TRENDS FOR 2015

TARGETING THE CORPORATE WORLD

ENJOY SAFER TECHNOLOGY™

CONTENTS

1 Introduction

① INTRODUCTION

The "Trends For 2015 – Targeting the Corporate World" report by the ESET LATAM Research Lab invites you to review some of the most significant cases that affected computer security in 2014, and to consider and present the challenges and threats expected for 2015. This report will try to address the different types of threats and security incidents we have witnessed during the year classified by category in order to answer the following questions: what will we find during 2015 in terms of IT security? And how, therefore, can companies and individual users prepare themselves to get through next year in safety?

Throughout the year, we have read many posts about attacks involving APTs (Advanced Persistent Threats). But what is an APT? What is its impact on a company? And why do we expect to keep seeing these kind of threats in 2015? These are some of the questions we will answer in this document, as we review the events of the last few years and prepare ourselves for the next.

2014 saw many important events take place in computer security: more than once we have found ourselves talking about data breaches, exploitation of vulnerabilities, and the appearance of different threats that compromised the data security and privacy of individuals and companies.

In our Trends 2014 article, we highlighted the importance of privacy of users, and what they could do to browse safely on the Internet. However, related incidents involving leakage of users' photographs and videos only reinforced the importance of privacy, as well as emphasized the importance of the methods implemented by cloud services and various social networks to safeguard information. At the same time, users' concerns about the protection of their online privacy continued and they complained when the services they had trusted became compromised. So, which methods to use to be safe online? And also, what are the challenges a company faces concerning privacy, both its own and that of its clients and employees?

Finally, we also stress that since the end of 2013 we have witnessed a new wave of threats that encrypt the information of their victims in order to demand that a ransom be paid for the recovery of their data. Ransomware – with CryptoLocker leading the list – became a headache for companies and users alike, even affecting mobile devices. Is this a passing threat or a trend that is here to stay?

In short, throughout this document we will review malware that encrypts users' information, the data leakage of millions of credit and debit cards put on sale by cybercriminals who attacked point of sale (PoS) systems, the vulnerabilities in heavily-used systems that threatened the security of lots of companies worldwide – regardless of whether they were large corporations or SMBs. Last but not leas, we will cover the targeted attacks, all of which were included in the challenges companies had to face during 2014, and that will most likely continue – and, in some cases, even deepen – in 2015. We invite you to see what's ahead in IT security trends for 2015 and the best practices needed to prepare yourself to face those challenges, at the corporate level as well as for home users.

ESET LATAM Research Lab

② Evolution of APTs

- The Danger from APTs
- Changes in Cyber-attack Strategies
- APTs Keep the Door Open for Cyber-espionage
- APTs in the Forefront of Attacks on Companies for 2015

② EVOLUTION OF APTS

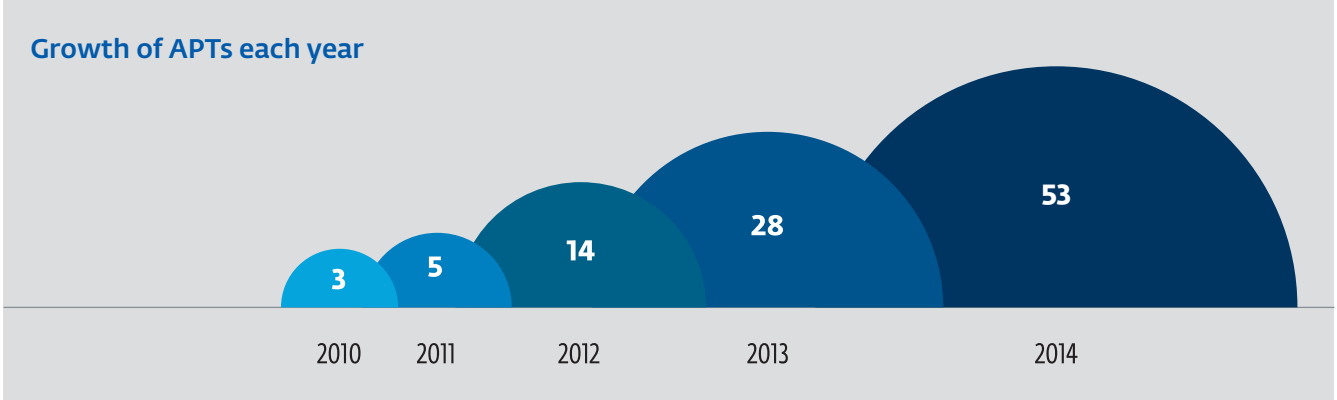


Chart 1. Growth in the amount of analyzed APTs

There is no doubt that in the last few years we have witnessed a change in the way cybercriminals perform their attacks. Even though "traditional threats" are still a significant risk for organizations, there has been a trend towards ones we have already seen throughout 2014: attacks that were tailor-made for particular victims.

This type of attack is known as an *Advanced Persistent Threat* (APT). According to the US National Institute of Science and Technology (NIST), an APT is "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."

As can be seen in **Chart 1**, the number of analyses and studies concerning APTs has increased in the last five years, even doubling the quantity seen in 2013 in just the first ten months of 2014.

