TRENDS 2016

(IN) SECURITY EVERYWHERE

ENJOY SAFER TECHNOLOGY™

INDEX

1 **Index** **Page 6**
Trends 2016: (In)security everywhere

2 **Internet of Things: security as a whole** **Page 9**
- Wearables
- Interconnecting homes
- Interconnectivity of all things
- Ensure, then connect

3 **Ransomware: first files... now complete devices** **Page 15**
- Varieties of ransomware
- The increase in the number of variants
- Evolution of threats
- From the computer to the TV
- Conclusion: the same goal for another threat

4 **Targeted attacks: implications, reasons and objectives** **Page 20**
- Kits for cyber espionage?
- Attacks on users and specific systems
- Are APTs considered to be the weapons of the future?

5 **Crimeware, malware and massive campaigns around the world** **Page 25**
- Botnets, zombies and global campaigns
- New families, new techniques, but the same goals
- Collaboration is the key to fighting cybercrime
- Where are we going?

6 **Haxposure: an emerging threat with important implications** **Page 30**
- Haxposed: Damaging company secrets and innocent customer
- The implications of haxposure
- Haxposure 2016?

7 **Mobile devices: threats and vulnerabilities** **Page 35**
- An overview of mobile security
- 2015 milestones
- But what happened with mobile malware?
- What may we expect from this trend?

8 **Windows 10:**
Security features and user privacy **Page 47**
- Security features
- Privacy and user acceptance

9 **Critical infrastructure:**
it's time to make security a priority **Page 51**
- Critical systems at risk
- Information asset management as a key factor
- Common threats targeting industries indiscriminately
- Healthcare – among the most affected sectors
- Highly vulnerable medical devices
- Record theft: more than just exposed data
- Focusing on security to prevent intrusion

10 **Laws and regulations** **Page 57**
- Meeting standards and better security practices
- Laws protecting personal information around the world
- Information Security: an effort shared between governments, companies and users

11 **Threats to kids on the web** **Page 64**
- Privacy and sexting
- Grooming
- Cyberbullyng
- Law and social contract as prevention

12 **2016: the security challenge** **Page 70**

1

Trends 2016:
(In)security everywhere

1 TRENDS 2016: (IN)SECURITY EVERYWHERE

Year after year, at ESET's Research Laboratories, we review some of the most important events of the year globally, and their impact on the worlds of both corporate and home IT users. Taking into account discussion and examination of what has happened in technology, it is difficult to sum up everything in one phrase. New technologies, attack reports, new malware families, and security flaws with a global impact: the speed at which these follow one another makes security an increasingly important challenge for businesses, enterprises, governments and users around the world.

In recent years, we have discussed how the web became one of the main channels for the spread of malicious code; the growth and professionalization of crimeware; the importance of botnets to the world of cybercrime; the spread of malware targeting mobile devices. Each of these trends has had an impact in recent years, and in our document *"Trends for 2015: Targeting the corporate world"* we not only emphasized how different companies had become the targets of computer attacks, but also broke the report down into different topics.

When distinguishing between trends, there is a clear relationship between the expanding number of devices, the growth of technology, and the increasing challenge of safeguarding information, whatever the scope of its implementation may be. In *"Trends for 2013: Astounding growth of mobile malware"* we added a first section for malware in new technologies, before there was talk about the Internet of Things (IoT), referring to Smart TV, and other smart devices. Today, three years after that document, IoT is more present than ever, and continues to grow not only in the home but also in the context of industry, business and government.

When we talk about IoT we are referring to devices we already know about and which are used as standalone appliances but with the additional ability to connect to the Internet, of generating information and sharing it with thousands of users, providers or companies. The information shared belongs to the users, either through devices that people use and carry with them all day (such as smartwatches), or through electrical appliances, or even sensors that collect information in public places. This trend poses a new challenge, a need to ensure the safety of information flowing to and from these new technology devices. This challenge, added to all other areas that have already been addressed by the IT department for years, significantly extends the level of protection and training needed.

2015 was a year in which the corporate sector was the target in various security incidents; in which the disclosure of vulnerabilities affected millions of mobile devices; in which there were continuing reports of directed attacks; and in which vulnerabilities emerged that affected many IoT devices, from cars to precision rifles. In this report, we will review the most important recent events in security and, based on the events that occurred, we will predict future trends and challenges for maintaining the security of information, both within the business environment and at home.

Throughout the various sections of this paper, we will review the state of crimeware and its impact on companies and users, and we will look at directed attacks and APT campaigns that have occurred in different parts of the world. Moreover, we will consider the risks faced by victims of ransomware when it comes to salvaging their information, and how they can protect themselves from this kind of extortion. Finally, we will review each of the most important topics in the security world, explaining why cybercriminals attack more and more platforms and technologies, and why, ultimately, security is no longer just a problem for a few individuals but rather a problem involving more and more people, and why security should occupy an important part in our lives.

It is our pleasure to introduce this document from ESET Laboratories in which we try to tell you what will happen and what the challenges are for next year in terms of computer security: ***"Trends 2016: (In)security Everywhere".***

> SECURITY IS NO LONGER JUST A PROBLEM FOR A FEW INDIVIDUALS BUT RATHER A PROBLEM INVOLVING MORE AND MORE PEOPLE

2

Internet of Things:
security as a whole

- Wearables
- Interconnecting homes
- Interconnectivity of all things
- Ensure, then connect

Author
Pablo Ramos

2 INTERNET OF THINGS: SECURITY AS A WHOLE

The Internet of Things (IoT, to use its English acronym) is a topic that became popular some years ago and which, from its very beginning, has generated controversy and debate, mainly within the information security community, since its emergence involved (and still involves, more than ever) big and new challenges.

Two years ago, more precisely in the report *Trends for 2013: Astounding growth of mobile malware*, ESET's Global Research Laboratories were already pointing out the threats faced by smart devices based on 2012 research, reports and detections. Today, three years later, the advance of technology keeps pushing boundaries and expanding the capabilities of this type of device; there are increasing numbers of devices connecting to the Internet and correspondingly easy access, causing an increase in the number of attacks against them. This became evident in the form of malicious campaigns which adversely affected millions of users worldwide. One of the most significant cases was *Moose, a worm infecting thousands of routers all over the world*.

According to a report from Gartner, today *there are 4.9 billion devices connected to the Internet*, and that number will keep growing over the next 5 years, reaching up to 25 billion Internet-connected devices by 2020. In brief, IoT is here to stay, and through the upcoming years the number of devices that generate, store and exchange data among users will continue to grow, with the aim of improving their experience and simplifying many of the tasks they perform. (Table 1)

In the forecast below, Gartner predicts that the consumer segment will be the fastest-growing over the next five years. Whether by the emergence of new wearables (devices used as body accessories) or by new household appliances, it is worth pointing out that they will need protection to prevent potential security incidents.

However, IoT is not just for consumers: companies and governments are investing and getting involved in this industry with the aim of improving people's lives and their own standing. This process is known as *Industry 4.0*; some even believe that it represent the "fourth stage of the industrial revolution", as it has been labelled by *the Federal Department of Education and Research of Germany.*

Table 1 IoT units of equipment by category (in millions)

Category	2013	2014	2015	2020
Automobiles	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Businesses	395.2	479.4	623.9	5,158.6
Services (Vertical Business)	698.7	836.5	1,009.4	3,164.4
Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Source: Gartner (November 2014)

The process entails the development of smart products through smart processes. Simply expressed, turning a current industry into a smart industry implies basing it mainly on IoT and services. Some of the most important areas involved include (but are not limited to) energy providers, sustainable mobility and health care.

Regarding Industry 4.0, there are some barriers, due to which many companies are still reluctant to engage. As we can see in the following graph, "data protection and security" constitute one of the biggest obstacles that must be tackled in order to advance change and encourage acceptance of new devices for goods and services within this new industrial revolution.(Graph 1)

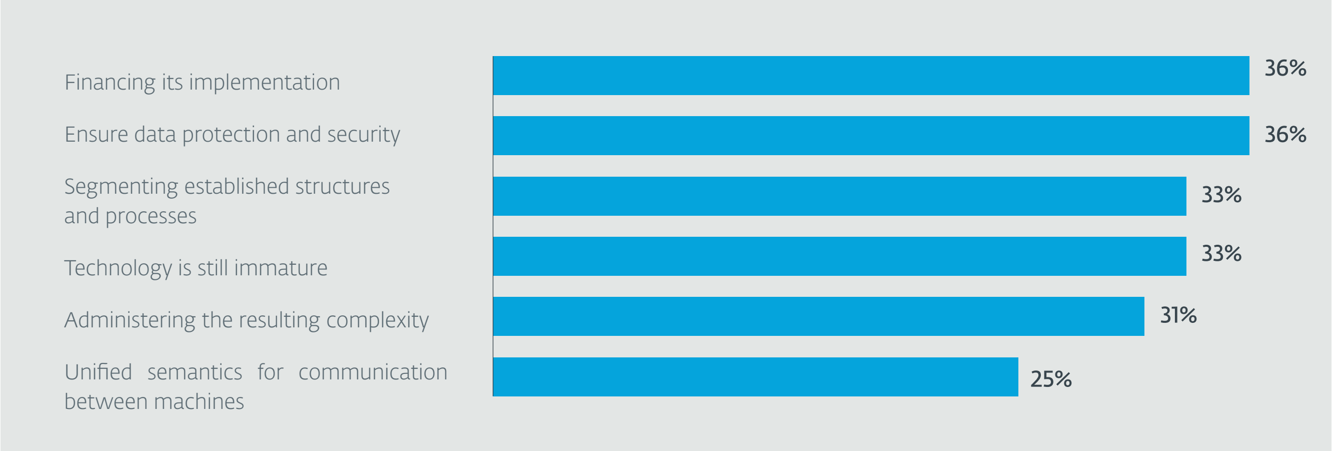
Every time a new technology emerges, researchers test it to understand how it works and, in some cases, to find out how its security can be violated. Throughout 2015, multiple reports have been seen of vulnerabilities in IoT devices, from baby monitors to cars remotely controlled via the Internet. *Both consumers and companies are concerned, and taking action towards achieving IoT security.* Securing these devices will be one of the biggest challenges in 2016 for information security suppliers.

Wearables

In 2015, many reports were prepared concerning vulnerabilities in wearables, presenting scenarios that would enable an attacker *to steal information from the device itself.* Among the attack vectors used, some failures have been found in applications and in the use of communication technologies such as *Bluetooth and the use of six-digit PIN codes.*

Bluetooth Smart is widely accepted in the IoT industry and its security is , therefore a key factor in the interconnection of devices. From smart watches to wrist-worn devices measuring sensory data during physical activities, this technology is used to connect with other devices such as smartphones. A security failure in the protocol might enable attackers to read

Graph 1 Obstacles to implementation of Industry 4.0



Source: IDC 2014; n=154 – Only companies which are acquainted with the concept of "Industry 4.0".

in plain text the information being exchanged among them.

Some of these incidents have attracted the attention of users, particularly since the *market launch of the Apple Watch.* In this respect, it was observed that software failures might offer the opportunity for a *cybercriminal to reset an Apple Watch* and to reconnect it to another iPhone without any problem, regardless of whether a security PIN had been set before the attack.

Interconnecting homes

IoT advances allow more devices to be interconnected through a single household network. In this way, users can connect their smartphones and computers to manage and communicate with other networked household appliances, all of which improves technology experience and equipment usability. In addition, in view of the higher-level of interconnection, improved security should be taken into account to maintain the privacy of data, protect communication protocols and ensure the integrity of application and operating system updates.

In September 2014, at the Virus Bulletin conference in Seattle, Jeong Wook Oh of HP *presented comprehensive research* on various devices used in homes and the feasibility of attacks on them. Today we can find TV sets, thermostats, IP cameras and other devices in the home that have Internet connections, and in the event of a security failure, a family's personal information or systems may become exposed.

This *research* also comprised cases of different household devices, and based on what has been reported in the last few years, it is possible to see this trend in IoT.

Along these lines, Smart TVs from various makers were considered by researchers at the **BlackHat 2013** conference, and the same researchers are still continuing to prepare reports on failures in this type of devices. In recent reports, we can see how a fridge may become the gateway for enabling cybercriminals to steal Google credentials. Moreover, a *baby monitor can be controlled remotely to play music* or even to access the network to which it is connected.

In view of the rapid evolution of technology, more security failures will be found in such devices – in which case their implementation within a household network will not be the best option. However, we should not be afraid of technology; on the contrary, it is important to become aware of and well-informed about its implications.

Today, many more devices are connected to household networks than was the case five or ten years ago. Therefore, all companies dedicated to information security understand the resulting challenges, especially with respect to helping users find simple but effective protection for their household network. As their devices get smarter, device owners should be checking their security by using device manuals, as well as tips and guides from trusted advisors.

→
We should not be afraid of technology; on the contrary, it is important to become aware of and well-informed about its implications.

Interconnectivity of all things

For the future, the challenge for security in IoT is not restricted to the household. Technology keeps improving and time and time again we see how governments, industries and markets in general are turning towards interconnectivity for all equipment, systems, and services. From market research to traffic systems, all things are being interconnected through existing technologies but, in certain cases, without the proper implementation of security protocols.

In the report *"Trends for 2015: Targeting the corporate world"*, by ESET Latin America's Research Laboratory, we mentioned that one of IoT's goals is to generate self-governing environments that can provide information and services by interacting with technology. To achieve this objective, various companies have started to implement reward programs for security experts so that they report security failures, as a way to provide their customers with better security, privacy and usability for their devices.

IoT challenges were a major topic of discussion throughout 2015; as a consequence, according to various announcements, companies are now working on standards and regulations to integrate the Internet of Things into industries, cities, and different areas with the purpose of improving their residents' lifestyle. Some examples of this are the investments proposed by the German Government and the Industry 4.0 initiative mentioned above, as well as the cooperation undertaken by the *European Network and Information Security Agency (ENISA)* towards helping to develop *good practices in emerging smart critical infrastructures.*

Ensure, then connect

2016 will be a year of security challenges, with new devices being connected to the Internet or enabling different ways of intercommunication - whether it's a *car that can be controlled remotely,* or security failures in drones, or the ways in which users protect their household networks. Any connected device should be checked to ensure that it's protected and properly set up to ensure the future privacy, security, and confidentiality of users, companies and government agencies.

There will be differences between how users and companies protect their information in all those devices onto which a security solution cannot be installed, a scenario that turns protection of the network into a critical factor. In the case of a household network, one of the most important points to take into account is the router, the device which provides access to Internet, and yet which is often disregarded, not updated, and often doesn't even have its default password changed.

If the device providing 24/7 Internet access in a house is not safe, the network may become adversely affected: a prominent example was reported by ESET's Laboratory concerning *Linux/Moose*, which was found to be changing the behavior of the affected networks.

At the same time, the integration of new networked devices should be taken into account by IT teams to guarantee that they do not become an entry point for non-authorized third parties that may bring about security incidents and loopholes.

In the current state of affairs as regards security, we have discussed and presented the highest-impact incidents worldwide, ranging from targeted attacks to cases of massive infection by malicious code. If we consider the recently-reported incidents and the security failures usually exploited by attackers, we can conclude that if a new range of smart devices is added to a corporate network, security will play an increasingly important and significant role. Providing security for any device connected to a corporate environment is a most difficult task for security equipment, and for the near future, IoT's role will become increasingly significant for those businesses that consider information security as one of the keys to maintaining their business operations.

> FOR THE NEAR FUTURE, IOT'S ROLE WILL BECOME INCREASINGLY SIGNIFICANT FOR THOSE BUSINESSES THAT CONSIDER INFORMATION SECURITY AS ONE OF THE KEYS TO MAINTAINING THEIR BUSINESS OPERATIONS

3

Ransomware: first files... now complete devices

- Varieties of ransomware
- The increase in the number of variants
- Evolution of threats
- From the computer to the TV
- Conclusion: the same goal for another threat

Author
Camilo Gutiérrez
Amaya

3 RANSOMWARE: FIRST FILES... NOW COMPLETE DEVICES

One of the main threats to computer security is malicious code. In fact, over the years it has become one of the main causes of security incidents; from the first viruses in 1986 to the most sophisticated malware of today. And this type of malware, although it is not new, has become increasingly troublesome for both businesses and home users.

→ This type of malware, although it is not new, has become increasingly troublesome for both businesses and home users.

Varieties of ransomware

Over the past year, cases of ransomware have gained importance in the field of computer security due to growth in the number of victims, which is in turn due to the significant profits that cybercriminals can obtain from this type of malicious campaign.

This form of attack may seem innovative, but it is not. In fact, the first widely-known case of ransomware *goes back 25 years*; the 'AIDS trojan' was malware that hid directories and encrypted the names of all the files on the C drive, thus making the system unusable. The victims were then requested to "renew their license" with a payment of 189 U.S. dollars. Since then, new programs seeking to extort money from users have been identified which, unlike PC Cyborg's symmetric encryption, used asymmetric encryption algorithms with larger keys. In 2005 GPCoder, and its subsequent variants, after encrypting files with specific extensions, requested a payment ranging from 100 to 200 U.S. dollars to recover the information.

