} *in the case of version v4 to* 2^{128} *in v6.*

[26] *HTTPS (Hypertext Transfer Protocol Secure). Protocol for secure application of hypertext transfer. It uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to create an encrypted channel of communication between the client and the server.*

[27] *STARTLS is an improvement to TLS protocol that does not require using a different port for encrypted communication.*

[28] *DNSSEC (Domain Name System Security Extensions). Security extensions for the domain name system, allowing authentication of DNS data origin.*

7 | TRENDS 2015

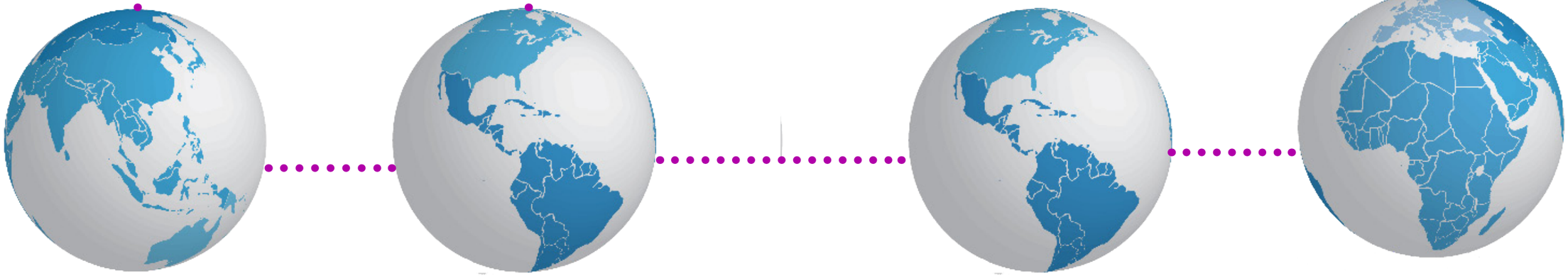
Where are we heading?

Cyber-threats are always one step ahead of the measures that are adopted. In 2015, and in the years to come, we can expect an increase in cyber-espionage and a rise in attacks-as-services run by groups with the right knowledge and technical skills to carry them out successfully.

AIn reference to previous points, we can expect the following trends over the coming years:

PROBABILITY OF THREAT	OCCURRING
Cyber-espionage	The use of cyberspace to obtain intelligence will increase in all countries around us because it is highly effective and also difficult to designate responsibility. Due to the publication of cyber-espionage campaigns carried out by security companies, countries will use more resources to secure their operations by isolating infrastructures and diversifying attack **Techniques, Tactics** and **Procedures (TTP)**.
Attacks as a service	Through groups with knowledge and technical skills. Contracting their services and planning a «custom-built» attack, with guarantees of success. It will require further knowledge regarding Deep Web[29], inetworks, increasing public-private cooperation and harmonising international legislation.
Fusion of TTP used by cyber-espionage and cyber-crime	Evolution of cyber-criminal activity to TTPs used in cyber-espionage by using APT type tools, particularly focussing on the financial sector, in an attempt to steal money.
Attack tools for mobile devices (mainly ANDROID)	The number of threats to Android will double alongside vulnerabilities in mobile devices, platforms and applications. Compromised data will be used for other attacks or sold on the black market.
«Hijacking» organisations using ransomware	Particularly in its most aggressive variants, including major companies and institutions.
Incremento de ataques contra cajeros automáticos y procedimientos de pago	A rise (and evolution) is expected in attacks on these devices (and ticket dispensing machines) using APT techniques to penetrate the financial entity's network. Using Windows XP[30] increases the risk.
New vulnerabilities in software and usual protocols	More names will be added to the list alongside dangerous vulnerabilities already revealed (Shellshock, Heartbleed y OpenSSL, etc.).
Attacks against Critical Infrastructures	Many states are getting ready to attack industrial control systems (SCADA)[31] and other critical systems such as electricity networks.
Attacks against Linux[32] y OS-X[33]	Encouraged by their increased use, deactivation of certain security measures by default (in order to install pirate software) and scarce development of security tools, given their security image.
Attacks against the Internet of Things[34]	Its expansion has brought about major debate on security issues, particularly privacy, as a result of connection. We will also discover vulnerabilities in devices that will allow malware to be included when monitoring user activity.

■ HIGHLY PROBABLE
■ PROBABLE
■ POSSIBLE



[29] *Deep Web or Hidden Web is not accessible using conventional browsers. It is usually accessed using tools such as TOR (The Onion Router).*

[30] *On 08 April 2014, Microsoft stopped giving support to Windows XP.*

[31] *SCADA (Supervisory Control And Data Acquisition). Software that can control and supervise industrial processes remotely.*

[32] *Linux: Free software operating system, similar to Unix.*

[33] *OS-X (or Mac OS X): Operating system based on Unix and developed by Apple Inc. For mobile devices, there is a specific version called iOS.*

[34] *Internet of Things: IoT refers to the inter-connection of daily objects (devices, systems and services) with the Internet using fixed and wireless networks and giving the user remote control and handling.*


www.ccn-cert.cni.es
www.ccn.cni.es
www.oc.ccn.cni.es
YouTube
CCN-CERT
centro criptológico nacional