However, the increase in volume of these threats does not mean they are more widely used. In fact, they are becoming increasingly discreet, since the attacker's objectives are to gain surreptitious access to information and clandestine control of the system. The implementation of APTs requires dedication and expertise in order to make attacks effective against a specific target and, as we have already mentioned, the idea is to remain inside the network as long as possible so as to exfiltrate the greatest amount of information.

The evolution in the frequency of the APTs does not show a behavior pattern with respect to the way they show up. As can be seen in **Chart 2**, the only pattern that can be observed in the appearance of APTs is one of growth. In fact, if we analyze their frequency of appearance on a monthly basis, we can see the values increasing over the last five years.

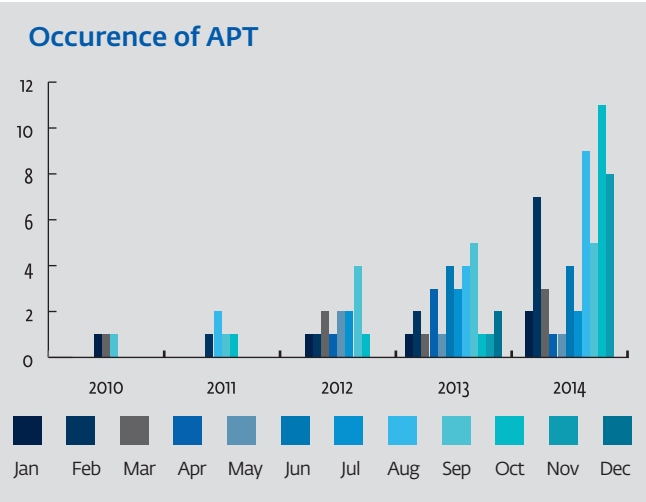


Chart 2. Evolution in the number of APTs

The Danger from APTs

By developing APTs, cybercriminals create a threat that can endure for a long time, with the ability to change itself and to infest the greatest number of systems possible within the same affected network.

We should add that APTs sometimes exploit 0-day vulnerabilities, making them much more difficult to detect and thus causing their victims to suffer more substantial losses.

Even though it is clear that attacks using APTs have become more frequent over the past few years, some cases had a bigger impact than others. One example is Flame, a threat that affected the Iranian Oil Ministry, which also had its predecessors Duqu and Stuxnet, both malicious programs which, by exploiting 0-day vulnerabilities, managed to access nuclear programs in the Middle East and cause significant damage.

Even during 2014, as can be seen in Chart 3, threats like the BlackEnergy family were employed for Distributed Denial of Service attacks, for distribution of spam, for bank fraud and even for targeted attacks, which all demonstrate the versatile functionality these threats offer to cybercriminals.

We could write a long list of examples of the most recent cases that would leave no room for the other issues we need to address in this document. However, what is really important is to remember that, regardless of a company's specific core business, we should be aware of this kind of attack in order to take the most effective protective measures.

Changes in Cyber-attack Strategies

When we talk about cyberattacks, we usually mean campaigns through which the technological infrastructure of companies is affected in order to exploit vulnerabilities and steal some kind of sensitive information that generates advantage for the attackers.

The difference with APTs is that, although the final purpose is usually very similar to the traditional attacks, we start to see that these are longer campaigns, more specifically targeted and stealthier, that seek to gather a greater amount of information to compromise systems in the long term or even to monitor what happens inside the victims' systems.

Given these differences, we find more complex Social Engineering campaigns that are not limited to the use of exploits and malicious codes, either generic or acquired on the black market.

APTs Keep the Door Open for Cyber-espionage

After talking about the differences between the APTs and the more traditional threats, and given that it is increasingly common to find more APT-affected companies and entities, it is important not to forget that what attackers are looking for is to steal specific data or to cause specific damage. Since they are looking for very important and sensitive data, it is normal for these attacks to last several months or even years, during which time the attacker identifies vulnerabilities and assesses the security controls that protect the target systems in order to acquire trusted access to privileged information and extract it without raising suspicions.