However, this type of malicious code goes further and, in fact, there are groups of cybercriminals offering this kind of malware as a service. *Ransomware as a Service* (RaaS) has been discovered through *the prominence* of tools to create ransomware automatically, allowing criminals to create this type of malware automatically, regardless of their technical expertise. Similarly, with the recent news of the publication of *Hidden Tear, the first open source ransomware*, a new window has opened for the development of such malware and its variants, so we predict the creation of increasingly sophisticated and massively prevalent malware

The increase in the number of variants

One of the highlights of ransomware evolution is the growth in the number of variants seen in recent years, targeting various platforms and technologies. The following chart shows that, as you might expect, Windows-related families are the ones that have been showing a year-on-year growth in terms of the number of detections.(Graph 2)

But, in addition to Windows, variants have also been designed for other operating systems. Such is the case with OS X since, during 2015, variants of the families of Filecoders unique to these systems were detected.

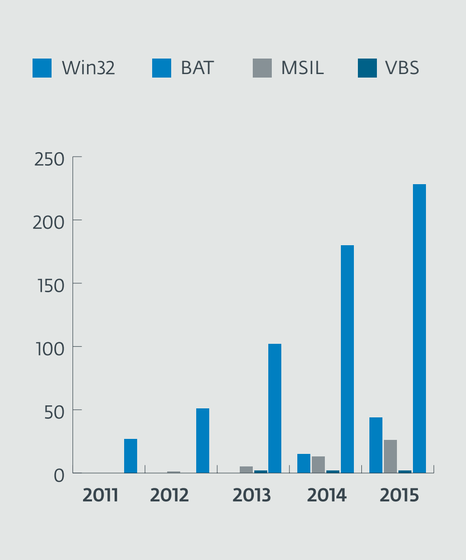
Other technologies such as VBS, Python, BAT and PowerShell are also used by cybercriminals to compromise users' systems for profit.

Evolution of threats

Although until now operating systems for desktop computers or laptops have been discussed, these are not the only platforms that are exposed to this threat. Cases of ransomware were also found to

Graph 2

Title: Growth of variants for the Filecoder family (in the last 5 years)



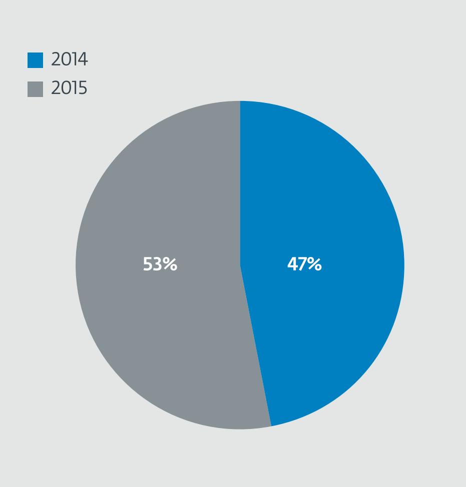
affect mobile devices, particularly those running Android, because that is the mobile operating system with the most users worldwide.

The first Android-targeting families included fake antivirus with the ability to lock the screens of the devices. In 2014 *Simplocker*, the first ransomware for Android activated in Tor that encrypts user files directly, was discovered by ESET. In fact, the number of malware families detected during 2015 is four percent higher compared to the number detected during 2014. A small percentage increase in malware families can represent a huge increase in individual samples. (Graph 3)

During 2015, ESET researchers discovered the *first type of ransomware for Android to lock the screen:* this modifies the phone unlock code to prevent the owner accessing his own device. This is a significant difference from the first Trojans to lock Android screens, which constantly put up windows, displaying the demand for ransom, in an infinite loop in the foreground. As this mechanism was not technically very complex, it was easily bypassed by users with a little knowledge, so cybercriminals stepped up their efforts and created new ransomware families intended to block access to the device. These new families, such as the one detected by ESET as LockerPIN, deprive users of an effective way to regain access to their devices without root privileges or an already-installed security management solution.

Graph 3

Title: Distribution of the amount of Simplocker's variants detected in the last 2 years



However, Android is not the only platform on which ransomware has evolved. In 2013 *CryptoLocker* rose to prominence due to the number of infections generated in various countries. Among its key features is encryption using RSA 2048-bit public key algorithms, targeting only files with certain filename extensions, as well as communication with the Command and Control (C&C) through the anonymous network *Tor*.

In 2015, a new wave of ransomware was identified with the appearance of CTB-Locker, downloaded to the victim's computer using a TrojanDownloader, as witnessed in January 2015 with Win32/TrojanDownloader.Elenoocka. Among its various versions, there was **one with messages and payment instructions targeting Spanish-speaking countries.**

These developments lead us to believe that ransomware has not yet found a limit as to the number of victims that could be reached and the complexity that its code and forms of attack it could attain. It seems that this type of malicious code is here to stay and will surely continue mutating in the coming years.

From the computer to the TV

So far, the evolution of this threat is evident by its large number of variants, with increasingly complex mechanisms that make it almost impossible to retrieve the information unless payment is made to the attacker - a practice that fosters criminality. It's even possible that the victim might pay without receiving a recovery key - or that there is some kind of legitimate technical support that wouldn't even be able to recover the files, as it is not susceptible to a brute force attack.

The threat has also diversified in terms of approach and vector. In the last months of 2015 there has been a significant growth in ransomware that focuses on equipment associated with the Internet of Things (IoT). Various devices, such as watches or smart televisions, are likely to be affected by malicious software of this type, mainly those which operate on Android.

But IoT encompasses more than watches and televisions; products ranging from automobiles to refrigerators already have the ability to connect to the Internet and all their operations are controlled by some form of CPU (Central Processing Unit). In other words, they are computerized. While there are many devices for which no threats have yet been found, their operation involves a software or firmware component and an Internet connection. Attackers may therefore be attracted to them and may be able to misuse them in order to obtain valuable information.

Proof-of-concept tests have already been performed where, for example, control of an automobile has been successfully affected totally remotely. For this reason, if the necessary precautions are not taken by manufacturers and users, there is nothing to prevent an attacker from seizing control of a device's functionality and demanding money to return it. Perhaps this is not a threat that we expect to see much of in the near future, but we shouldn't lose sight of it if we are to avoid serious problems later.

Conclusion: the same goal for another threat

In recent years, the seizure of information stored by users and companies on various platforms has become one of the most important trends. The impact it can have on users, by preventing them from accessing all their information due to the action of malicious code, is of growing concern. It is one of the most important types of security incidents, as it takes full advantage of cases where a company's lack of an effective backup strategy and

→ In the last months of 2015 there has been a significant growth in ransomware that focuses on equipment associated with the Internet of Things (IoT).

ineffective security implementation exposes it to risk.

Unfortunately, the success of this type of attack for cybercriminals has not only led them to extend it beyond the Windows systems and mobile devices, but its increasing impact has made it one of the greatest current concerns of consumers and companies alike. During 2015, we have seen large ransomware campaigns in multiple languages, as was the case with CTB-Locker in January 2015, which must not be seen as an isolated event. Cybercriminals seek to convince users to accede to their threats by encrypting their files and seizing their information, and this is something that is likely to continue happening.

As technology has evolved, the protection mechanisms to counter threats such as ransomware have improved based on experience, and they must be accompanied by user management and education. However, not all devices can be protected with a security solution, and this threatens to become a future risk for consumers and companies. Based on these points, by 2016, we expect to continue seeing ransomware campaigns, trying to exploit new attack surfaces by prohibiting users from accessing their information or services. The increasing trend toward more and more devices being supplied with an Internet connection provides cybercriminals with a greater variety of devices that might be attacked.

From the security side, the challenge is not only to detect and block or remove such attacks, but also to ensure the continuing availability of information. In the near future, network security, the prevention of exploits and the appropriate configuration of devices will take on greater importance to prevent such attacks, so that users can enjoy the technology: we are on our *way towards a fivefold increase in the number of devices connected to Internet over the next five years, thus reaching 25 billion online devices,* so the challenge is to protect them properly against this type of attack.

> THE CHALLENGE IS NOT ONLY TO DETECT AND BLOCK OR REMOVE SUCH ATTACKS, BUT ALSO TO ENSURE THE CONTINUING AVAILABILITY OF INFORMATION

→ During 2015, we have seen large ransomware campaigns in multiple languages.

4

Targeted attacks:

implications, reasons and objectives

- Kits for cyber espionage?
- Attacks on users and specific systems
- Are APTs considered to be the weapons of the future?

Author
Pablo Ramos

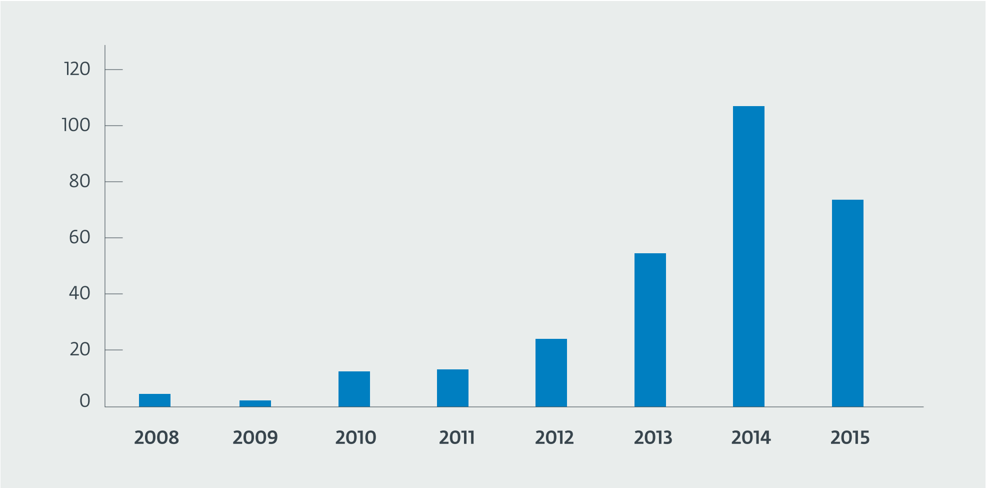
4 TARGETED ATTACKS: IMPLICATIONS, REASONS AND OBJECTIVES

In the last few years a series of attacks categorized as *APTs (Advanced Persistent Threats)* have been reported. When this terminology is used, it means that we are not talking about ordinary malware campaigns, which are intended to spread as widely as possible, but about attacks with a more specific objective. In the report *"Trends for 2015: Targeting the Corporate World"* we discussed the impact APTs have on the security of companies and how they became one of the biggest challenges an organization may face in terms of information security.

In 2015 the trend continued, and reports of targeted attacks, APTs and "*sponsored malware*" (that is, campaigns where there is a government or entity behind the attack) generated debate around the world. *APTNotes*, a repository of *GitHub* created and maintained by the security community, has collected published reports about targeted attacks since 2008. Based on the latest update, in August 2015, a cumulative total of 291 targeted campaigns had been observed against companies, institutions and governments. Seventy-three of these were observed during 2015, more than double the number seen in the same period of the previous year, and a similar quantity to that seen in the second half of 2014. (Graph 4)

Beyond the growth in reports of targeted attacks or APTs, 2015 witnessed specific attacks generating controversy on the basis of the information that was leaked. One of the most important of such cases was the *Hacking Team incident, when about 400GB of information was leaked from the Team's servers*, thus causing a great stir about the list of tools the company marketed, and its customers. In consequence, continued attention was drawn to the incorporation of various leaked Hacking Team exploits into malware by different cybercriminals, as was the case for the *APT group Sednit, who incorporated these exploits in their arsenal within a very short time*, as did the *Webky group*.

Graph 4 APTs reports



Graph 4 - reports of APTs - source: https://github.com/kbandla/APTnotes

In addition, *the Ashley Madison* leakage of *data belonging to 37 million of its users* also generated a huge impact on this service's clients. The strategy of Impact Team, which perpetrated this attack, was to force the company to stop providing its services and, due to the initial lack of response to its demands, *the team published Ashley Madison users' details on the web,* by initiating a series of *blackmail campaigns and spreading threats against victims.*

These targeted attacks have various objectives, which vary according to the actors behind each incident. ESET Research Labs analyzed cases on a global scale, directed against certain countries, regions or organizations; among the most important events of 2015, we noted *Potao Express*, *Animal Farm*, *Terracotta VPN*, *Mumblehard* and *Carbanak*, among others.

→ These targeted attacks have various objectives, which vary according to the actors behind each incident.

Kits for cyber espionage?

The first mentioned case was the ***Potao Express Operation,*** a campaign of specific malware using multiple tools for cyber espionage. It focused mainly on targets in the Ukraine, but also targeted other countries of the Commonwealth of Independent States (CIS), including Russia, Georgia, and Belarus. Among its targets were various sectors of the Ukrainian government, Ukrainian military institutions and even news agencies in the country.

This family of malware, known as Win32/***Potao,*** has a modular structure that allows the attackers to choose different tools according to the action they decide to perform, based on their objective. Potao was first seen in 2011, but it had more of an impact during 2014 and continued to launch campaigns throughout 2015. The increase of Potao detections is related to the addition of USB drives as a threat vector, functionality that was observed for the first time in October 2013.

On the topic of targeted threats or campaigns, we should also mention the group called Animal Farm, which was known to create malware families such as *Dino*, *Casper*, *Bunny* and *Babar*. Each of these families of malware was reported in the course of 2015 and identified in targeted campaigns that date back to April 2014, as reported by ESET researcher Joan Calvet. In some particular cases, such as Babar, reports date back to 2009, which shows clearly how persistent this type of attack and/or targeted campaign is.

The relationship between the four families of malware was established based on the findings reported in April 2015 about similarities in the ***Babar*** and ***Bunny*** coding which were then seen in ***Casper*** and ***Dino,*** analysis by Communications Security Establishment Canada suggests an operation whose targets might have been *systems in Iran and Syria.*

Attacks on users and specific systems

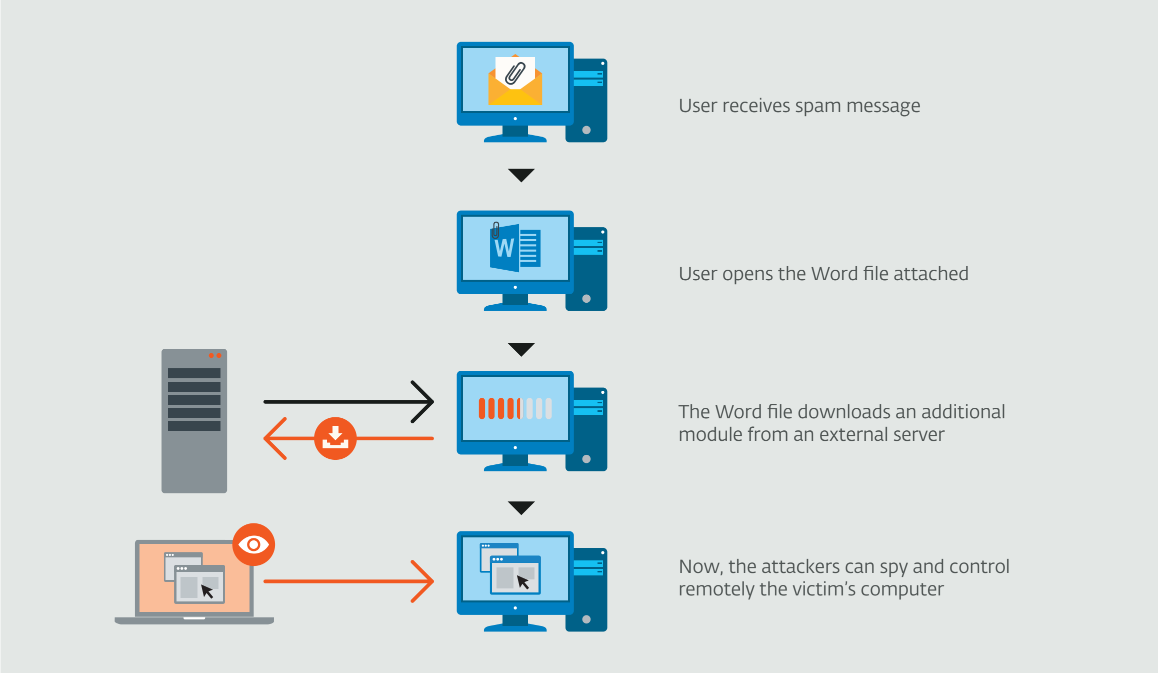
Another research topic that caused a big stir was *Operation Buhtrap*, whose targets were various Russian banks. In this campaign, which was discovered at the end of 2014, the attackers only installed their threats into systems set up to use Russian as their default language.

In this case, attackers exploited a *vulnerability in Microsoft Word* as an infection vector for more than three years. Based on the analysis of detections of malware families associated with these campaigns, it seems that 88% of victims are in Russia. Although this way of operating was in part similar to most global malware campaigns, such as Operation Liberpy, the objectives were specific to Buhtrap. (Graph 5)

During the first few days of November 2015, threat propagation campaigns were detected again as part of Operation Buhtrap, spread by compromising a well-known legitimate website. In this case, the approach was broader but equally oriented towards Russian users, using *spear-phishing* techniques. The first malware detected was the Lurk downloader, distributed on October 26. Then Corebot appeared on October 29, Buhtrap on October 30, and finally Ranbyus and RAT Netwire on November 2.