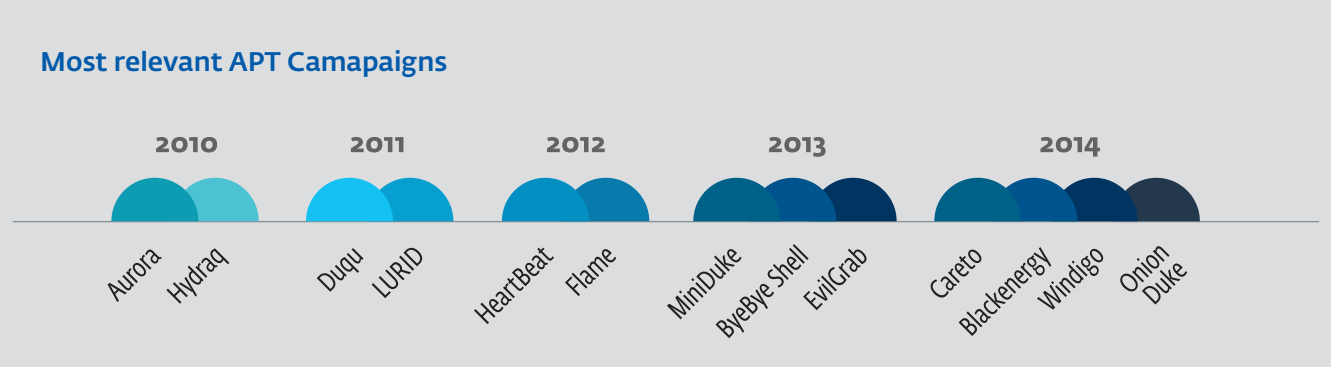


Chart 3. Evolution of the APTs

For the last few years, the ESET Research Labs from all over the world have been announcing the discovery of attacks of this nature in the Latin American region. Consider, for example, the targeted attack seeking to steal confidential information from Peruvian institutions and companies. The Medre operation managed to collect more than 10,000 files of blueprints and projects created with the Autodesk AutoCAD program.

Cases worldwide, like the reappearance of BlackEnergy in 2014, tell us this is a phenomenon we can find at the global level. This trojan, originally created to perform Distributed Denial of Service (DDoS) attacks, evolved into sophisticated malware with a modular architecture: a tool just as capable of sending spam and committing bank frauds online as of performing targeted attacks.

Also in 2014, the ESET Research Lab reported a campaign titled Operation Windigo, which managed to affect more than 25,000 Linux and Unix servers during the past two years, sending spam and redirecting people visiting infected websites to malicious content.

In the case of Windigo, it is important to highlight that over 25,000 servers have been affected over the last two years, and 10,000 of them were still infected at publication time. Moreover, if we consider that each one of these systems has access to considerable bandwidth, storage, computing power and memory, it is not surprising that this single operation was responsible for sending an average of 35 million spam messages on a daily basis, and that more than half a million visitors to legitimate websites hosted on infected servers were redirected to an exploit package daily.

▶ APTs in the Forefront of Attacks on Companies for 2015

As we have reviewed in previous section, it is clear that the growth of APTs over the last five years has led to the development of new attacks. Therefore, for 2015 we can expect that more companies will report having suffered the consequences of ever more complex and evolved APTs, which will exploit the constantly appearing security vulnerabilities, leaving the door open for even more data exfiltration.

We should remember, given the nature of these threats, that most of the cases that will be reported in 2015 will probably have been perpetrated in 2014. Unfortunately, these cases of infection are only reported and known after the company has been compromised. Therefore, it is of utmost importance to take all precautionary measures to avoid becoming a victim of this kind of attacks, both through the implementation of technology, and also by user education and proper Information Security Management on part of the company.

At the same time, it is important to note that although the largest companies can seem to be a more interesting target for attackers, the truth is that no organization is immune to attacks of this nature, given that the attacker looks for valuable information – something that every company, organization or entity has. Therefore, it is a challenge for companies of all sizes to adopt the necessary security measures so that they do not become victims.

Finally, we have already seen companies affected by APTs; though we expect that in 2015 (and henceforth) this kind of attack will become more prevalent, as has already happened with other threats that originally were more common in some regions and shortly after have spread more globally.

3 Point-of-Sale Malware

- The Objective is Information
- POS Malware and 2015

③ POINT-OF-SALE MALWARE

Since the end of 2013, there have been multiple reports reaching the news that dealt with points of sale terminals of large retail chains being compromised by malicious code. It soon became clear that this was a new wave of attacks which, in barely a few months, passed millions of credit and debit card records to the hands of cybercriminals. In the next few paragraphs we will share with you some of the most important facts about these attacks and discuss why in 2015 companies will have to pay attention to this kind of threat.

Point-of-Sale Malware or PoS Malware, as it is usually called, refers to different malware families that compromise Point-of-Sale terminals in order to steal credit- or debit-card data while the user is making a purchase. To reach this objective, the cybercriminals not only need to infect the machines used to read the users' magnetic-band cards, but they also need to bypass all of the security levels of the POS systems. Large companies like Target, Home Depot, and UPS, among many others, fell victim to this type of attack in spite of the controls they had implemented. One characteristic that both the Target and the Home Depot attacks shared is that the malicious code used to steal the card data from the points of sale were BlackPOS variants. The code of this malware family was leaked in 2012 and, as happened with Zeus, this could have generated multiple variants. Even the Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) in partnership with the United States Secrets Service (USSS) issued a warning on some PoS malware attacks with a technical report of the threat.

The information theft happens directly at the point of sale, where malware families such as JacksPos, Dexter, BlackPOS and other threats – detected by ESET products as Win32/BrutPOS or Win32/POSCardStealer – extract the credit card data from RAM. While for some the process may seem simple, the cybercriminals in fact had to bypass many additional security controls and, even today, how they managed to access the terminals to infect them in the first place remains unknown or was not disclosed. It is more than clear that we are facing complex large-scale attacks, similar to the APTs presented in a previous section of this report; however, the final objective in this case is the theft of credit card information and not the confidential data of companies or governments.

▶ The Objective is Information

Credit cards have magnetic bands that store their information. The necessary data to make a purchase, such as the credit card number, the cardholder, the expiration date and the security code are stored in the three tracks that make up the magnetic band. The moment we swipe our card through the magnetic stripe reader, all this information is loaded into the point-of-sale system to validate the purchase.

Due to safety regulations, all communication between the credit card company and the retail store where the purchase is made has to be encrypted, as is any stored data. However, there is a small window of exposure in which the card data are not encrypted – this is the moment when they are read and stored in the computer's RAM. This is the point when threats like Dexter come into play and read the memory of the process corresponding to the payment system so that they can extract the card data afterwards. Once the card data have been extracted, the next step for the malicious code is to send the credentials and, according to different investigations, this step can be very varied: in some cases, the information was sent via HTTP or FTP; in others, the collected data were stored on one of the targeted organization's own servers, to be accessed later on by the cybercriminals for extraction.

At the 2014 Virus Bulletin conference, one of the most important in the antivirus industry, we had the chance to attend the talk "Swipe away we're watching you" by Hong Kei Chan and Liang Huang, where the authors presented a detailed description of the mechanisms implemented by the most widely used families in these kinds of attacks to read the memory of processes and extract information from the credit cards, as well as the mechanisms used to send data to attackers.

It is important to understand how serious these threats are. They were responsible for 40 million credit- and debit-card leaks in the Target case, an event that led to the resignation of its CEO. One of the most famous cases was that of UPS, where almost 105,000 transactions with credit and debit cards were recorded. Finally, one of the cases that affected the most people due to the amount of data leaked was the one of Home Depot, where data were stolen relating to 56 million cards. In this case, the affected stores were not only located in the US, but also in Canada. The Home Depot incident is the largest relating to end-user financial information leakage yet reported.

One of the critical points regarding these kinds of attack is the time that it takes to notice that the corporate networks have been compromised. This is one of the greatest challenges for companies and, in particular, for their security teams. According to data from Verizon's 2013 Data Breach Investigations Report, it took months for 66% of the companies that were victims of data theft in 2012 to realize they had been breached. In one of his articles, Brian Krebs notes that in the case of Target, the first card leakage records go back to November 27th, 2013, giving the attackers months to operate without being noticed. According to the declarations by the CEO of Target, the incident was detected after security forces warned them about this threat, on December 15th, 2013.

In the case of the data theft at Neiman Marcus, out of a total number of 1,100,000 records, the investigations determined that the real number of affected credit and debit cards was 350,000, from July 16th to October 30th, 2013. Of these affected accounts, approximately 9,200 were subsequently used to shop fraudulently.

Specifically regarding the case of Home Depot, between the month of April – when the breach is believed to have first occurred – and the publication of the press release acknowledging the existence of the incident (on Tuesday, September 2nd), 56 million records were leaked through the company network.

Thus, becoming a victim of threats as in these cases is a matter for serious concern, given that many times a server vulnerability and lack of controls in the software update processes could open a breach compromising a company's whole point-of-sale network.

With a view to protecting points of sale, there are some things that companies should consider to minimize the exposure risk against this kind of incidents.

↘ Use a Strong Password

In general it is important to notice that many of the breached machines used default passwords or simple variants of the PoS vendor's name. For example, the three most common passwords were "aloha12345", "micros" and "pos12345." It is a better compromise between security and convenience to use a password phrase instead of a simple word, since a phrase can be easily remembered and it would still take too much time to be deciphered, given its length. Default passwords should never be used on PoS software.

↘ Limit the Logon Attempts

A common strategy is to block people after the 3rd to 5th incorrect attempts. This drastically reduces the effectiveness of Brute Force attacks, because the attacker will not be able to try the amount of incorrect passwords he needs in order to guess it.

↘ Limit the Access

Limit access whenever you can. For example, if you do not need to access the machine remotely, do not enable RDP. If you need to, make sure it is safe.

↘ Review the Update Processes

Among the PoS security measures, among other security solutions, it is possible to find tools that only allow whitelisted processes and applications to run, which means they permit only the execution of processes marked as safe. In some incidents, the threats were installed during software updates which, based on the number of machines that will be updated, may remain from a couple of weeks to several months.

▶ POS Malware and 2015

It is clear that since the end of 2013 and throughout the whole of 2014, the most important attacks have targeted the retail market. However, as far as next year is concerned, we may see now as yet unknown attacks. Cybercriminals have been able to find vulnerabilities in the networks or infrastructure of some of the most important retail chains worldwide. It is crucial for companies to rethink the way they protect their Point of Sale systems and the entire infrastructure associated with them.

Protection of large volumes of information requires the implementation of the most rigorous controls and tests that can be imagined. Even though some of the cases we mentioned in previous paragraphs seem to have been perpetrated by different groups acting against the USA, there is plenty of evidence to show that other retail chains or stores outside this country are also being attacked by BlackPOS variants.

In 2015, security teams in charge of point-of-sale systems must review the way they are protecting and isolating them to limit breaches such as we saw in the last 12 months. Information leakage of this nature is a direct blow to the business that companies can ill afford, due to both the economic impact and to the damage to the company's reputation and the trust of its clients.

That is why, after the Target and Neiman Marcus incidents, companies like VISA, MasterCard and Europay have made an open invitation through VISA's CEO, to reinforce the security measures in the payment systems and wherever the use of mobile devices could be a solution to pay, or else, a new problem for next year.