Up to this point, all the campaigns presented in this section were particularly oriented to Windows systems and aimed at stealing confidential information from users, spying on their activities or collecting information. However, this was not all that happened in 2015, since different research initiatives have identified campaigns that have run for more than five years, targeting Unix-based servers, in order to send spam. In this category, we found Linux/Mumblehard, malware developed in Perl with two main components: the first is a backdoor that provides attackers with remote access, while the second is a daemon responsible for sending spam. When ESET researchers estimated its size, they realized that they were connected to the sinkhole from 8,500 unique IP addresses, and that in early April 2015, its size was approximately three thousand systems, mainly servers.

Graph 5 Structure of a Buhtrap campaign


User receives spam message
User opens the Word file attached
The Word file downloads an additional module from an external server
Now, the attackers can spy and control remotely the victim's computer

Our Trends Report for 2015 previously addressed *Operation Windigo*, affecting more than 500,000 systems via propagation campaigns all over the world.
Specific campaigns against web servers or other Internet services are intended by cybercriminals to augment their attacks and, in many cases, to go unnoticed so as to keep their activities alive for the longest possible time. In addition to attacks described on these pages, there have been many other reports of targeted attacks, in which companies, institutions or governments observed the exfiltration of their information. In order to combat this type of event, companies need to improve their defenses and computer security processes..

Are APTs considered to be the weapons of the future?

Whenever we refer to targeted attacks or malware campaigns for a specific purpose, there are always enquires from companies who want to know whether they have been the targets and/or victims. It is very difficult to predict when or how a company will become the target of a group of cybercriminals, so they must be always prepared and protected for that eventuality, given that the point of security installations and software is to protect companies from any type of attack, directed or not.

The IT security of a company is, more and more, a key factor for its continued operation, as evidenced in this section by the impact that data leaks have had on some companies. For this reason, the best approach that a company, institution or government can implement as regards IT security is to be proactive: assessment of its defenses, empowerment of its users, and training of its teams are among the actions that need to be taken to minimize exposure to the risk of a security breach.

But, how should we protect companies from an attack that is unknown until it happens (and maybe for some time afterwards)? Our report on trends for 2015 asserted that businesses are an increasingly tempting target for attackers, an expectation that was confirmed throughout 2015 and strengthened with the emergence of attacks such as those mentioned above.

Protecting a company is not a project; it is a process. The technologies used to protect endpoints should be evaluated on an ongoing basis by a security team, as should the protection of the perimeter and servers. Encryption helps to protect confidential information, and it is not a very common defense measure adopted by small or medium-sized companies. In addition to protecting systems and networks, or relying on the encryption of important, sensitive, and/or confidential information, the management and education of users further helps protect the organization. In other words, management is necessary to understand the business and role of safety, in order to ensure its continuity, and thus decide to invest and use technological resources to protect the business. Additionally, users should be included and trained to play their part in information security processes through awareness workshops, internal courses or practices to assess their security awareness when it comes to protecting their company's assets.

→
It is very difficult to predict when or how a company will become the target of a group of cybercriminals.

5

Crimeware, malware and massive campaigns around the world

- Botnets, zombies and global campaigns
- New families, new techniques, but the same goals
- Collaboration is the key to fighting cybercrime
- Where are we going?

Author
Pablo Ramos

5 CRIMEWARE, MALWARE AND MASSIVE CAMPAIGNS AROUND THE WORLD

Within the world of IT security, one of the biggest concerns for companies and users is malicious code that can compromise their systems and/or information networks. This concern is not at all unfounded, as cases of malware, and crimeware incidents are reported daily and around the world. Indeed, the number of reports, detections and threats observed by the various antivirus laboratories grows constantly and daily, and shows increasing diversity.

2015 was no exception, and not only was the growth of cybercrime observed worldwide but we also saw a change in its aggressiveness and in the types of attack (see the section of this report dedicated to ransomware).

IOCTA (Internet Organized Crime Threat Assessment) reported a shift in the way attackers acted, focusing on confrontation as one of the most important changes, ranging from the actions of zombie computer networks that seek to infect users' systems with ransomware variants so as to extort money from them, to cybercriminals who used physical force to intimidate security companies into not exposing their threats.

When speaking of malware campaigns, we do not mean directed attacks or APTs (Advanced Persistent Threats), but the mass propagation of malware commonly used to steal information from users and companies. 2015 presented different challenges for identifying and blocking mass campaigns of spreading malware through channels such as email, mass storage devices or compromised websites that redirect their visitors to different types of exploits. The increasingly rapid changes in code and the volume of threats that affect companies are some of the challenges that victims have to face.

The cybercrime ecosystem has different actors who cover a wide framework of criminal activity involving goods and services that provide infrastructural support for malicious action. Such actions, involving banking Trojans and RATs (Remote Access Tools) were the subject of several investigations on the part of security agencies.

However, cyber criminals continue to find ways to reach users. Such is the case with regionalized malware campaigns like Operation Liberpy, initially spread through email; Operation Buhtrap, infecting its victims through compromised websites that served malware installers; Brolux**,** a Trojan that attacked Japanese online banking sites; and cases with global impact such as Dridex.

It is important to stress that these campaigns affect not only home users, but "small businesses, medium-sized companies, and even large enterprises. According to the latest report by the Ponemon Institute, the average cost of these incidents was USD 7.7 million for the first half of 2015. Some of the companies cited in the report lost up to USD 65 million as a consequence of security incidents they suffered.

→
The cybercrime ecosystem has different actors who cover a wide framework of criminal activity.

Botnets, zombies and global campaigns

Zombie computer networks, also known as botnets, have for several years been the most important infrastructural component in the world of cybercrime actors. Their role in the world of cybercrime is central, within a model where the purchase and sale of services, information theft or campaigns spreading ransomware are facilitated by botnets. In other words, hundreds or thousands of computers that are part of such networks are used for sending spam, launching Denial of Service attacks, and performing other malicious actions.

The threat impact of botnets has led to the conducting of in-depth studies on how to identify their behavior: that is, how to identify patterns that allow security teams to detect and block connections within their networks. Moreover, there are security solutions such as those offered by ESET, which include functionalities capable of recognizing these communications, in order to block them and prevent information theft.

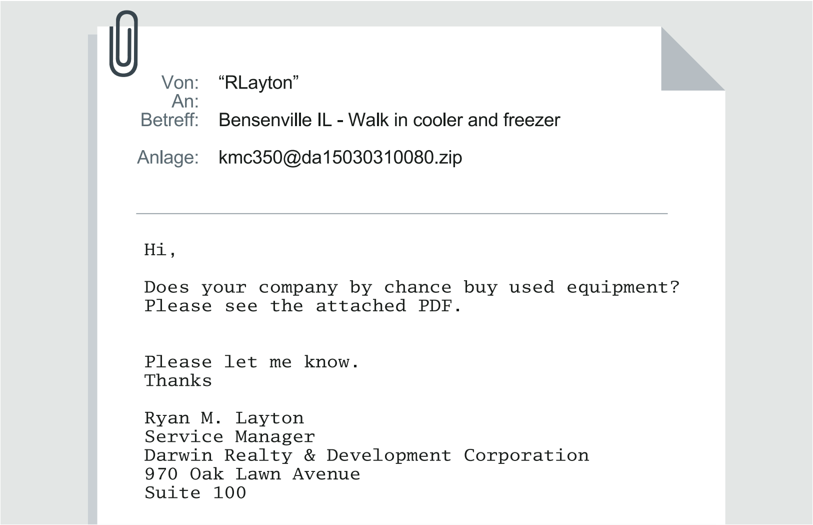
As for botnets dedicated to information theft, ESET Research Laboratories this year reported the actions of Operation Liberpy, a keystroke logger installed on more than 2,000 machines in Latin America – 96% in Venezuela – that stole credentials from its victims for more than eight months. This threat, detected as ***Python/Liberpy,*** initially spread through emails and then continued to spread via USB devices, taking advantage of Windows shortcut files to infect new systems. This latter propagation method is similar to that used by other families as *Bondat*, *Dorkbot* and Remtasu, all mainly active in Latin America.

Some campaigns are not directed at any particular country, but aim to spread to as many systems as possible. One of the cases reported during 2015 was *Waski*, a global campaign that sought to install banking Trojans worldwide to compromise victims' systems with a variant of *Win32/Battdil*. The campaign started by sending emails that attempted to trick users into opening a document that would do nothing but infect their system. (Graph 6)

Email is one of the main vectors for spreading malicious code and, as in 2014, there were multiple reports in 2015 of massive mail campaigns related to banking Trojans such as *Dridex* through Microsoft Office documents infested with malicious macros, or the spread of ransomware, such as the waves of *CTB-locker* in mid-January that reached so many users' Inboxes.

Graph 6

False e-mail that infects system with Waski



Von: "RLayton"
An:
Betreff: Bensenville IL - Walk in cooler and freezer
Anlage: kmc350@da15030310080.zip

```
Hi,

Does your company by chance buy used equipment?
Please see the attached PDF.


Please let me know.
Thanks

Ryan M. Layton
Service Manager
Darwin Realty & Development Corporation
970 Oak Lawn Avenue
Suite 100
```

Although during 2015 we have seen many *joint operations between security agencies,* businesses and governments to disrupt or dismantle these criminal networks, we expect to see botnets continue to be a threat and a risk for organizations and users around the world during 2016.

New families, new techniques, but the same goals

Throughout 2015, the emergence of new families of malicious code or even the incorporation of new features into previously known Trojans were reported, such as the case of CoreBot, which added to its capabilities the opportunity to steal banking information from its victims. *The evolution of families of malicious code* to incorporate new modules or tools is constant, and part of the world of cybercrime.

Botnets were not the only area of innovation where new families of malware code appeared. As noted in last year's trends *document*, Point Of Sale Malware was one of the types of malicious code where new players appeared, as was the case with *PoSeidon*. This code attacks retail outlets and attempts to compromise terminals that take credit card payments and to scan its memory so as to "scrape" card data. Another instance of PoS malware was Punkey, which appeared a month after PoSeidon and was reported at more than 75 different IP addresses, filtering information from credit cards.

Incidents involving this kind of threat – including cases reported last year such as *Home Depot*, UPS or *Target* – showed that cybercriminals seek to access large retail chains to infect outlets and thus steal data from millions of credit cards. Such incidents accelerated the need for a reassessment of how *PoS machines are protected* and brought to light some curious cases, such as that of *certain manufacturers who used the same default password* for 26 years.

At other times, cybercriminals have abused flaws in websites or even *fake game pages, where they hosted copies of their malicious code*. Through CMS (Content Management System) plugin flaws, the attackers breached the security of thousands of websites so as to use them to host content harmful for users.

Collaboration is the key to fighting cybercrime

Enforcement agencies and businesses around the world collaborate to fight cybercrime and make the Internet a safer place. During 2015, in addition to *announcements by Europol on how threatening cybercrime has become*, joint operations have been performed to disrupt or dismantle networks of zombie computers.

Some of these operations, coordinated and distributed around the world, successfully culminated in cases such as the dismantling of Dridex, Liberpy, *Ramnit*, and the arrest of the creator of the Gozi Trojan. In addition to this direct action against certain families of malware, the security agencies also succeeded in arresting a number of cybercriminals associated with criminal forums, such as the case of *Darkode* where 62 people in 18 countries were arrested for various computer crimes.

→

Some of the companies lost up to USD 65 million as a consequence of security incidents they suffered.

Where are we going?

To summarize the most important events of recent times in terms of more general-purpose malware, we can see that the barrier separating it from directed attacks is becoming more transparent. Cybercriminals continue to employ different propagation techniques in order to infect as many systems as they possibly can, either by *incorporating newly-discovered vulnerabilities into different Exploit Kits or by using campaigns to spread malware.*

In other words, the evolution of cybercrime continues to threaten users, and malware-spreading campaigns have grown in scale and achieved different levels of effectiveness. To combat these actions, the collaboration of experts, security agencies and other entities is key to disrupting cybercrime and helping users to enjoy the Internet without undue anxiety.

2016 will continue to reveal the further development of families of malicious code, either in new variants or in the incorporation of features that they did not have before. Cybercrime has become more threatening, *companies globally have increased their investment in security by 4.7%*, and security agencies are enhancing their efforts to take down botnets and to put cybercriminals behind the bars. In other words, 2016 will present new security challenges, but also a more active and organized front in the fight against cybercrime.

→

We can see that the barrier separating general purpose malware from directed attacks is becoming more transparent.

> 2016 WILL PRESENT NEW SECURITY CHALLENGES, BUT ALSO A MORE ACTIVE AND ORGANIZED FRONT IN THE FIGHT AGAINST CYBERCRIME

6

Haxposure:
an emerging threat with important implications

- Haxposed: Damaging company secrets and innocent customer
- The implications of haxposure
- Haxposure 2016?

Author
Stephen Cobb

6 HAXPOSURE: AN EMERGING THREAT WITH IMPORTANT IMPLICATIONS

One 2015 cyber threat trend was not widespread, but deserves attention because of a pair of high profile security breaches: Hacking Team and Ashley Madison. In both cases the perpetrators of the breach not only stole confidential information, they published it to the world. This combination of criminal data theft via hacking and public exposure of internal secrets represents an emerging threat – which I have dubbed *haxposure*. I see haxposure as categorically different from data theft for resale, a much more common type of hack. Data theft is epitomized by the 2013 Target payment card and 2014-15 Blue Cross insurance policyholder breaches. In this article we discuss how haxposure differs from other threats, why it may be on the rise, and what organizations should be doing to protect against it..

→ Haxposure is categorically different from data theft for resale.

Haxposed: Damaging company secrets and innocent customer

In July of 2015, some 400 gigabytes of information were stolen from Italian security company Hacking Team and published. In an unconnected incident later that month, a group calling itself Impact Team published a subset of account data stolen from Canadian firm Avid Life Media that operates the Ashley Madison website which promises to connect men and women who want to have an affair. The hackers demanded the website be shut down. When that didn't happen, they released gigabytes of internal data in August, causing embarrassment to some individuals, and providing evidence for lawsuits against the company. The publication of the data also made the HT hackers the center of a large law enforcement operation and the target of a large reward.

What the Hacking Team and Ashley Madison incidents have in common is that a security breach led to exposure of secrets that were damaging to the reputation and business model of the organization. In the case of Hacking Team, the exposed data appeared to prove that the company had been selling its digital surveillance tools to repressive regimes, despite the company's past claims to the contrary. In the case of Ashley Madison, the exposed data appeared to prove claims that the company did not remove customers from its database, despite charging them money to do so. The exposed data also supported allegations that a lot of female participation was fabricated, seriously undermining the company's credibility and its claim to facilitate affairs.

In both cases, it would appear that the people behind the attacks were unhappy with the business models of the targeted companies. This led me to draw some parallels with the Sony Pictures hack of 2014 in an August 2015 webinar that addressed some of the enterprise security implications. Whatever the true motives for the Sony Pictures attack, there is no doubt that it exposed some confidential information that did not reflect well on the company and its executives. Given that there appeared to be a political/moral motive to all three incidents, I was tempted to see them as a new level of hacktivism. Early acts of hacktivism tended to be website defacements (for example, Kriegsman Fur in 1996: warning adult language). The practice of doxing also emerged, the researching and broadcasting personally identifiable information about an individual; however, unpleasant as doxing can be, it is quantitatively different from, and less damaging than haxposure.

Hactivism became more aggressive about 10 years ago. The 2008 *Project Chanology* protests associated with Anonymous used distributed denial of service (DDoS) attacks, along with some exposure of internal communications of the targeted organization.

Of course, it is reasonable to argue that genuine hacktivism does not include ransom demands, which attackers made in the case of Ashley Madison and Sony. When data thieves issue demands in return for not publishing internal company information they compound thievery with extortion, going beyond the ethical pale as far as most activist creeds are concerned. And when the threat involves exposing personally identifiable information belonging to employees or customers of the organization you enter a whole new level of irresponsibility.

→ Genuine hacktivism does not include ransom demands, which attackers made in the case of Ashley Madison and Sony.

The implications of haxposure

Whether or not the Hacking Team and Ashley Madison attacks qualify as hacktivism, the strategy of haxposure represents a potentially more damaging threat to an organization than data being looted and sold to people who secretly exploit them. The damage potential is a function of the sensitivity of the data you are trying to secure, where *secure* = *keep secret*. Consider a scenario in which you are a food company and hackers steal your secret recipe for baked beans. If they sell it to one of your competitors or publish it on the internet, that is bad news, but it probably won't sink your company. Unless your secret recipe contains a harmful secret. Suppose one of your secret ingredients is a banned carcinogen. Exposure of that kind of secret can seriously damage reputation, revenue, and valuation.

Several factors have combined in recent years to increase the risk of companies keeping harmful secrets:

1. Access to hacking:
anyone can hire a hacker. Gone are the days when only a few technically skilled persons were capable of performing acts of digital disruption, and when the only disgruntled employees capable of digital revenge were in the IT department. Nowadays, hacking attacks are an option for anyone who has a beef with your organization, regardless of their technical knowledge and hacking skills.