④ Information Leakage

- What Can be Done to Prevent Information Leakage?
- Why Should Companies Implement Two-Factor Authentication?
- Attacks and Their Numbers
  - Incidents in the Last 5 years
  - Breached Records – in Millions
- Protection of Company Information in 2015
- What Can a Company Do in 2015 to Protect Their Information?

④ INFORMATION LEAKAGE

Over the past few years, newsworthy cases of information leakage from companies, governments and other entities have had an impact on thousands or even millions of users. 2014 was no exception – there were major information leakage cases and some of that stolen data appeared on different cybercriminal underground forums.

We began 2014 with the piece of news that a retail company's security had been breached in the last months of the previous year, leaving data from more than 40 million credit and debit cards in the hands of attackers. Although PoS systems were one of the main victims of information leakage, they were not the only victims.

Companies like eBay and Yahoo! had to notify thousands or millions of users that their passwords had been breached during an attack. Unfortunately, these breaches were not enough of a warning sign to get business to take action. Instead, companies continued to be affected either directly or through third-party tools, and the list goes on with names such as KickStarter, Spotify, Bitstamp, Snapchat, and Dropbox, among others. One of the last cases reported in 2014 involved Sony once again like in 2011. Cybercriminals managed to exploit their systems and among the losses were full versions of movies yet to be released.

What Can Be Done to Prevent Information Leakage?

In our previous report "Trends for 2014: The Challenge of Internet Privacy," we stressed the need for a two-factor authentication tool to improve security during user logon. According to the data revealed by Risk Based Security, during the first half of 2014, 70% of security breaches involved password exposure. This figure points to once more the importance for companies to have a two-factor authentication system, a challenge that they will have to face during 2015.

If we consider the services and sites that introduced two factor authentication to protect their users, we find companies like Google, Facebook, Twitter, and Github, among others. The incorporation of a second authentication factor through, for instance an OTP (One-Time-Password) enhances security during user logon and it also safeguards data in the event that users' passwords are stolen or leaked, either by means of a malware infection in their own systems or through a security incident on the company's network.

Why Should Companies Implement Two-Factor Authentication?

Implementing two-factor authentication for connection to the corporate VPN, CRM or other Web services is not merely protection for employees, but also a value-added service that can be offered to clients and providers who interact with the company. In order to face all the challenges of information leaks and other attacks that can affect companies, implementation of a two-factor authentication system will help protect them in 2015.

Attacks and Their Numbers

Many of the security incidents this year have had financial or point of sale systems as targets, as you will be able to see in the corresponding section of this report; nonetheless, other industries were also affected. One of these cases is the US Community Health System (CHS), which became the victim of a data breach involving 4.5 million healthcare records. According to a statement made by the institution, its systems fell victim to an APT attack originating from China, based on the results of the investigation conducted by the company and Mandiant.

The CHS case was not the only one targeting the healthcare industry. According to a report carried out by the US Identity Theft Resource Center, as of December 2014, there were 304 reports of security breaches in medical institutions, representing 42.2% of the total incidents. Even though this report indicates that the greatest number of attacks targeted healthcare institutions, around 80% of the data actually breached corresponds to the business sector, where information leakage account for 3 out of 10 cases.

Industry	Number of breaches (% of the total amount)	Stolen records (% of the total amount)
Banking/Credit/Financial	41 (5.7%)	1,182,492 (1.4%)
Business	237 (32.9%)	64,731,975 (79.3%)
Education	54 (7.5%)	1,243,622 (1.5%)
Government/Military	84 (11.7%)	6,494,683 (8%)
Medical/Healthcare	304 (42.2%)	7,944,713 (9.7%)
Total	**720**	**81,597,485**