2. Access to open source intelligence:
when you use the Internet to advertise your business you expose your business to the world. The full implications of this reality continue to elude some business folk. To be clear: You cannot use the World Wide Web to promote controversial goods and services to a select group of people; that is not how the Web works. Whether you are selling furs or rhinoceros horn powder or surveillance tools that can be abused by repressive regimes, trying to do so discreetly via the Web is not possible; history and logic clearly show that when you try this, your business will be discovered by critics, explored, and possibly exposed.

3. Publication tools abound:
sites like Wikileaks and Pastebin enable anonymous publication of stolen information, reducing risks for those who engage in haxposure.

4. Appetite for anger:
the global reach of social media, which can act as an amplifier for outrage – sometimes in the absence of supporting data – can be an attractive platform for the crusading hacker, increasing the spread and impact of published secrets.

5. Complexity is the enemy of security and secrecy:
it is clear that keeping secrets is hard when they are kept in digital form. Complex systems typically contain multiple unpatched vulnerabilities that are known and can be exploited, plus some number of zero-day exploits that are not known, much less patched. Furthermore, digital secrets are much easier to exfiltrate, potentially a mere blip in outbound network traffic, or a tiny piece of physical media. Remember when *VW was accused of stealing secrets from GM* back in the 1990s? The information allegedly stolen included 20 boxes exfiltrated by plane. While the secret nature of the paper information was denied by the person at the center of the incident, that much data, in digital form, could today fit on a flash drive smaller that a postage stamp, and much easier to exfiltrate.

What are the implications of these factors? First and foremost they underline the need to get the security basics right. You are definitely going to need, at a minimum:

- Strong authentication, anti-malware, and encryption (these could have limited damage for both Hacking Team and Ashley Madison).
- Backup and disaster recovery plans and capabilities.
- An incident response plan (lack thereof was apparent at Sony Pictures and Avid Media).
- Insider threat monitoring (one trusted party with privileged access can cause way more trouble than thousands of external attackers – see Snowden v. NSA).

Beyond these basic security techniques, there are strategic factors that need to be adjusted to address the threat of haxposure:

- Risk assessment: Do your security policies and controls reflect awareness of the haxposure threat?
- Operational awareness: Is the organization mindful of the potential to invite haxposure attacks in the way it conducts its operations?
- Organizational transparency: Is the organization being unnecessarily secretive in its operations? And are decisions to keep secrets made with a full awareness of the potential for leaks and associated blowback?

→
What are the implications of these factors? First and foremost they underline the need to get the security basics right.

Haxposure 2016?

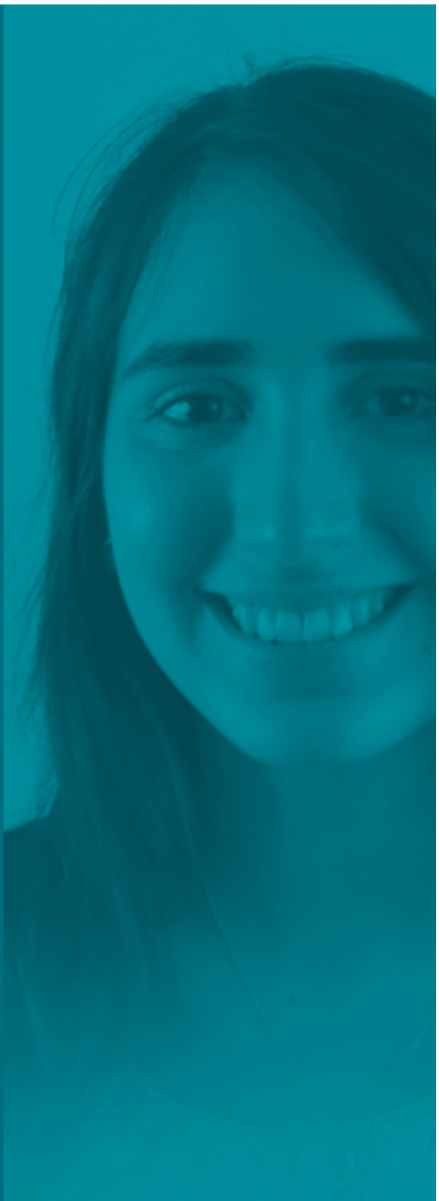
Will we see more cases of haxposure in 2016? The answer depends upon several factors, including the extent to which organizations educate themselves about this threat and take appropriate countermeasures. If a few high profile companies succeed in heading off such attacks and work with law enforcement to bring perpetrators to justice that may act as a deterrent. Unfortunately, it is also possible that haxposure will be encouraged by risky corporate secrecy. Consider the widespread cheating on *diesel emissions tests by Volkswagen* and the serious information system *security vulnerabilities in Chrysler-Jeep-Fiat vehicles*. Here you have some of the world's largest companies and best known brands putting at risk public health and safety with actions that were bound to backfire if they became known. Hackers who feel they have right on their side and a right to act as arbiters of justice may feel inclined to seek out further secrets and expose them, potentially damaging innocent victims in the process.

> IF A FEW HIGH PROFILE COMPANIES SUCCEED IN HEADING OFF SUCH ATTACKS AND WORK WITH LAW ENFORCEMENT TO BRING PERPETRATORS TO JUSTICE THAT MAY ACT AS A DETERRENT

7

Mobile devices:
threats and vulnerabilities

- An overview of mobile security
- 2015 milestones
- But what happened with mobile malware?
- What may we expect from this trend?



Author
Denise Giusto Bilic

7 MOBILE DEVICES: THREATS AND VULNERABILITIES

As smartphones and tablets increasingly offer services that process sensitive information, such data are becoming a more attractive target for cyber attackers. The primary risk scenarios are still the same: users who lose their devices or unwittingly install malicious applications. However, the consequences of an attack become more and more critical.

An overview of mobile security

To understand where society is headed in terms of using mobile technologies safely, a starting point is to evaluate to what extent mobile devices are currently protected, which will provide us with an overview of mobile security milestones so far.

A look back

2014 was an eventful year in the information security realm. The discovery of critical vulnerabilities on various high-impact operating platforms – such as *Heartbleed*, *Shellshock* or *Poodle* – illustrated the importance of keeping operating systems and applications updated.

Nor did mobile systems escape this trend: for instance, hackers found a way to deactivate iCloud, the cloud computing service that blocks iPhones when they are stolen or lost. Basically, this flaw made it possible to unlock the phone remotely.

On Android, a *vulnerability was exposed that allowed attackers to bypass the security mechanism of the browser.* This bug allowed hackers to access the sites that were open on the device and take control of it. Specifically, researchers found out how it could be used to compromise Facebook accounts.

As for malware, 2014 saw the onset of new varieties of ransomware targeting Android devices as forecast in ESET Research Lab's *Trends for 2014 Report*, which led to the reappearance of the Police Virus, this time for Android.

For example, ESET analyzed the *Android/Simplocker* ransomware, which scans the SD card of an Android device for certain file types, encrypts them, and demands a ransom in order to decrypt the files. Simplocker was the first malware of the Filecoder family aimed at Google's operating systems, and it sought to breach files with common extensions such as .JPEG, .JPG, .PNG, .GIF, .DOC, .AVI and .MP4.

Ransomware continued to spread and a new malicious program was detected, known as *Android/Locker*, which disguised itself as a fake antivirus application. Also, it asked to be assigned administrator rights to the user in order to take control of the system, which made it difficult to uninstall.

Toward the end of 2014, a new type of ransomware appeared that used the browser to show child pornography images and then lock the device, claiming to act on behalf of the FBI. Once installed, *"Porn Droid"* requested users to provide the system's administrator rights in order to lock the device screen.

In addition, Trojans developed for the Android platform reached new levels of sophistication, and propagated through underground markets and social networks. This was the case with *iBanking*, a malicious application capable of spying

→

As smartphones and tablets increasingly offer services that process sensitive information, such data are becoming a more attractive target for cyber attackers.

on users' communications, in an attempt to bypass mobile two-factor authentication methods used by some financial institutions.

Turning to iOS, a noteworthy case is that of *WireLurker*, a malicious program that attacked Mac systems and iPhones; this was one of the first malware to be able to infect even non-jailbroken devices. According to the BBC, approximately 400 apps were infected and downloaded more than 350,000 times.

- **Old trends come back with a vengeance**

Come 2015, it became clear that these trends, which gained momentum during 2014, had taken hold in the mobile ecosystem and become the new rule. In this sense, cybercriminals have stepped up their game in the diversification and sophistication of threats, so now we are witnessing more organized malware-spreading campaigns that include new infection vectors and attempts to hinder threat removal.

Throughout the year, a large number of vulnerabilities have been detected, and their exploitation has become an increasingly useful mechanism for attackers to gain control of devices.

This is putting further pressure on OS vendors to deliver platform updates faster, which is a problem on operating systems such as Android, as the large number of device providers with varying priorities can mean that critical updates take too long to be rolled out to end users' devices.

As a consequence of better-orchestrated attacks, malicious programs have started sneaking, by the hundreds, onto official distribution platforms that provide legitimate apps. This poses new challenges for the future, as it increases the need for manufacturers of mobile operating systems to develop better methods for detecting malicious activity.

Ransomware, one of the most profitable activities in the cybercrime world, dominates mobile platform infections with new device-locking techniques, showing a diversification of the techniques used to compromise the various devices.

Finally, attackers also leverage popular mobile platform apps such as WhatsApp or Facebook in order to extend the reach of cross-platform malware campaigns by using traditional social engineering techniques.

- **How do these incidents impact users?**

There are two decisive factors that lead cybercriminals to focus on a given platform: the size of its user population and the number of vulnerabilities available for exploitation. As computers and mobile devices are used more and more worldwide, the number of potential victims susceptible to a single malware campaign rises. There are no invulnerable operating systems; the number of threats aimed at a given platform is in direct proportion to the number of users it has.

With this in mind, a good way to identify the most exposed systems and to extrapolate the likely impact of mobile threat proliferation to each existing platform is to

→

Ransomware, one of the most profitable activities in the cybercrime world, dominates mobile platform infections with new device-locking techniques.

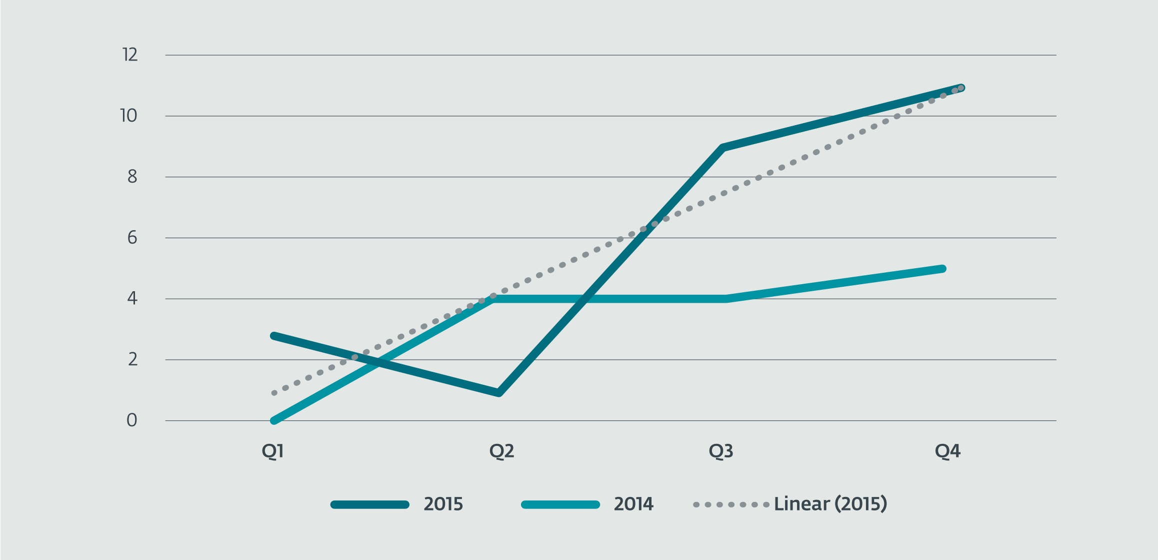
compare the market share each one holds. According to *Gartner*, Android held an 82.2% share of the market for the second quarter of 2015, compared to iOS's 14.6% and, lagging far behind, Windows Phone's 2.5% and BlackBerry's 0.3% share. Android – in spite of having slipped down compared with the same period a year earlier – continues to lead the market, while Apple's share has grown gradually. This means that with every new Android security vulnerability exploited, millions of users worldwide become unprotected.

Meanwhile, a new question arises: Are there more threats to iPhones and iPads nowadays? The answer is yes. With respect to iOS, if we compare the number of new threats detected by ESET products since the beginning of 2015 to the number of new threats detected during the same period in 2014, the figures have doubled. (Graph 7)

A large percentage of these families of malicious code seek to breach iOS systems through deception, using social engineering techniques that trick users into providing their information. Also, the large number of vulnerabilities recently detected in these systems leaves users unprotected if they fail to catch up with newly available updates to their operating systems and apps.

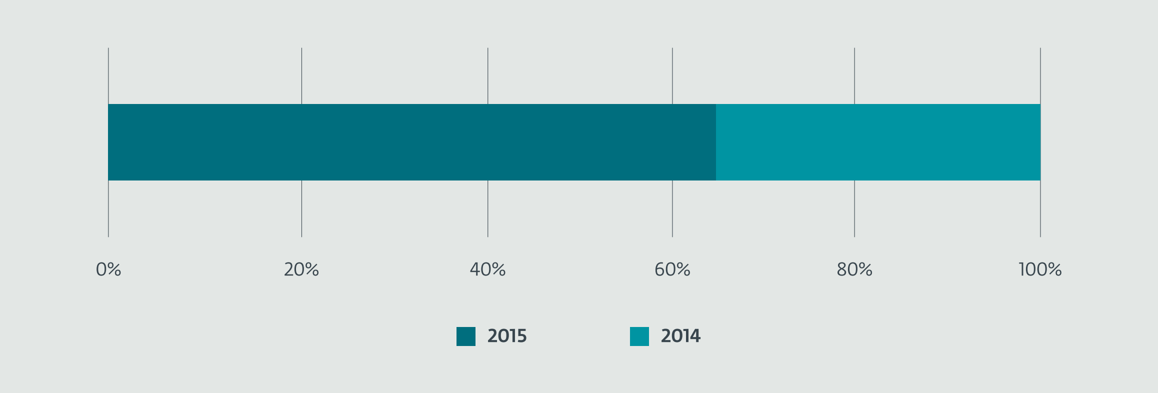
Similarly, jailbroken devices – or rooted devices, in the case of Android – can end up hosting malware such as Trojans, worms and backdoors, among others. This is because jailbreaking makes it easier for malicious code to execute commands requiring administrator-level privileges without the user having knowingly given authorization. Besides, jailbreaking breaks the update deployment mechanism normally afforded to

Graph 7 New malware variants for iOS



Note: figures for the fourth quarter of 2015 only include statistics up to November, so the estimated final percentage for this quarter will be even higher once the year ends.

Graph 8 New iOS malware variants



users of the platform, thus preventing the user from getting the latest system versions or security patches, and leaving the device vulnerable to attacks..

2015 milestones

- Vulnerabilities galore

The detection of vulnerabilities in applications used by millions always causes a great stir, especially if they affect privacy or render devices unresponsive. Earlier this year, a vulnerability in Android's email management app had a serious impact as it made the devices become unresponsive simply by sending a message specially designed for this purpose.

Other vulnerabilities in 2015 have affected Android systems, such as the one known as *CVE-2015-3860*, allegedly exploited by attackers to bypass the lock screen on Android and take control of the smartphone. Although the attack proved to be possible, the flaw was promptly fixed.

Meanwhile, *Samsung also discovered an important security flaw on their devices:* the SwiftKey keyboard installed on their smartphones failed to validate updates, which could allow a Man-In-The-Middle attacker to send malicious files to the device. About 600 million Samsung Galaxy smartphones could have been exposed.

To be sure, the standout flaw on the Android platform was the one known as *Stagefright*, which allowed hackers to steal information from devices by simply sending a text message designed for this purpose. With 950 million Android users potentially affected and the serious possible consequences of its exploit, certainly this vulnerability was by far the most serious to be discovered this year so far.

In turn, iOS devices were also exposed to risks due to various flaws. Halfway through the year, an *academic paper* revealed a series of flaws that, if combined, might exploit malicious apps to gain unauthorized access to the data stored on different applications (iCloud passwords, authentication token or web credentials stored on Google Chrome).

Another iOS vulnerability allowed attackers to use the *Airdrop* feature to install malicious apps covertly masquerading as genuine apps. Airdrop is a feature added in iOS 7 that enables users of supported devices to share files with any other device in the local vicinity. The vulnerability allowed attackers to send files even if they were rejected by the user.

In 2015 Apple also introduced changes to the data privacy mechanisms for their applications: they designed a new privacy update for iPhone to prevent iOS apps from viewing which apps have been downloaded to the device. In this way, advertisers will not have access to those apps' data.

But what happened with mobile malware?

2015 has seen a significant rise in the number of malware variants for mobile platforms. Moreover, what was most striking to users was the revelation that hundreds of malicious apps were being distributed through official stores.

This highlights the importance of raising awareness among users and teaching them how to discern which developers they should trust and what permissions should be granted to each application.

In the case of Android, *over 30 scareware applications available for download from the official Google Play store have been discovered*. These malicious applications, which pretended to be cheats for the popular Minecraft game, have been installed by more than 600,000 Android users.

Also, over 500,000 Android users were targeted by fake phishing apps on Google Play which, if installed, harvested their Facebook credentials. ESET has identified these Trojans as *Android/Spy.Feabme.A*.

ESET Labs have detected more than *50 Trojan porn clicker apps available for download*. Four of them had more than 10,000 installs and one of them had more than 50,000 installs.

In addition, among the samples found in the Google Play Store was *Android/Mapin*: this is a backdoor Trojan that takes control of the device and makes it part of a botnet. In some variants of this infiltration, at least three days must elapse before the malware achieves full Trojan functionality. It's probably this delay that enabled the code to get past *Google's malware prevention system* for such a long time. According to MIXRANK, one variants, masquerading as the well-known game Plants vs. Zombies 2, was downloaded over 10,000 times before it was pulled from the Google Play Store.

Ransomware continued to spread in Android systems. In this category, ESET discovered an *aggressive threat to Android capable of changing the device's PIN* and rendering it useless. This is the first code of its kind for this operating system and was dubbed Android/Lockerpin.

This Trojan obtains device administrator rights by pretending to be an 'Update patch installation.' Not long after, the user will be prompted to pay a 500 USD ransom for allegedly viewing and harboring forbidden pornographic material. Neither the owner nor the attacker can unlock the device, because the PIN is generated randomly and is not sent to the attacker. The only way to unlock the device is to reset it to factory defaults.

As for iOS, Apple has had to remove over 300 iOS apps infected with malware from the App Store, after a security

→
What was most striking to users was the revelation that hundreds of malicious apps were being distributed through official stores.

problem was confirmed. This attack, known as *XCodeGhost*, was carried out by ingenious, effective malware that has managed to pass off dozens of infected apps as if they were tested and found to be secure.

How did these apps make their way into the official store? Cybercriminals opted to infect the XCode compiler used to create applications on iOS. In this way, developers included malicious code in their apps without even knowing it and, because they use the legitimate developer's signature, they were uploaded to the App Store without any fuss.

For Apple, this incident marked a watershed moment: from now on, the company must do a better job of optimizing malicious code verification systems in applications before they are submitted to the online store.

Soon after this, researchers found another 256 apps that violate Apple's App Store privacy policy, which forbids the gathering of email addresses, installed apps, serial numbers, and other personal identification information that can be used to track users. These apps represent an invasion of the privacy of the one million people estimated to have downloaded them.

Also noteworthy is *YiSpecter*, a new malware program that abuses private APIs in the iOS system to deploy malicious functionalities. Its alarming aspect is that it attacks both jailbroken and non-jailbroken iPhone devices. This malware can download, install and launch arbitrary iOS apps, and even replace existing apps with those it downloads.

- Cross-platform scams

This year has also seen *large scale fraud campaigns spreading through mobile apps* and the compromising of a variety of popular store brands such as Zara, Starbucks and McDonald's, among others, with the object of stealing the victims' personal information.

Social engineering – in computer security, sometimes defined as the art of manipulating people for the malicious purposes of the manipulator – is one of the pillars of this type of fraud. This type of scam shows why education is the first layer of protection; in that sense, there is a need to warn users about these new trends that use old techniques through channels such as WhatsApp.

It is also notable that these malicious servers used geolocation techniques to achieve high propagation rates by turning a target user not only into a victim, but also at the same time into an accomplice in the spread of this type of scam. Thus, servers redirected traffic to the various rogue pages, according to the country and the type of device that received the message. This heralds the beginning of a new era of cross-platform threats, with campaigns designed to compromise users by targeting their various devices.

→

How did these apps make their way into the official store? Cybercriminals opted to infect the XCode compiler used to create applications on iOS.

What may we expect from this trend?

So far, some organizations and individuals have downplayed the importance of mobile device security, yet this is a mistake, and a new type of response is needed. It is essential to understand that mobile computing does not exist in a void – on the contrary, it actually impacts the various security components contained in the systems we use every day. In this sense, it is imperative to implement security strategies that include personal mobile devices as potential compromise vectors.

In addition, it is necessary to consider the relationship between the Internet of Things and mobile operating systems, as the latter will be the platforms supporting the data structure of upcoming interconnected gadgets. *Android Auto* is an interesting example of this upcoming trend. Today, ransomware hijacks desktops, laptops, tablets and smartphones, but soon it might hijack vehicle ignition systems, as discussed in other sections of this report.

As for these programs that hijack devices' information or operation, we expect an increase in the number of attacks, as cybercriminals discover the gems stored on mobile devices. As is the case with any highly lucrative business, its growth over time seems inevitable. As the cloud is used for storing user profiles available across various platforms, the use of these devices as an attack vector to deny access to data could have great impact, expanding the range of potential attacks against personal information.

New cross-platform malware campaigns might also crop up, either regarding distribution techniques (malicious servers that deliver specialized content for the requesting platform) or as regards execution techniques (the use of platforms and languages to generate executable software supporting multiple environments).

As the search for better protection mechanisms intensifies, mobile platform malware writers will develop new ways to make analysis of their code more difficult. It is inevitable that, over time, these malicious samples will be increasingly difficult to analyze.

Throughout 2015, ESET Research Labs have seen the threat creation rate remain relatively steady within the Android ecosystem, with an average of 200 new malware samples per month. Almost all of these are malicious programs of the Trojan type, as shown in the following diagram. Consequently, we are likely to see greater sophistication in the compromise techniques used by these programs in the following year.(Graph 9)

Of the new threats that have emerged this year, some have increased more than others, as shown in the diagram below. As can be observed, the volume of SMS Trojans has already increased considerably this year.(Graph 10)

Similarly, we discovered lots of new mobile spyware that seeks to steal banking and credit credentials, and capture private data on the device, such as messages and contacts.

There was also a significant rise in malicious mobile programs that try to prevent their victims from using their own devices and then, in general, go on to demand ransoms. In particular, the combined growth of the *Android/Locker and Android/LockScreen* families increased

→

It is imperative to implement security strategies that include personal mobile devices as potential compromise vectors.

by nearly 600% compared to last year in terms of the number of new variants. This figure does not include new samples such as *Android/Lockerpin*, mentioned before.

These trends could become more pronounced during 2016, which means we could face more diversity in types of ransomware and more sophisticated Remote Access Trojans that will try to gain control of devices so as to steal the users' sensitive information.

Although the volume of malware detected for iOS is still noticeably lower than that for Android, as shown in the diagram below, this new surge of malicious mobile code is bound to target iOS. An analysis of the rise in the number of malicious families for this platform during 2015 shows a significant growth towards the end of this year.(Graph 11)

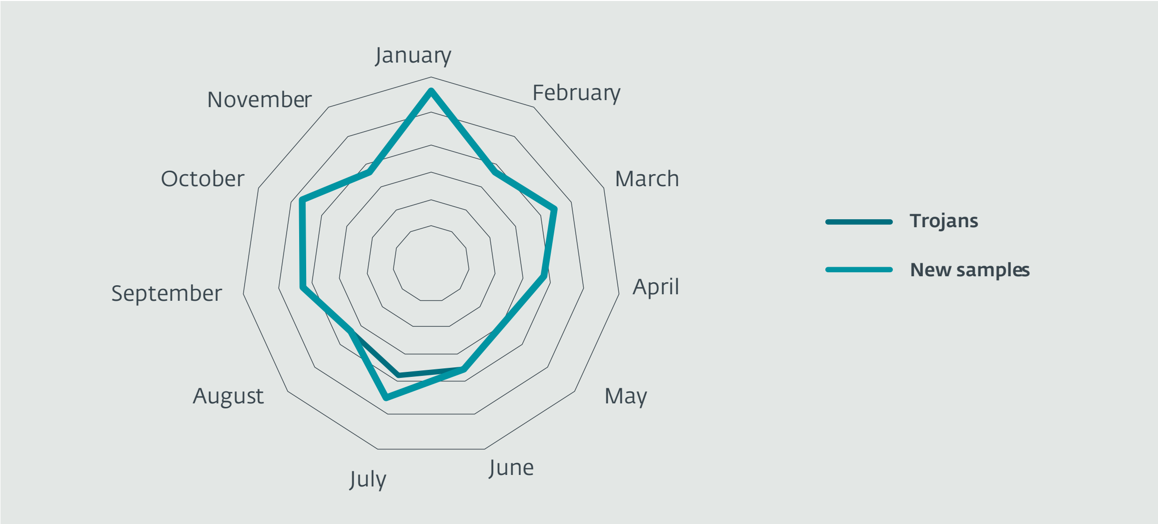
Within this new threat category, the variants within the families shown in the diagram below have had the greatest growth this year. Together with a larger amount of malware for iOS, new varieties of spyware are expected to emerge targeting smartphones, even when the manufacturer's protections remain intact, i.e. phones that have not been jailbroken. (Graph 12)

Finally, secure development focused on preventing vulnerabilities will be essential in order to create robust applications. Security cannot be an afterthought in the design process, but rather it should be central from the very beginning. Likewise, implementing procedures to perform static and dynamic system testing will be necessary for the early detection of potential vulnerabilities.

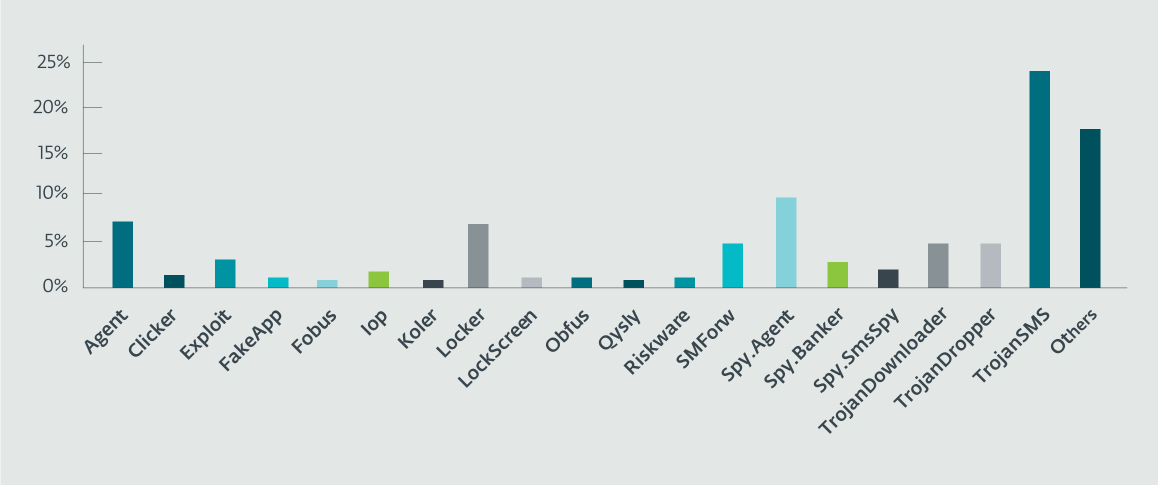
Defense strategies

Mobile malware is a real threat, so it is important to be on the lookout for infection attempts. It is time to reflect on what users can do in the face of this wide range of mobile threats.

Graph 9 Android Trojans in 2015



Graph 10 Android malware families with biggest growth during 2015



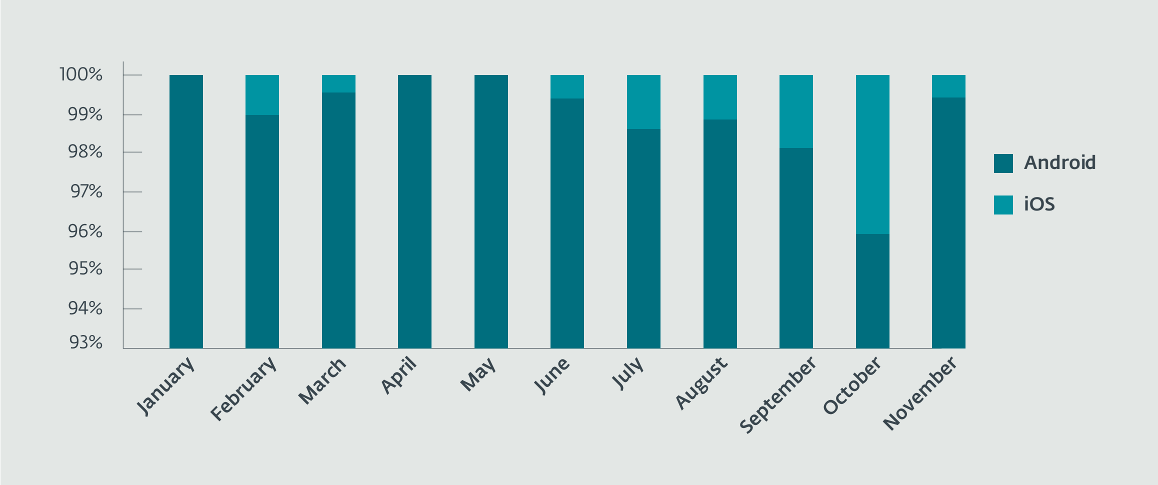
- **Home users**

In addition to installing a mobile security solution, users must be extremely careful when downloading applications from unofficial stores. In fact, the best practice would be to refrain from installing this kind of app, avoid installing apps from unknown sources and learn how to recognize legitimate applications. Here are some pointers.

When surfing the net, it is important to ignore sites that encourage users to download APK files from suspicious pages. Moreover, users should not trust text messages with dubious links, even if they appear to have been sent by one of the user's known and trusted contacts.

We have seen that malware spread through official platforms continues to increase, both on Android and iOS. In

Graph 11 New malware variants in 2015



the light of the high potential for new cases to emerge, make it a habit to be cautious on these sites too: users should find out who the developer is, what other apps they have created and whether they have been accused of fraud. Also, companies must strengthen the app review processes in their repositories further to minimize the number of cases of malicious apps finding their way into legitimate repositories.

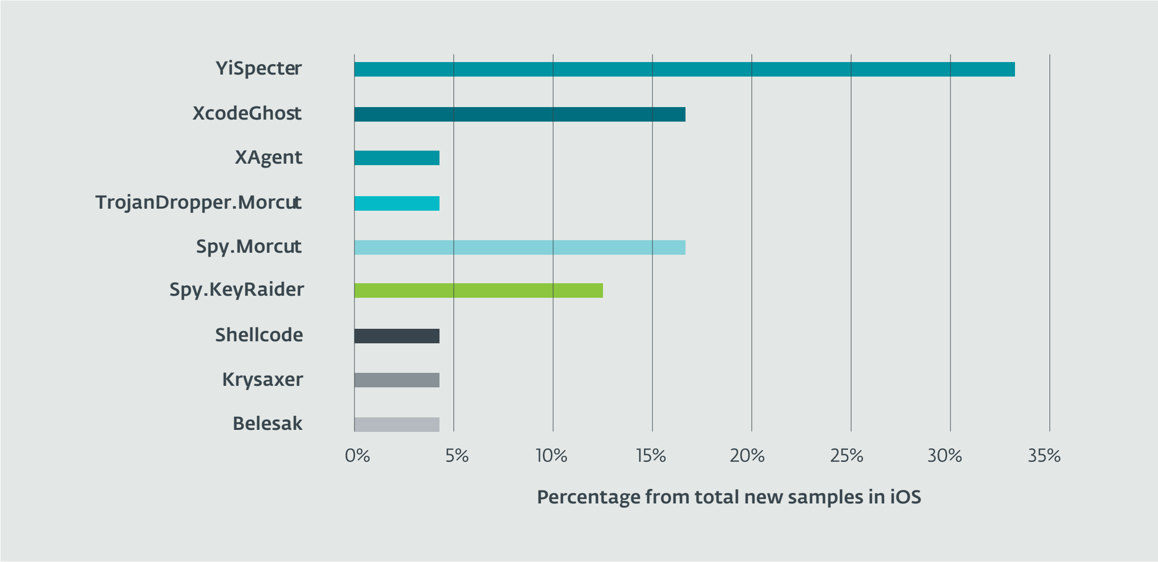
Rooting or jailbreaking a device breaks the security mechanisms that operating systems aim to provide, making them more susceptible to threats. This is why we recommend that you avoid this practice.

As has been stated throughout this section, there are numerous vulnerabilities that can be exploited to execute malicious code. Thus, it is important to keep operating systems and applications updated, and always install the latest security patches.

Particularly on Android, due to the wide variety of device models available, users have little control over the time manufacturers take to roll out updates to their devices. As there is no hard and fast solution to this problem, it is recommended that you consider roll-out times as a determining factor when it comes to choosing a device to purchase. Google devices – the Google Nexus range – will always lead the pack in this regard, as they reduce the vulnerability exposure time.

To protect the data confidentiality of a lost or stolen device, it is advisable to encrypt the device and install a security solution with remote management capabilities to lock and/or track the device. Because mobile ransomware is rampant, it is extremely important for users to back up their critical information to other trusted media – in that way they can avoid having to pay a ransom to recover it.

Graph 12 iOS malware families with biggest growth during 2015



Finally, analyzing the charges made to mobile bills is a useful measure to identify early any infection that might have bypassed the precautions mentioned above.

- What about corporate environments?