Table 1

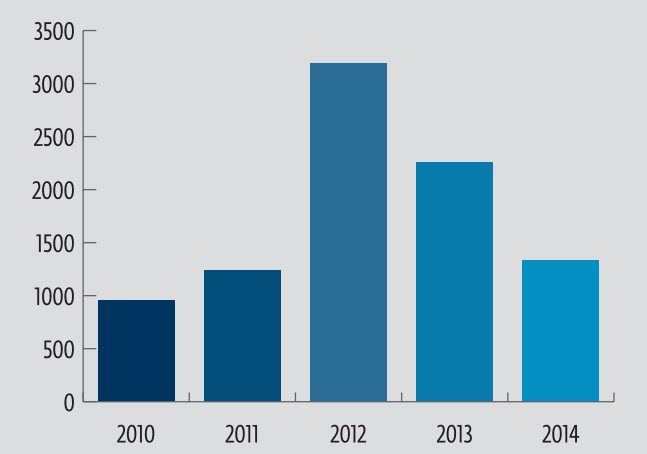


Chart 4. Incidents in the Last 5 years

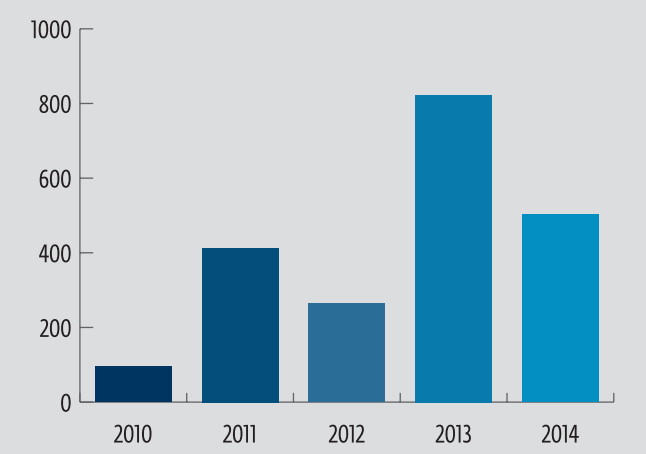


Chart 5. Breached Records – in Millions

The information contained in the ITRFC report accounted for a lower number of attacks if we consider the Risk Based Security report. According to the security firm, attacks during the first six months of 2014 were fewer than in previous years. However, in spite of having recorded half the number of incidents seen in 2013, during 2014 there were 60% more of information leaks as compared to the previous year, making the point that "more attacks" does not necessarily mean "more data leakage."

▶ Protection of Company Information in 2015

Safeguarding information is an increasingly important requirement for companies, as well as a guarantee for the continuity of the business. Based on the main security incidents witnessed throughout 2014 and on the methodologies used to breach corporate defenses, we can expect that this year corporate IT teams will have to face more complex and stealthy attacks. The evolution in the complexity of attacks is, like the actors taking part in this process, a constant challenge for corporate security, since the companies not only have to pay attention to the vulnerabilities the attackers are trying to exploit, but they also need to understand the reasons why their businesses might become a target for attackers.

What Can a Company Do in 2015 to Protect Their Information?

The implementation of data encryption on mobile devices, corporate servers, laptops or other endpoints minimizes the chance of exposing corporate information due to a malware attack, the loss of equipment, or an unauthorized intrusion. In addition, a well-implemented two-factor authentication solution increases the security of company systems during logon. According to the data in the 2014 Risk Based Security report, 57% of the breaches during the first half of 2014 involved usernames, email addresses and user passwords. In 2015, companies in Latin America and the rest of the world will be able to enhance their system and infrastructure security through the implementation of two-factor authentication, which ensures securelycontrolled access to corporate information.

5 Vulnerabilities – Impact and Challenges for 2015

⑤ VULNERABILITIES – IMPACT AND CHALLENGES FOR 2015

The year 2014 was a critical one regarding software vulnerabilities, not only due to their impact on the affected systems, but also due to the large number of systems involved. If we merely mentioned the cases of Heartbleed, Shellshock and Poodle, – as well as the impact they had in the media and in the course of action taken by security teams – it would be more than enough. However, though these may have been some of the vulnerabilities with the greatest recent impact, they were not the only ones. With the creation of unknown vulnerabilities that exploit software bugs, cybercriminals have managed to compromise the systems of companies, government entities, and more.

The potential impact of a critical vulnerability is extremely important, especially when it affects two thirds of Internet servers, as happened with the Heartbleed case. This vulnerability in OpenSSL affected thousands of servers worldwide, because it allowed the attacker to read a memory space that could host the access credentials or the keys used for data encryption. As a result, the Free Software community responded to the incident by issuing a vulnerability patch and also created LibreSSL, a new project developed as an alternative to OpenBSD group's OpenSSL. At the same time, many services and servers kept on using vulnerable versions of OpenSSL, enabling various cases of information leakage that led to arrests.

Another vulnerability was Shellshock, an error in the most widely used command-line interpreter of GNU/Linux and other UNIX-based systems, such as Android and Mac OS X. This bug allowed remote code execution, so that an attacker could take control of a system affected by this vulnerability. Shellshock was the second vulnerability reported in 2014 that affected a large number of systems. Once again, the Open Source community responded quickly, so system administrators were able to install the security patches. Nonetheless, some cases were reported in which this vulnerability was used for malware propagation because some systems were not patched promptly.

Apart from looking for critical 0-day vulnerabilities, attackers generally use different exploits to perform these kinds of attacks. ESET's labs have reported many cases where cybercriminals exploited specific vulnerabilities to bypass security measures. Notable exploited vulnerabilities include those that feature in the BlackEnergy campaigns that targeted Ukraine and Poland, a case where cybercriminals chose Microsoft Word exploits (CVE-2014-1761) or Microsoft PowerPoint exploits (CVE-2014-4114) to compromise different targets. In other instances, there were reports about websites that, once infiltrated by attackers, were used to exploit vulnerabilities on the systems of the users who visited the pages. One example is Win32/Aibatook, a banking trojan that propagated through adult websites in Japan; this particular case used a Java vulnerability discovered in 2013.

Software vulnerabilities are hard to predict, but once they show up, cybercriminals start exploiting them over time, either for targeted attacks – as part of an APT attack or by including it in an Exploit Kit – or for malware propagation through a hacked website. Their uses are many and they are a challenge both for security teams and for home users. Thus, minimizing or eradicating the window of exposure to a vulnerability is one of the most important factors to enhance the security of a system, either in corporate or in home environments.

Throughout 2015, vulnerabilities will play an important role in corporate security, given that they always represent a risk. Those companies that decide to play a proactive role will not only be one step ahead of possible attacks, but will also have available the latest techniques to protect their systems and information. Defining the proper security policies, implementing security solutions that allow detection of exploitation attempts, and having varied security measures are the main weapons to counter these attacks. Some of the challenges brought about by software vulnerabilities can be mitigated with the installation of security patches and OS/application updates. In the case of unknown threats – i.e., 0-day threats – they are much more complex, and having a well-trained, proactive security team is one of the best defenses against them.

6 Internet of Things... or Internet of Threats?

- Home Automation Opens the Doors to New Threats
- More Connected Devices, More Online Threats
- IoT Security Concerns
- Threats Follow the Path of Technology

⑥ INTERNET OF THINGS... OR INTERNET OF THREATS?

The phrase Internet of Things (IoT) has been going around for a few years and it refers to the network of physical devices that have the necessary technology to communicate and interact, through the Internet, with other devices or human beings to affect the environment that surrounds them.

Nowadays, we can find examples of these devices in some cars, lighting systems, refrigerators, home security systems, televisions and telephones. Though these may be the most common devices today, the list is much longer and can even include the corporate environment if we consider, for instance, SCADA systems or any other industrial control systems.

Their widespread use has reached the attackers' radar and, given the fact that in 2014 we have started to see some proof-of-concept threats for these devices, in 2015, it will be interesting to see how may IoT vendors actually start addressing these security concerns.

▶ Home Automation Opens the Doors to New Threats

There are many household appliances that have evolved to the point that the most recent generations allow for connectivity to the Internet in order to consume content or share information that might be sensitive.

Throughout 2014 we were already seeing some proof-of-concept threats. For instance, we have witnessed vulnerabilities found in Smart TVs that would allow mass wireless attacks.

Even in the first months of 2014, more than 300,000 routers were attacked globally and some online content services fell victims to password leaks as well. This proves not only that the machines used are vulnerable to these attacks, but also that the services themselves are becoming more attractive to attackers. Furthermore, the Lizard Squad DDoS-for-hire service, which was powered by thousands of hacked routers, has even been hacked itself.

▶ More Connected Devices, More Online Threats

However, the domestic appliances are not the only affected devices. Smart TVs, for instance were one of the first devices for which we began to see attacks and vulnerabilities, given that they are the most widely spread. But there are also other devices that are becoming more and more widely used and for which we are also witnessing some exploitable vulnerabilities.

Just like in 2013 we saw some proof-of-concept attacks for Smart TVs, during 2014 we witnessed the first spyware samples for Google Glass, which aired concerns about wearable devices and privacy.

▶ IoT Security Concerns

The idea of being in increasingly autonomous environments that make life easier for us may seem tempting for many people. But the need for vendors to address security issues is real.

Just as some car manufacturers began in 2014 to offer rewards to security researchers who detect a security problem in their new generation of automobiles, in 2015 we would start to see these issues becoming more and more relevant.

There is an additional factor regarding the security of these IoT devices. Computers had enough time to develop before they began to communicate through complex communication networks, and when they did, these environments were stable, so that technology had its space to develop. For the new devices, the environment in which they interact is much more hostile and, therefore, they need to be designed to be secure from the very beginning.

▶ Threats Follow the Path of Technology

The possibility that the IoT becomes more of an "Internet of Threats" will depend mostly on two fundamental factors: vendors and users. So far, threats have focused on devices with the greatest number of users. As this is not likely to change, security must depend on other factors.

Therefore, the main security considerations that should be considered for 2015 are among the following:

→ Connectivity

The main characteristic of these devices is to allow interaction with the Internet; therefore, protecting the way they connect and share information is fundamental.

→ Easy updates

Due to the fact that this is an emerging and developing technology, it will be common to find vulnerabilities that will have to be resolved once the device is in the hands of its new owner. Consequently, the speed and ease of update deployment will be important if vendors are to win the race against the attackers.

→ Authentication

Since these devices will be connected to the Internet all the time, it will be important to guarantee that those people interacting with the information are really who they claim to be, so as to avoid leaks of sensitive information.

→ Trustworthy applications

The specific features and manifestations of this technology open up many possibilities to develop everyday tasks automatically. To build trust in using these devices, it will be necessary to guarantee that this is not exploited via maliciously modified applications.

→ Data encryption

Given the fact that these devices handle confidential information, they have to do it safely and securely. Therefore, encrypting this information is a good option so that third parties cannot access it in order to change or steal it.