To be sure, malware trends that affect personal users will have to be addressed at the corporate level too. After all, everything from a massive SMS Trojan infection that incurs charges on the phone bills of corporate accounts, to information leaks caused by spyware, to data loss resulting from mobile ransomware, will all hit an organization hard where it hurts - in its profit margins.

It is vital to understand that corporate users' mobile devices can be used to implement attacks against the organization's networks. The first pillar of a good defense is acknowledgment of the risk posed by these devices in the era of cross-platform interconnection.

One mitigation might be to invest in devices exclusively for corporate use, featuring tools that support remote management. They should be duly encrypted and connected to the organization's intranet over a VPN. Also, separating mobile traffic on enterprise transactional networks and using security solutions on devices are essential measures in developing a preventative approach.

These measures must be accompanied by the strengthening of Data Loss Prevention (DLP) and Content Monitoring and Filtering (CMF) systems, and the creation of policies to guide mobile application management and secure platform configuration.

Measures commonly used in security policies for desktop computers are equally valid, such as defining secure passwords with mandatory requirements for length, duration and expiration date.

Such policies should also establish which platforms, versions and vendors are allowed and which are not. Handling applications only if they are duly signed must be obligatory, as must the disallowing of unapproved procedures intended to obtain administrator rights to the system.
Along with these technology-based solutions, security training programs must be created to warn end users against the growing variety of malicious code they will be exposed to over the coming year.

> MEASURES COMMONLY USED IN SECURITY POLICIES FOR DESKTOP COMPUTERS ARE EQUALLY VALID

→

Rooting or jailbreaking a device breaks the security mechanisms that operating systems aim to provide.

8

Windows 10:
Security features and user privacy

- Security features
- Privacy and user acceptance

Author
Aryeh Goretsky

8 WINDOWS 10: SECURITY FEATURES AND USER PRIVACY

Microsoft Windows 10 arrived in mid 2015, marking the first release of Windows under its new CEO Satya Nadella. With Windows 10, Microsoft is beginning to fulfill its vision of reinventing itself, transitioning from a software company to one focusing on devices and services, and has set an ambitious goal of having one billion devices running its new version of Windows in three years. For this to occur, though, Windows 10 has to be more secure and also be trusted by consumers and businesses alike.

Security features

With Windows 10, Microsoft has invested heavily in security. These enhancements include several improvements to Windows Defender, such as the detection of file-less malware in memory and adjusting the sensitivity of scanning files depending upon where they are located or downloaded from – a feat that can improve detection of new malware, but can also increase false positive alarms. In addition, improvements to manageability and offline scanning should make the software easier to use by system administrators.

With the increasing trend towards BYOD (Bring Your Own Device) and remote working, keeping compromised computers off corporate networks becomes more challenging, and Microsoft's solution for this is Conditional Access, which replaces Microsoft's older Network Access Control (NAC) technology with a more scalable and cloud-aware solution not just to prove the health of PCs connecting to the network, but to sense the integrity of the system as well, a facility that was unavailable with the older technology.

Also new for Windows 10 is Device Guard, a combination of operating system, management and hardware features that allow system administrators to lock down computers securely. While similar in concept to – and partly based on – AppLocker, Device Guard is enforced through Secure Boot and is not meant for use on general-use PCs. The use of Secure Boot also means that computers must have UEFI firmware and a TPM chip in order to use Device Guard. In its current iteration, Device Guard is intended for tightly-managed single-use systems, such as ATMs, kiosks, point-of-sale (POS) terminals, and other embedded systems where only a standard-use account is logged in, if a user account is used at all.

Security improvements have been made to the internals of the Windows 10 operating system as well. Virtualization Based Security (called Virtual Secure Mode in Windows 10 until recently) moves the core part of the operating system, its kernel, into a hypervisor, along with other

> WITH THE INCREASING TREND TOWARDS BYOD AND REMOTE WORKING, KEEPING COMPROMISED COMPUTERS OFF CORPORATE NETWORKS BECOMES MORE CHALLENGING

heavily-targeted Windows services, such as the Local Security Authority Subsystem Service (LSASS), which is the service that manages the operating system's security.

Microsoft Edge is Windows new web browser. Written from the ground up as a replacement for Internet Explorer, it is meant to provide a modern and secure web browsing experience. Its simplified code base means fewer vulnerabilities for attackers to exploit. And although it is a desktop application, Edge is implemented in a similar way to a universal app, which means that it runs in a sandbox-like container. These techniques, combined with the dropping of support for binary extensions like ActiveX and improvements to SmartScreen, make Edge a more secure web browser than its predecessor, Internet Explorer. Internet Explorer is still present in Windows 10 for sites that require it, but Microsoft strongly recommends using Edge.

Privacy and user acceptance

It does not matter if Microsoft has made Windows more secure, if users don't trust it. Windows 10 marks a change in the type and volume of information that Microsoft collects about its customers, which has left many people with concerns over upgrading to the latest flagship desktop operating system. Microsoft's data and telemetry collection is not actually new, though: the company initially began collecting crash reports and telemetry during the Windows XP era, and this is just a continuation of those efforts. While the scope of collection may be new to Microsoft, this level of collection has been the norm now for some time in operating systems from companies such as Apple and Google, and Microsoft is merely playing catch-up in this regard. It is, however, a first for the Windows desktop and some users and privacy advocates are understandably concerned about Microsoft's intentions.

Another area of concern is Microsoft's new update procedures for Windows 10. Updates to Windows 10 Home, the version of Windows 10 supplied on most consumers' computers, will not only be installed automatically, but will be mandatory. Windows 10 Pro has an option to defer these upgrades, but that is only temporary, and doesn't include security-related updates. Businesses will have some additional level of control over whether and when to accept updates, but will still have to apply them to most computers running Windows 10 except for certain licenses and use cases of Windows 10 Enterprise.

This marks a major shift where system administrators and home users have had granular controls over which updates to apply and which to defer, and, coupled with Microsoft's decision no longer to share details about what it is that the updates actually fix has left some folks anxious about what bugs are getting fixed and how those fixes might affect their computers.

There is no question that Windows 10 has made great strides in security, but concerns about privacy and transparency are also mounting, and Microsoft will need to address these if it is going to reach its goal of a billion devices running Windows 10 in three years.

→

It does not matter if Microsoft has made Windows more secure, if users don't trust it.

For further information about Windows 10, see the following two blog posts on We Live Security:
Will Windows 10 leave enterprises vulnerable to zero-days?

Windows 10, Privacy 0? ESET deep dives into the privacy of Microsoft's new OS

Also, look out for *ESET's white paper* on Windows 10 security and privacy.

> THERE IS NO QUESTION THAT WINDOWS 10 HAS MADE GREAT STRIDES IN SECURITY, BUT CONCERNS ABOUT PRIVACY AND TRANSPARENCY ARE ALSO MOUNTING

9

Critical infrastructure:
it's time to make security a priority

- Critical systems at risk
- Information asset management as a key factor
- Common threats targeting industries indiscriminately
- Healthcare – among the most affected sectors
- Highly vulnerable medical devices
- Record theft: more than just exposed data
- Focusing on security to prevent intrusion

Author
Camilo Gutiérrez
Amaya

9 CRITICAL INFRASTRUCTURE: IT'S TIME TO MAKE SECURITY A PRIORITY

The security of industrial systems has been a matter of analysis and debate for years, especially after the onset of threats against them such as the Stuxnet worm in 2010, and the recognition of the vulnerability of these systems to external attacks.

Five years after Stuxnet and in the wake of other threats that followed, such as Flame or Duqu, IT security teams face numerous challenges in the quest to safeguard critical data against threats which no longer differentiate among different types of industries.

Thus, one question becomes clear: are all these businesses and industries prepared to face future challenges?

Critical systems at risk

The importance of ensuring information security on critical infrastructure has been recognized for years, yet there are still cases that illustrate the need for improvement.

To a large extent, one of the major sources of security deficiencies is the fact that a large number of the manufacturers of these platforms do not allow the introduction of changes or updates to the hardware-controlling systems.

In summary, organizations are managing critical infrastructure using operating systems that are obsolete, vulnerable and yet connected to the Internet, increasing the likelihood of a security incident. Thus, there is a need for manufacturers and industries to join forces to update their infrastructure and mitigate security breaches that leave the door open to potential attacks.

Information asset management as a key factor

In addition to the fact that many industries still have obsolete operating systems in place, what is also striking is that, because of the functions they have been designed to perform, control devices tend to have a public-facing connection to the Internet in order to carry out maintenance and management tasks. This presents a major security risk, as access is available at all times, so unless proper management actions are taken, unauthorized individuals might be able to access the systems. Thus, a good management policy should consider granting access only for technical support purposes, or implementing a secure connection such as a VPN to send and receive data.

In addition, it is necessary to consider the functionality of control and protection mechanisms such as firewalls. Many organizations base the configuration of these devices on predetermined and generic rulesets that control in what circumstances two computers can establish a communication over a certain network. However, there is no analysis of the traffic that may be unique to that connection, as each control system has specific protocols in place, and these are unknown to firewalls designed for more generic environments. This means we are dealing with easy-to-interpret communication protocols, so analysis tasks should be performed there when setting up existing firewalls, so as to enhance the control

→
Organizations are managing critical infrastructure using operating systems that are obsolete, vulnerable and yet connected to the Internet, increasing the likelihood of a security incident.

capacity and the identification of proprietary protocols used in industrial systems. Although there are now industrial firewall developers that are starting to implement devices with these capacities, the evolution of such hardware in the industrial sector is very slow and there is still much to be done.

In addition to all of this, a big problem closely connected to business management is that management and security tend to be handled as two separate matters. This has a very negative impact on communication, and can lead to considerable security problems within an organization: if the business management people consider security to be an 'obstacle' rather than an integrated, essential growth driver for the company, this increases the likelihood of security incidents occurring, ultimately creating problems for organizations. The availability of certain critical industrial services, in both public and corporate sector infrastructure, usually ranks above the proper configuration of security systems, potentially enabling remote attacks on industrial systems exposed to the Internet. Even when the concept of availability is very important in this particular case, the confidentiality and integrity of data must be considered as well.

Finally, in some cases, with the aim of achieving business goals, a prevailing approach – and one that is very questionable in terms of security – is the saying 'if something works, don't touch it,' which means that on occasion, for fear of tinkering with something that allegedly works just fine, the security teams fail to do the appropriate maintenance work. This poses several security problems, since outdated, unpatched operating systems could lead to their failure or even to unauthorized access by an attacker. Basically, the fact that something works right now doesn't mean that you shouldn't protect it against future risks. It's a good thing to fix the roof before it starts to rain.

Common threats targeting industries indiscriminately

When it comes to cybercriminals targeting industries such as energy, oil, mining and various industrial systems, attacks are not restricted to sophisticated, complex threats such as Stuxnet, Duqu or Flame. During 2015, several ***cases were reported*** of energy companies being attacked by malware dubbed ***Laziok***, used to collect data on compromised systems, including machine name, CPU details, RAM size, hard disk size and what antivirus software was installed.

With this information, cybercriminals can determine if the computers are viable targets for future attacks. What is curious about these cases is that it was an attack based on emails containing an attachment that exploited a Microsoft Windows vulnerability. Even more problematic was that although a patch for this vulnerability was created in April 2012, many industries had not applied it yet.

Healthcare – among the most affected sectors

In addition to the industrial sector, the healthcare industry has been an important component of the security debate over the past year. During 2015 and as part of ***Verizon's Data Breach Investigations Report***, analysts identified approximately

→

The saying 'if something works, don't touch it,' sometimes means that the security teams fail to do the appropriate maintenance work.

80,000 security incidents, of which 234 were healthcare-related, and 2,100 data-loss breaches, with 141 occurring in the healthcare industry.

A large number of security issues have become more evident, including primarily insider abuse or bad practices, which caused 15 percent of security incidents in the healthcare industry in 2014, compared to 20% in 2015, according to Verizon's report.

Also, healthcare organizations have become more vulnerable to web application attacks and distributed denial-of-service (DDoS) attacks, as this industry suffers four percent more of this type of attack than all other industries combined.

Add to this the findings of the *Ponemon Institute* report, which revealed that the root cause of security breaches in healthcare organizations has shifted from accidental to intentional. Criminal attacks are up 125 percent compared to five years ago, and lost laptops are no longer the most common data breach threat.

In addition, a 2015 study called *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data* found that most organizations are unprepared to respond to new cyber threats and lack the proper resources to protect patient data. 45 percent of healthcare organizations said the root cause of data breaches were cyberattacks, compared to 40 percent in 2013.

Highly vulnerable medical devices

In addition to the security management issues mentioned above, new medical equipment also brings with it significant risks. Improved capabilities in these devices include the fact that they feature an Internet connection, but this can be a mixed blessing. For instance, in the case of implantable medical devices (IMDs), which are intended to treat a variety of conditions, security concerns are often underestimated and even overlooked.

The threat posed by this medical gear is very real, and numerous types of device have been infected by malware, in most cases inadvertently. In fact, *during 2014 over 300 different surgical devices reportedly suffered a vulnerability* that might allow attackers to alter their configurations.

As is the case with industrial security, connectivity is a critical aspect. In this sense, it can be argued that the security level of wireless connections is often very low, and that the medical equipment industry continues to put off the inclusion of security mechanisms on their devices.
For these reasons, medical devices are considered an easy target, as they feature outdated applications with insufficient security. The large majority of networked biomedical devices do not enable modifications and do not support third-party-vendor authentication agents, making them vulnerable to access via web browsers.

→
The healthcare sector should be more aggressive in its defense planning, and should adopt a faster pace in assessing risks.

In 2015, security researchers found vulnerabilities in critical medical systems which put them at risk of being exploited by attackers. In *the report detailing their research*, they say they were able to access Internet-connected devices, and that they accessed the network of a United States health provider and found *up to 68,000 medical systems and equipment with vulnerabilities* that were exposed to attacks.

This is why the healthcare sector should be more aggressive in its defense planning, and should adopt a faster pace in assessing risks, to guarantee that funds are well invested and that resources and assets are well protected. Ideally, risk assessments should be carried out continuously rather than periodically. This helps to guarantee that new assets, as well as physical and digital strategies and defenses, are promptly included in business plans and incident response plans.

Record theft: more than just exposed data

Successful attacks exploiting the flaws discussed so far allow cybercriminals to gather a wealth of information, especially from the healthcare industry, such as patients' names, health insurance numbers, telephone numbers, home addresses, email addresses and other personal data. However, even more critical data can be breached, such as medical records containing diagnoses and medication details. This information is very valuable to attackers, and if stolen, it can be sold for profit, along with the personal data mentioned above, on a much more specialized black market.

Regardless of where the information is obtained – whether it is openly-available data that was published online or very specific information stolen from medical records – if criminals manage to harvests a large amount of information, they can sell it and even steal victims' identities to commit various crimes such as creating false IDs, opening bank accounts and applying for credit cards, committing tax fraud, and even using the data to reply to security questions in order to access online accounts, thus taking the threat to new digital horizons.

Clearly, the benefits of the Internet and wireless networks are very appealing to the healthcare industry. Above all, they provide the user with immediate access to a treasure trove of information about patients' medical records from any location with an Internet connection. However, these are very sensitive data, and it is essential not only to have smart protection systems on the devices that hold or access them, but also to add further barriers such as encryption and *multi-factor authentication*, as well as sound network segmentation and reliable incident recovery strategies.

Focusing on security to prevent intrusion

Analysis of these cases makes it clear that there is still much to do to raise awareness and provide education on information security in private and public sector organizations. Attackers are always looking for ways to access a system through any kind of gate that is left open, and once they have managed to trespass the limits, they can not only steal information, or

→

Medical devices are considered an easy target, as they feature outdated applications with insufficient security.

compromise equipment so as to upload data to a malicious network and misuse it at will, but they can also alter the functioning of industrial equipment for improper purposes.

In an effort that illustrates the focus on the protection of critical infrastructure, the National Science Foundation in the United States awarded Texas Christian University (TCU) *approximately USD 250,000 in funding to help it come up with effective measures* that will protect medical devices from cyberattacks. Similarly, the *European Union Agency for Network and Information Security (ENISA)* has revealed that it will be looking to focus on developing good practices when it comes to 'emerging smart critical infrastructure' in 2016.

The industries that use these systems with major security flaws are ones that provide essential services to the population. Their infrastructures include water treatment, electric power generation and distribution, natural gas distribution plants, and even medical record database facilities. Their systems handle truly sensitive information, which explains the criticality of the associated risks and the great impact in case of vulnerability or failure.

Although some changes that improve security have been introduced in many of these industries, there is still a long way to go in the various sectors. The number of attacks against this kind of infrastructure will rise by 2016 unless protection actions continue to be taken at a fast pace, and that is why all activities related to information security in these sectors will continue to gain prominence as a key management factor.

→

The systems handle truly sensitive information, which explains the criticality of the associated risks and the great impact in case of vulnerability or failure.

10

Laws and regulations:

- Meeting standards and better security practices
- Laws protecting personal information around the world
- Information Security: an effort shared between governments, companies and users

Author
Miguel Ángel
Mendoza

10 LAWS AND REGULATIONS

Compliance is considered essential for the achievement of goals in the management of security information. It can be defined as conformity with previously established requirements that are applicable to the companies, according to their functions and characteristics, which is why it is vital to satisfy these requirements. Among the set of conditions that organizations are looking to cover, we can list specifications imposed in the areas of politics, standards, laws or regulations.

In information security it is mandatory to comply with some requirements: for example, legislation focused on protecting the personal information of users or companies' clients. In the same way, organizations commit to the protection of their own information and also, with third parties, comply with security regulations that have been adopted voluntarily.

So, it does not matter if it is a public or a private organization, a big or a small one, for-profit or not: the sensitive information that they process, archive or transmit requires protection measures that can be established by their own initiative or by any interested party: suppliers, partners, clients or the government.

Lack of data protection has played a large part in the big information leakage stories of the past year, such as those concerning Sony, Ashley Madison or Target. The personal information of users and the compromising of the companies' systems are very important issues and will continue to be in the future.

The requirements codifying the rules must be fulfilled in order to satisfy basic security necessities, which are established according to the value of the information. Among these requirements, the most relevant issues in recent years are related to the laws that protect information and adopt and mandate security standards.

Meeting standards and better security practices

Organizations can adopt regulations either as a personal initiative in the interests of data protection or in order to fulfil a contractual or regulatory requirement. In the same way, there are reference frameworks or standards that support and certify the security measures adopted and adapted in companies.

One reference in security issues still is ISO/IEC 27001, a standard used internationally to provide a model for establishing and maintaining an Information Security Management System (ISMS). It represents the experience of experts in security standards. Since it is an open document, everyone can read the documentation; its implementation must be done according to the characteristics, necessities and conditions of each organization, no matter what their activities are.

The structure of the standard is reduced to two basic issues: the requirement clauses for an organization to work in alignment with an ISMS, a system for managing information security, and a set of objectives to control the security, which considers different approaches for protection. Based on that, companies can manage the risks associated with the information. In accordance with this principle, organizations have aligned themselves with the guidelines and good practices defined in

→
Organizations can adopt regulations either as a personal initiative in the interests of data protection or in order to fulfil a contractual or regulatory requirement.

ISO/IEC 27001. Since the publication of the 2005 version, and with its update in 2013, the number of certificates granted has grown every year. (Graph 13)

According to a study by the International Organization of Standardization (ISO), *in 2014 there were 23,972 ISO/IEC 27001certificates granted around the world*, representing an increase of seven percent compared to the previous year. Compared with the preceding years, ISO/IEC 27001 experienced a slight slowdown in growth.

Japan *heads the list* of countries in the information security sector with 7,181 certificates, although the UK also occupies an important place and had the most significant growth in absolute terms, with 2,261 certificates obtained in 2014; in the third place was India, with 2,170.

On the basis of these results, it is obvious that there is a trend towards increasing certification around the world in recent years, but it is also true that there is a need for more effort, considering that, for example, there are serious gaps between the countries.

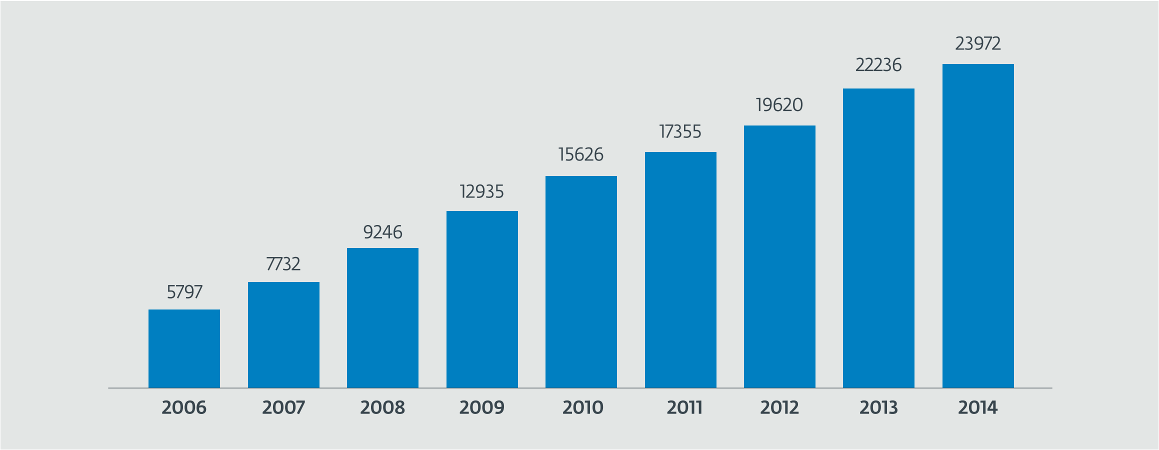
The following map shows the quantity of certificates obtained by each country. (Graph 14)

Although a certificate by itself doesn't guarantee that an organization is immune to threats, certification is proof that actions related to the protection of information are being undertaken. It shows that the management of risks and security is being considered at a high level within the organization, fulfilling three very important aspects: corporate governance, risk management, and compliance (GRC).

Laws protecting personal information around the world

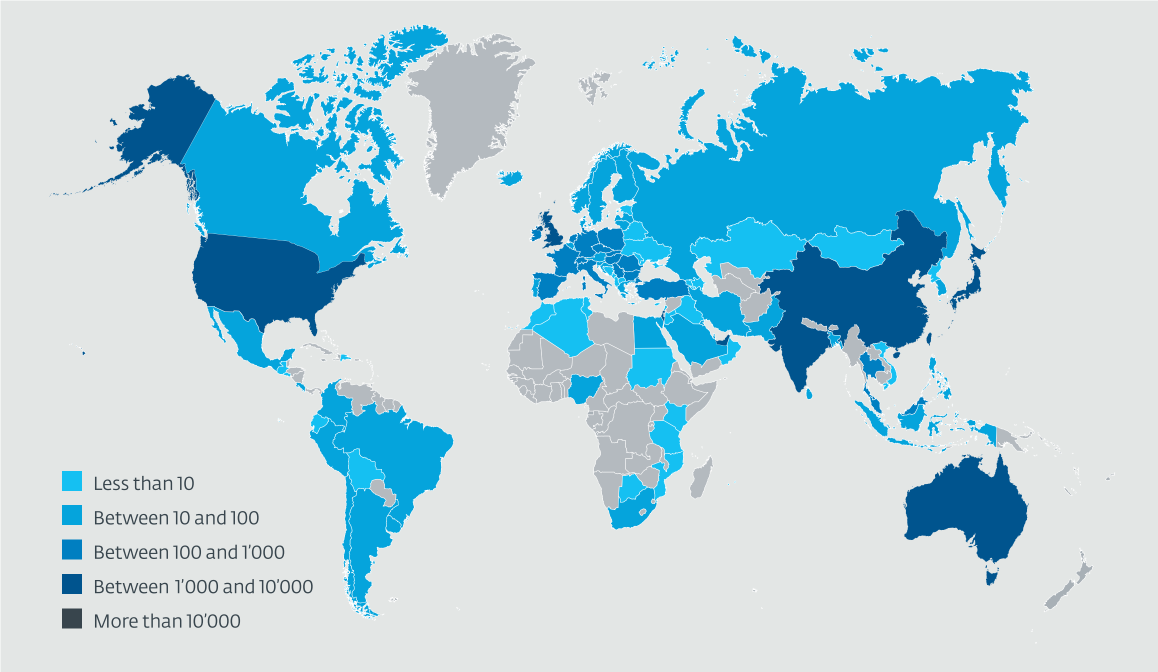
Another compliance issue is related to the laws pertaining to protection of personal information. Privacy has acquired more relevance and visibility over the years, since the appearance of the right to pri-

Graph 13 ISO/IEC 27001 certificates around the world



Source: ISO

Graph 14 ISO/IEC 27001 certificates around the world



source: http://www.iso.org/iso/home/standards/certification/iso-survey.htm

vacy as part of the [Declaration of Human Rights](), which affirms says in [Article 12:]()'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

With the growth of new information technologies, more and more information is in digital format, which represents more challenges that demand a balance between the right to privacy of the individuals and the manipulation of the information by third parties, as a result of the use of technology.

This refers to any type of information that is concerned and associated with a person and that allows the identification, characterization and determination of the individual's activities, private or public. Each individual owns his or her personal information and decides to share it or not, as well as the way in which it should be treated by the entities that have access to it.

Among personal information we include data that identifies the person (Personally Identifiable Information) or allows communication with the principal: information related to employment, physical characteristics such as appearance, anatomy or traits of the person. It is also considered to include information related to training and professional activities, their property and their biometric information.

In addition, other information could be important, such as the information that involves the individual's personal value system. Its misuse could lead to a negative impact, such as discrimination. This type of information includes aspects like ethnic origin, health, religious beliefs, sexual preferences, affiliations and political opinions.

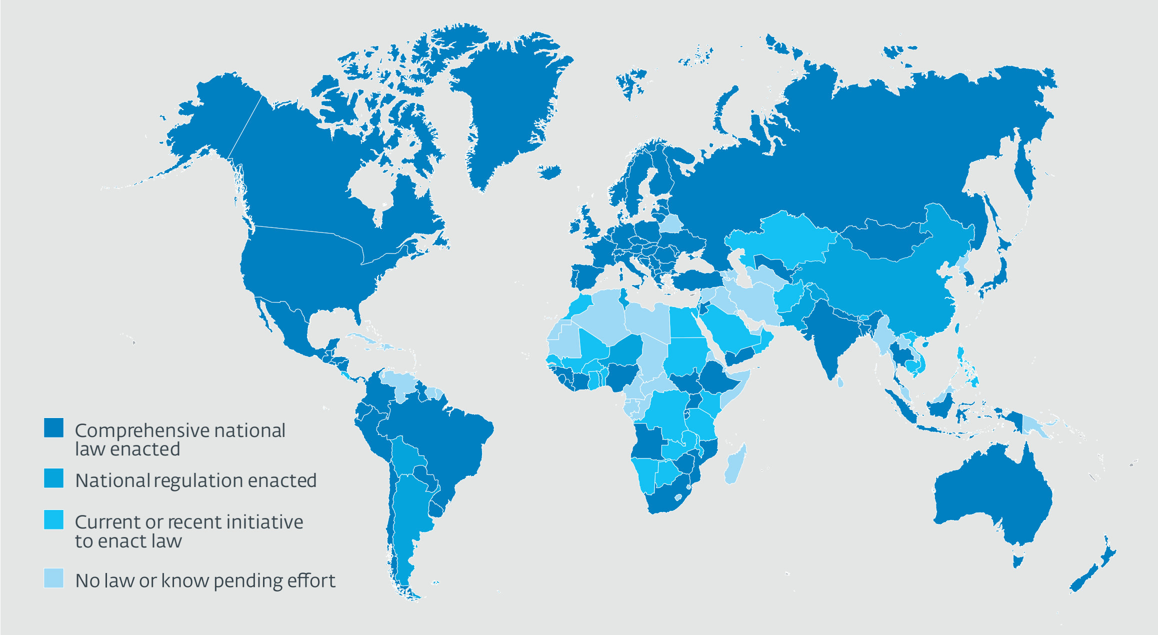
This is the reason why international organizations urge countries to legislate on these aspects. According to a [study conducted at the end of 2014](), more than 100 countries had adopted laws governing privacy and the protection of information in the possession of governments and private companies. The map below shows the countries that have this kind of law and the ones that have pending initiatives for the adoption of such legislation.. (Graph 15)

Different protection initiatives have tended to incorporate the protection of personal information rights afforded by the laws and rules developed in different parts of the world, as such protection is considered – in theory, at any rate – a universal right that offers people the power to control their personal information.

Another driving force behind laws relating to the protection of information is business. Privacy has become a necessary condition for trade between countries. Non-compliance with the rules could mean the loss of business opportunities. International trade agreements that consider the protection of personal information urge countries that sign up to them to legislate in this area.

One example is the principles of safe harbor privacy, established in 2000, which affirmed a framework for the recompilation, use and retention of personal information transferred from European Union member states to the USA as being in compliance with the European Union's ***Data Protection Directive.*** This directive forms much of the basis for data protection legislation in the EU, and this af-

Graph 15 ISO/IEC 27001 certificates around the world


Comprehensive national law enacted
National regulation enacted
Current or recent initiative to enact law
No law or know pending effort

Source: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 firmation was the basis for exchange of data between the US and the EU.

However, last October 6th, the agreements of safe harbor were declared no longer valid by a European court, since the European Court of Justice considered that it has flaws because it had allowed the authorities of the US government to have access to the information of European citizens exceeding the scope of the Data Protection Directive and other regulations still under discussion at time of writing.

The court's declaration includes the statement that "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."

Information Security: an effort shared between governments, companies and users

Compliance with rules and regulations is necessary if organizations are to achieve their objectives, and remain aligned with requirements made voluntarily or by an interested party.

> COMPLIANCE WITH RULES AND REGULATIONS IS NECESSARY IF ORGANIZATIONS ARE TO ACHIEVE THEIR OBJECTIVES

It is possible to forecast that the adoption of information protection measures as a way of self-regulation will remain in force, especially if we consider that the constant development of threats and the continuous identification of vulnerabilities determine the dynamic nature of the risks associated with information storage and processing. These last factors, which could be considered "external" to the interests of organizations, are the ones that could weigh in favor of the decision to adopt and comply with the rules, given the importance that personal information has nowadays.

In addition, privacy will continue to be crucial to conducting business in the coming years if we consider that the exfiltration of information we have seen in recent years. The information of citizens and of the world in general, continues to reverberate in the sphere of international relationships. Here we find another factor that could continue to push public and private organizations toward the adoption and fulfillment of privacy protection rules and legislation: the pressure that could be exerted by individuals towards the protection of their personal information.

The importance now afforded to laws or standards shows us the relevance that information security continues to acquire, if it is associated with the protection of information and its privacy. To achieve those objectives requires the participation of governments that are interested in legislating security-driven issues and promoting the creation of institutions entrusted with the making and fulfilment of laws enforcing those objectives.

> →
> **It is possible to forecast that the adoption of information protection measures as a way of self-regulation will remain in force, especially if we consider the constant development of threats.**

On the other hand, it is also necessary that companies process user information within the framework of regulations, standards, legislation and rules; that users participate by acting in accordance with the application of good security practices; and, finally, that companies and organizations regard as one of their principal aims the preservation of the confidentiality, integrity and availability of such information.

> THE IMPORTANCE NOW AFFORDED TO LAWS OR STANDARDS SHOWS US THE RELEVANCE THAT INFORMATION SECURITY CONTINUES TO ACQUIRE, IF IT IS ASSOCIATED WITH THE PROTECTION

11

Threats to kids on the web

- Privacy and sexting
- Grooming
- Cyberbullyng
- Law and social contract as prevention

Author
Sebastián Bortnik

11 THREATS TO KIDS ON THE WEB

The relationship between minors and computers has in recent years become a full-time and, in some cases, dependent one. Whereas just a few years ago "being online" represented specific segments of time scattered throughout a life lived mostly offline, children today almost "live online". In the digital world, its young inhabitants use computing devices from a very early age; smartphones, tablets and computers are used daily, allowing young people to not only stay connected, but to "live" on the Internet. Their social life is split between what is done in the physical world and their intense life in the digital world. *95% of adolescents use the Internet through social networks*, where they share dialogue and information, generally interact with their friends and also, perhaps, with their not-quite-friends.

In addition to social networks, tools such as WhatsApp, online games and other portals enhance the use of the Internet for communication, and the type of data consumed and shared. In the same way, the number of portals and communities for minors has grown and many of these have paid features and services, so there is a financial risk associated with the use of credit cards in connection with children and teenagers.

How prepared are adults to handle this situation? The digital gap between parents and children has increased in recent years. *Surveys show* that 50% of parents do not know what their children do on the Internet, and one in every ten children says that their parents do not know about the technologies they use.

In this context, cyber attacks against minors on the Internet are confirmed as a significantly growing trend, and attacks on the Internet privacy of minors emerge as a risk based on three pillars: personal data, financial data, and sexuality..

Privacy and sexting

Privacy on the Internet can be defined as the power exercised by users to control access to their information by limiting the extent of that access according to what they authorize, and to whom. This includes personal information, photos, files, and so on. When it comes to minors, effective control requires skills that children do not yet possess, such as social awareness of the risks associated with sharing certain information; that awareness develops (in the best cases) during adolescence or adulthood.

Both social networks and games with social features (chats, interaction, friendships and so on) that are targeted towards child audiences are environments in which the malevolent can deceive minors, and thus access their data or information through social engineering manipulation.

On the other hand, children often share their own information with others without being aware of the wide range of people it might reach. A clear example of the latter is sexting, a term that means voluntarily sending sexually explicit content through digital channels. It is a common practice among young people and is observed among large groups of adoles-

→

How prepared are adults to handle this situation? The digital gap between parents and children has increased in recent years.

cents. The surveys quoted above suggest that at least 25% of children interviewed have at some time sent or published nude or semi-nude photos electronically. Moreover, more than half of young people claim to have seen private images that were not intended for them.

Often these materials, which originally were explicit content shared between two people, are passed on to a less limited group of people, without thought being given to the potential for them going viral. The mainstream platforms involved in this behavior are applications for smartphones such as WhatsApp, Kik, Snapchat or Twitter.