7 Conclusion

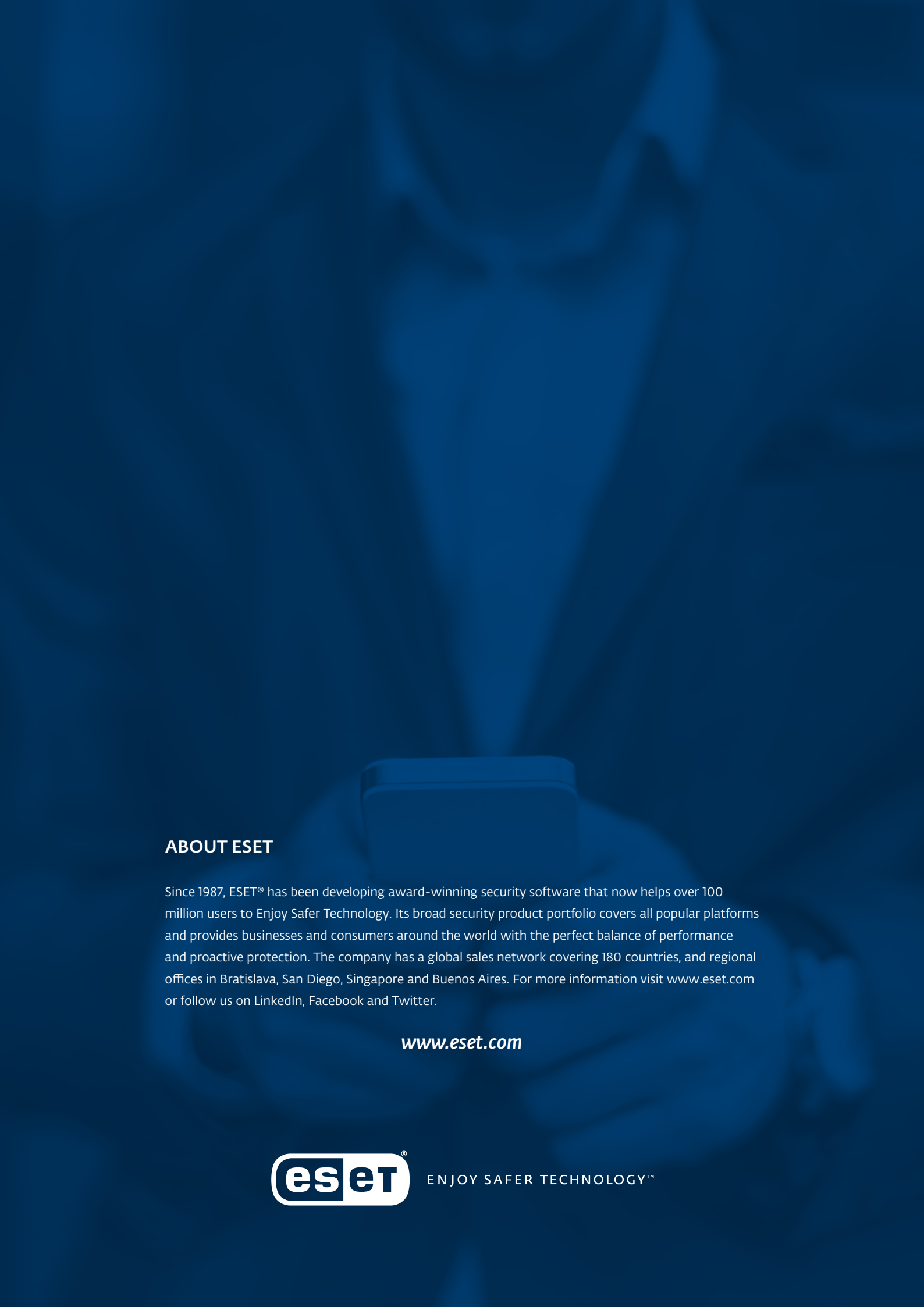
7 CONCLUSION

Throughout this document on the trends for 2015, we have reviewed some of the most important security incidents of 2014. We discussed the role of the APTs in computer attacks and the risk they represent for companies, we recalled how more than 100 million credit and debit cards were leaked in retail market attacks, and we have also mentioned that ransomware managed to encrypt information from users and companies, in order to attempt to extort money. But is there a relationship between the attacks? Who is affected? What are the complications this brought about throughout the year?

As years go by, cybercriminals keep on improving their persuasive and deceptive modi operandi, either to deceive users through Social Engineering or to use vulnerabilities to bypass protection mechanisms. The appearance of critical vulnerabilities, programming bugs and massive cases of information leakage continued to have an impact on the corporate world. Companies are protecting their information to try to protect business continuity, since corporate valuable information is one of the cybercriminals' main targets.

Within this framework of valuable information, the challenge for companies in 2015 lies in the way they will protect their data, their business, and in particular how they will manage to convince employees to become invested in their security programs. In a world where we are increasingly connected and interconnected, where our online lives are inextricably bound to our physical lives, where the Bring-Your-Own-Device policy has become commonplace in so many places, users will have to live with a profile for work, and for outside work. This user's double profile means that people can be users of different online services such as email accounts, social networks, cloud storage, and so on, and at the same time many of them develop professionally and have access to classified information. They may sometimes even be the ones responsible for protecting the data at companies, governments or other organizations.

From what we have seen in the last few years regarding targeted attacks, information leakage cases, and the evolution of cybercriminals to hijack users' and companies' data, we could certainly expect that 2015 will be a year full of challenges for IT security. The IT security teams of companies and governments will have to adopt a more proactive role in terms of defenses, using different tools to foresee and forestall the possible attacks and rely on education as a means of defense. Beyond the probabilities of what can be predicted, it's clear that businesses will continue to be one of the cybercriminals' main targets, but that is just one of the threats we will need to manage in 2015.



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.

www.eset.com

ENJOY SAFER TECHNOLOGY™