Grooming

Grooming is one of the crimes whose impact on children has grown on the web in recent years. It is the deliberate manipulation of a minor by an adult via the Internet aimed at culminating in actions of a sexual nature, such as sending explicit photographs or performing sexual actions in front of a web camera. In other cases, this action is a precursor to initiating a physical encounter with the minor.
The adult usually pretends to be of a similar age when they make online contact with the minor, in order to earn the friendship of the victim, thus creating an emotional connection. That is, they create enough empathy in order to reduce the child's inhibitions.

In many cases, once certain material has been obtained, the criminal may attempt to blackmail the minor by threatening to share the explicit content among their friends and relatives if they do not continue complying with the requirements of the "groomer".

This type of problem, although not new in offline crime, has begun to emerge also in the digital world, where it's easy for the attackers to exploit their own anonymity, steal the identity of the victim, and work on many potential victims at the same time. In the majority of cases, communication starts on social networks and then extends in some cases to the physical world; thus leading in extreme cases to situations linked to pedophilia or child rape.

The groomers can be men or women of any age and any economic or social stratum. The process often starts online and on many occasions, the attacker invests considerable time during this cycle: building trust with the minors; repeatedly changing identities, giving gifts, or simply spending time with them in a virtual community or online gaming environment.

Cyberbullyng

The same lack of control that minors exhibit on the Internet may extend to difficulties in identifying a reasonable criterion when publishing content, not only around privacy, but also around aggressive or violent content.

Harassment is referred to as *cyberbullying* through computer-borne traffic such as social networks, chat, email, or web sites. It consists of annoying, threatening, humiliating or harassing a person using such means. The most common forms are the spread of false rumors, humiliating videos or photos, and the creation of profiles or sites promoting physical or psychological assault against the victim. It may also happen that the aggressors impersonate other people in order to say nasty things or to threaten the victims with publication of their personal information. Generally, those affected are vulnerable people who are seen as "different" by those who victimize them. *Cyberbullying* expands virally on the web and is difficult to stop. For this reason, it is particularly invasive and harmful.

Many years ago, harassment was only conducted in person at school or in clubs, but since the emergence of *cyberbullying*, this harassment is more constant and traumatic for children because it can be kept going and spread even further over the Internet and social networks throughout the day.

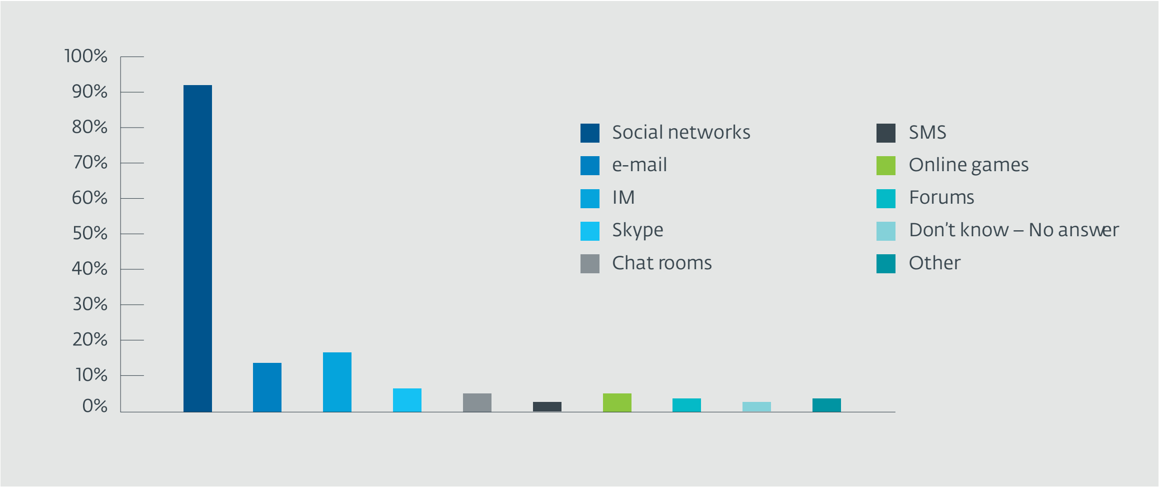
Although it is not a practice unique to minors, *cyberbullying* is more difficult to control in this segment of the population. Additionally, attacks may remain in cyberspace for a long time, so they affect those who suffer them over the long term.

According to the results of a survey conducted by ESET Latin America, social networks are the most likely place to find this kind of incident, with instant messaging in second place, especially via mobile devices. (Graph 16)

According to this survey, 42% of the people surveyed know someone who has encountered this type of threat over the Internet, and 80% of those affected were in the age range of 11 to 18 years, which is already curious since Facebook, for example, only allows people older than 14 years old to create accounts. (Graph 17)

Without being specifically a computer threat, *cyberbullying* is already becoming one of the main risks to minors on the Internet and this trend will deepen in the next few years.

Graph 16 Places where cyberbullying actions were seen



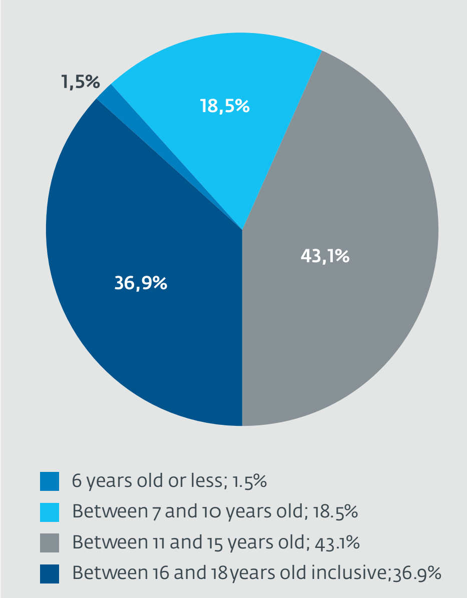
Source: ESET Latinoamérica

Law and social contract as prevention

The big challenge that adults now face is how to become aware of these types of incident when they occur among children; it is therefore advisable for specialists to pay attention to changes in **children's behavior or mood.** If a child exhibits sudden sadness, a decline in school performance or desire for solitude, it is necessary to talk in confidence to understand what it is happening, since he/she could be a victim of any of the situations described above. In this context, addressing the child's digital social life in these dialogues is essential for a correct understanding of any such issues that might be emerging in their lives.
Moreover, parental control applications (for both *desktop* and *mobile* environments) are becoming an indispensable tool for adults, due to the increasing use of technology by children.

Graph 17

Age range of cyberbullying victims



Source: ESET Latinoamérica

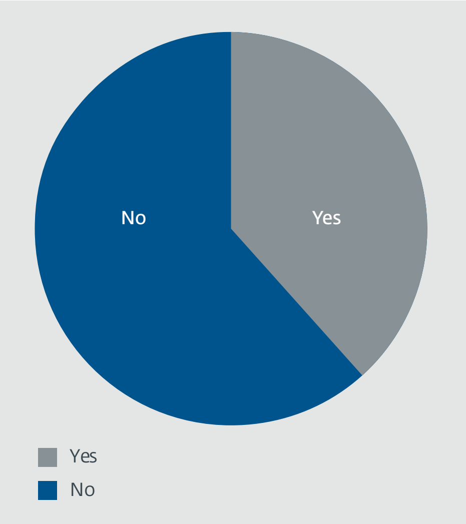
Unfortunately, the trend tends to be towards an increase in the problems already mentioned. According to 75% of those surveyed by ESET in Latin America, this type of problem occurs frequently; nevertheless, a sizeable proportion of the population is unaware of laws punishing these types of acts.

In this context, it is essential not only to continue creating laws to give support and protection to minors affected by such incidents in the online world, but also to promote and raise awareness of these laws.

Such legislation must be accompanied by "home rules"; that is, social standards. Fathers and mothers at home, and teachers and principals at educational

Graph 18

Do you know any law in your country that penalizes these acts?



Source: ESET Latinoamérica

institutions should promote awareness of such standards by encouraging the use of the Internet in an orderly fashion, with clear rules and guidelines.

For example, the non-profit organization *Securing Our eCity proposes the use of an Internet Contract*, so that parents talk with their children about these issues and make basic agreements about the use of computers, mobile phones, the Internet, and technology in general.

One of the biggest concerns among adults about this topic is how they can monitor minors in social networks and online games. Communication and awareness form the first barrier of defense for dealing with this kind of abuse, and so it is of vital importance to encourage discussion periodically between children and adults, with the aim of narrowing the generation gap and so that at the first hint of doubt or suspicion, minors can alert their parents. It is essential to deal with the notion of anonymity and false identity on the web, by explaining how easy it is to generate a profile with false data.

Ultimately, awareness between adults and minors will be essential to better address these issues as these disquieting trends continue to grow.

> ULTIMATELY, AWARENESS BETWEEN ADULTS AND MINORS WILL BE ESSENTIAL TO BETTER ADDRESS THESE ISSUES AS THESE DISQUIETING TRENDS CONTINUE TO GROW

12

2016:
the security challenge

12 2016: THE SECURITY CHALLENGE

Throughout the preceding sections of this Trends Report by the ESET Research Laboratories, we have reviewed and discussed the problems, events and challenges that information security will have to face in 2016 and the years to come. In an increasingly dynamic and challenging situations, individuals and businesses will need to undergo regular training in order to protect their information properly.

It is a fact that attacks are growing more sophisticated. Protecting a company's information and data seems to be an arduous and complicated task, and finding trained personnel willing to combat continuing attacks gets more difficult all the time. However, though ***it seems to be an uphill struggle***, at ESET Research Laboratories we believe that it is possible to protect individuals and businesses, and that technology, management and education, combined together, are ***key factors*** for security.

As we have stated, technological advances bring new possibilities for individuals and for businesses. And cybercriminals are well aware of this fact. Given that technology affects so many aspects of everyday life, insecurity could be "everywhere". Consequently, at ESET, we believe instead that security should be everywhere, and insecurity banished. And therein lie the challenges for businesses, governments and individuals.

The challenges for the future are not impossible to accept: the fact that in 5 years there will be 25 billion devices connected to the Internet, according to ***Gartner***, does not mean that users must become paranoid about their privacy and information security. As well as needing ***to continue investing in security***, companies will have to assess the technologies they use to ***detect and eliminate the threats from their networks***. The implementation of layers of protection, or technologies able to detect an attack in its various stages, to minimize the exposure to cases of information leakage and data hijacking, to reduce the exposure gap and the response time of each incident – all these factors need to be considered.

Employees' ability to detect possible attacks, which occur mainly through emails, helps to reduce the time needed for the identification of such attacks. This ability is not possible, though, without education and training in information security. However, this will not be developed if the organization does not see user involvement in security as an important aspect of its business. In other words, if the company does not care about the education of its employees and the correct implementation of protection technologies, it will be a lot more vulnerable to cyberattack.

Based on what we expect to see in the future, it is important to stress that information security does not wholly depend on advances in cybercriminals' attack methodology, but also on the measures taken by individuals, governments and companies to defend their information, systems and infrastructure. Indeed, each group has to accept the challenge and assume responsibility for improving and maintaining information security.

There are different challenges for the years to come: from users' demands for ***higher levels of security and privacy***, the importance of keeping children safe on the Internet, and the actions that security agencies should take to combat cybercrime, to the implementation of millions of new devices that interconnect the lives of individuals, businesses and governments. Security software companies, protection technologies and the education of consumers and end-users will play major roles in the understanding, analysis and protection of the most diverse technologies.

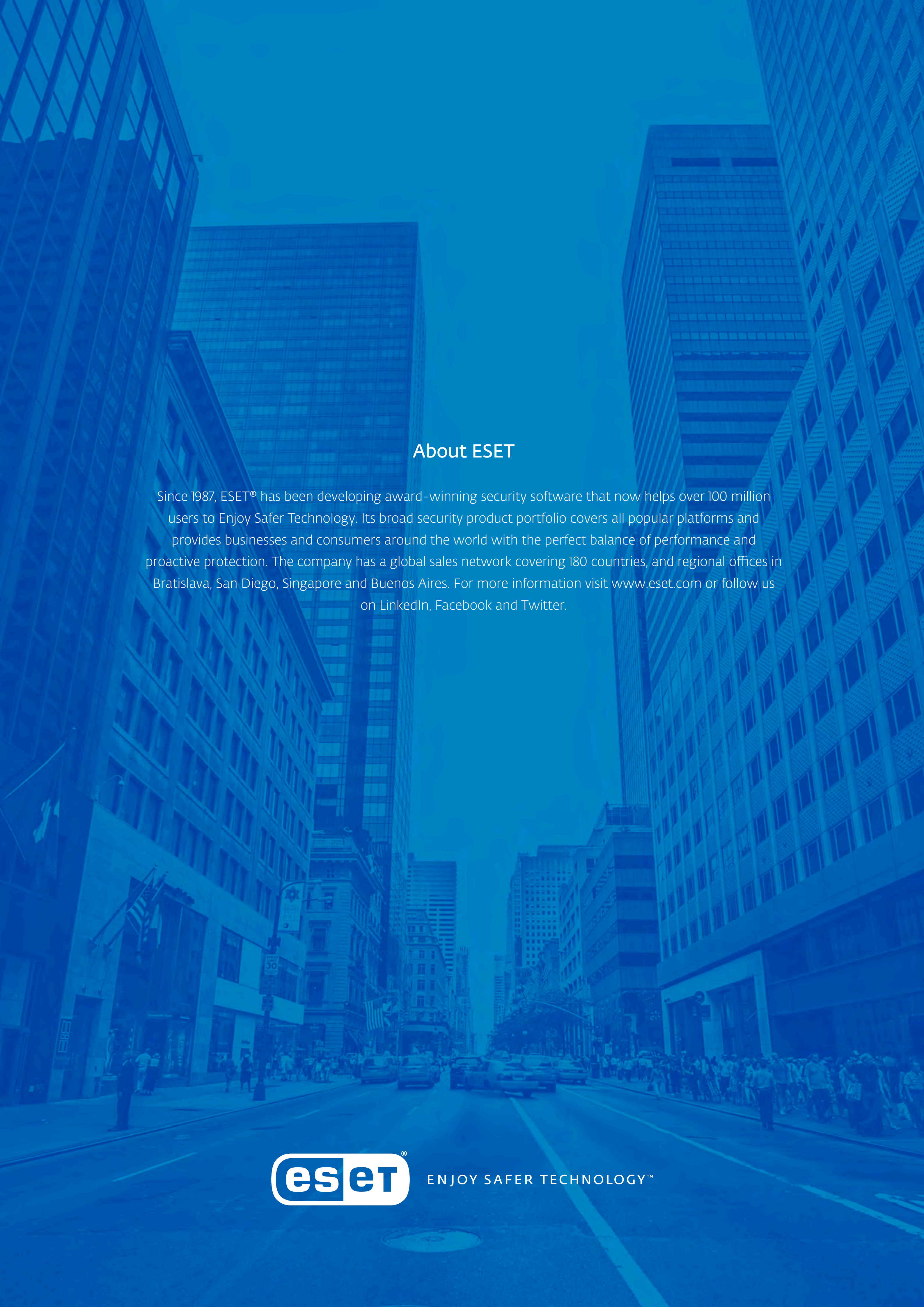
The role of the user is becoming more important and this is a trend that will continue to grow. For some years now, users have been demanding that companies provide more and better security to protect their data and information. But beyond these demands, it is more important to educate individuals about Internet security and how to be protected. In other words, users can no longer be indifferent towards their information, since most of it is stored in different digital formats and in many different places far beyond the borders of their own systems. In 2016 and the years to follow, users will have to play a more active role regarding their own security, by continually learning to protect their data as well as relying on the protection afforded by software security companies and the services they use.

Companies will have to base their strategies on three pillars: technology, management and education of employees. That said, the roles of the state and the security agencies should be stressed as well, in terms of passing laws that serve to encourage the secure evolution of new technologies, defining standards and rules that promote respect for users' privacy, and ensuring that services and infrastructure continue to serve to facilitate countries' development. In addition, investment in research and development into new technologies must be accompanied by a security plan that assesses and describes the security measures to follow.

Therefore, with a larger potential attack surface and new vulnerabilities emerging in widely-used technologies, the greatest challenge for 2016 will be to focus on protecting networks, Internet access and the way in which devices are interconnected. From the router that provides access to the Internet in the home to the infrastructure of the most modern cities, the best security practices should be applied to protect data, information and privacy. This is collaborative work that requires more active participation from users, companies with a critical understanding of information protection and a proactive role in security strategy, and governments promoting economic development while ensuring the establishment of (and compliance with) standards, so that both companies and individuals will be protected in the event of a cyber incident.

2016 will be a most challenging year. We must face it with a proactive attitude of security awareness. We must take account of all the aspects of security presented in this report; we must focus on all the new devices that will come onto the scene in the near future.

→
2016 will be a most challenging year. We must face it with a proactive attitude of security awareness.



About ESET

Since 1987, ESET® has been developing award-winning security software that now helps over 100 million users to Enjoy Safer Technology. Its broad security product portfolio covers all popular platforms and provides businesses and consumers around the world with the perfect balance of performance and proactive protection. The company has a global sales network covering 180 countries, and regional offices in Bratislava, San Diego, Singapore and Buenos Aires. For more information visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

ENJOY SAFER TECHNOLOGY™