ANNUAL REPORT PANDALABS 2014

January 2015

panda

pandalabs

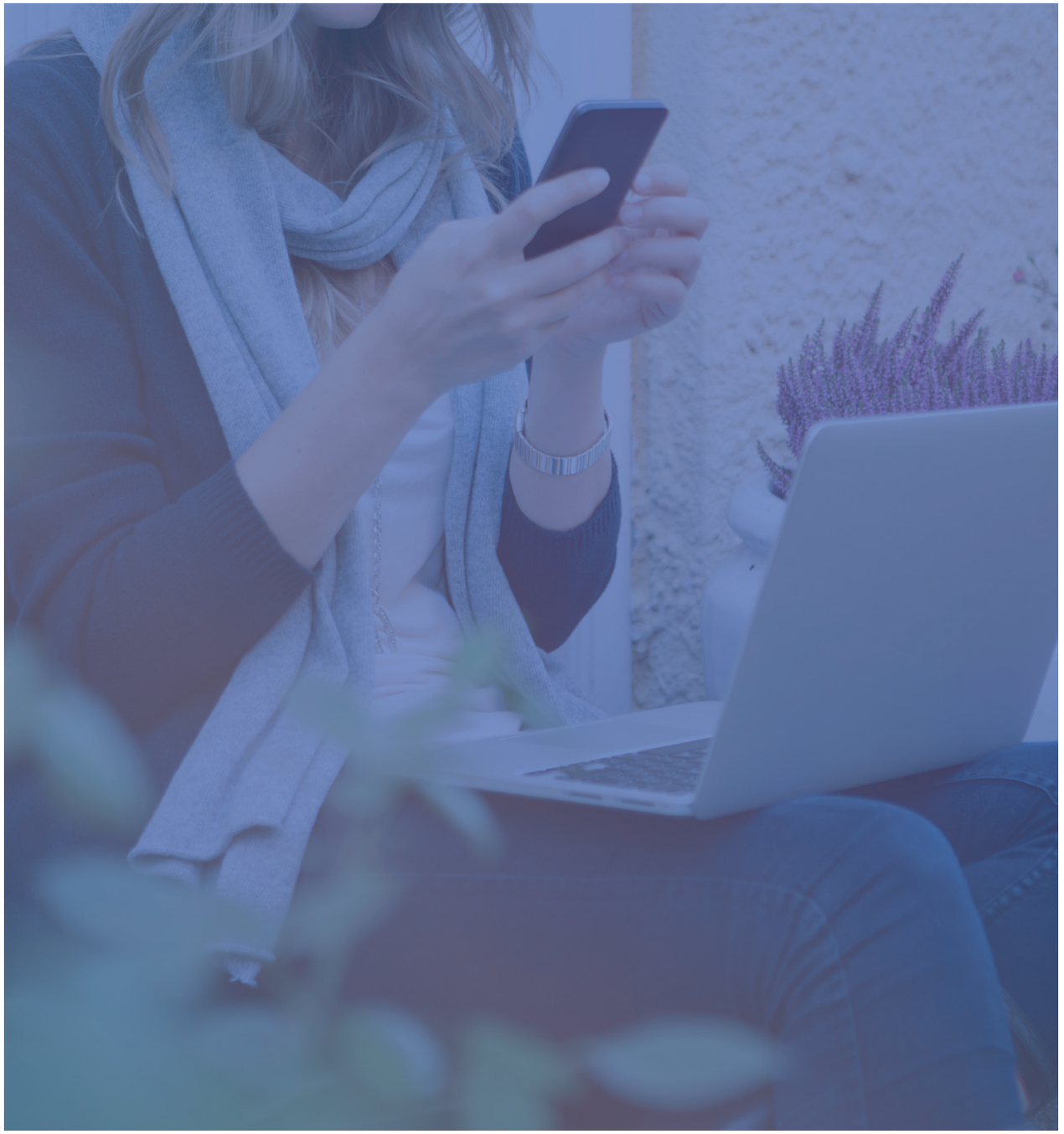
1. INTRODUCTION

Introduction

Throughout Panda's 25-year history we have had the opportunity to follow the evolution of the IT security world very closely, witnessing and participating in some of the great advances that have changed the world over the last few years. From the beginning, when only a few people had desktop computers, to the emergence of Windows as the king of operating systems, the birth of the Internet, the popularization of laptop computers, the arrival of Wi-Fi connections, the appearance of new devices such as smartphones and tablets which have become an integral part of our lives.

The world has changed dramatically over the past quarter century and data security has become a global security priority.

At the same time things have become too complex and difficult to understand at times. There is so much information available that it is overwhelming, and it is difficult to keep up-to-date with everything that happens around us. This report aims at shedding some light on the current state of affairs, analyzing the most significant events that have taken place in the IT security world over the last twelve months. We will also take a look at the security trends we can expect to see in 2015 and how to protect ourselves against future threats.



2014 was dominated by news reports of cyber-attacks.

We have witnessed large-scale data breaches at some of the world's biggest corporations, combined with smaller, indiscriminate attacks on the entire Internet user community.

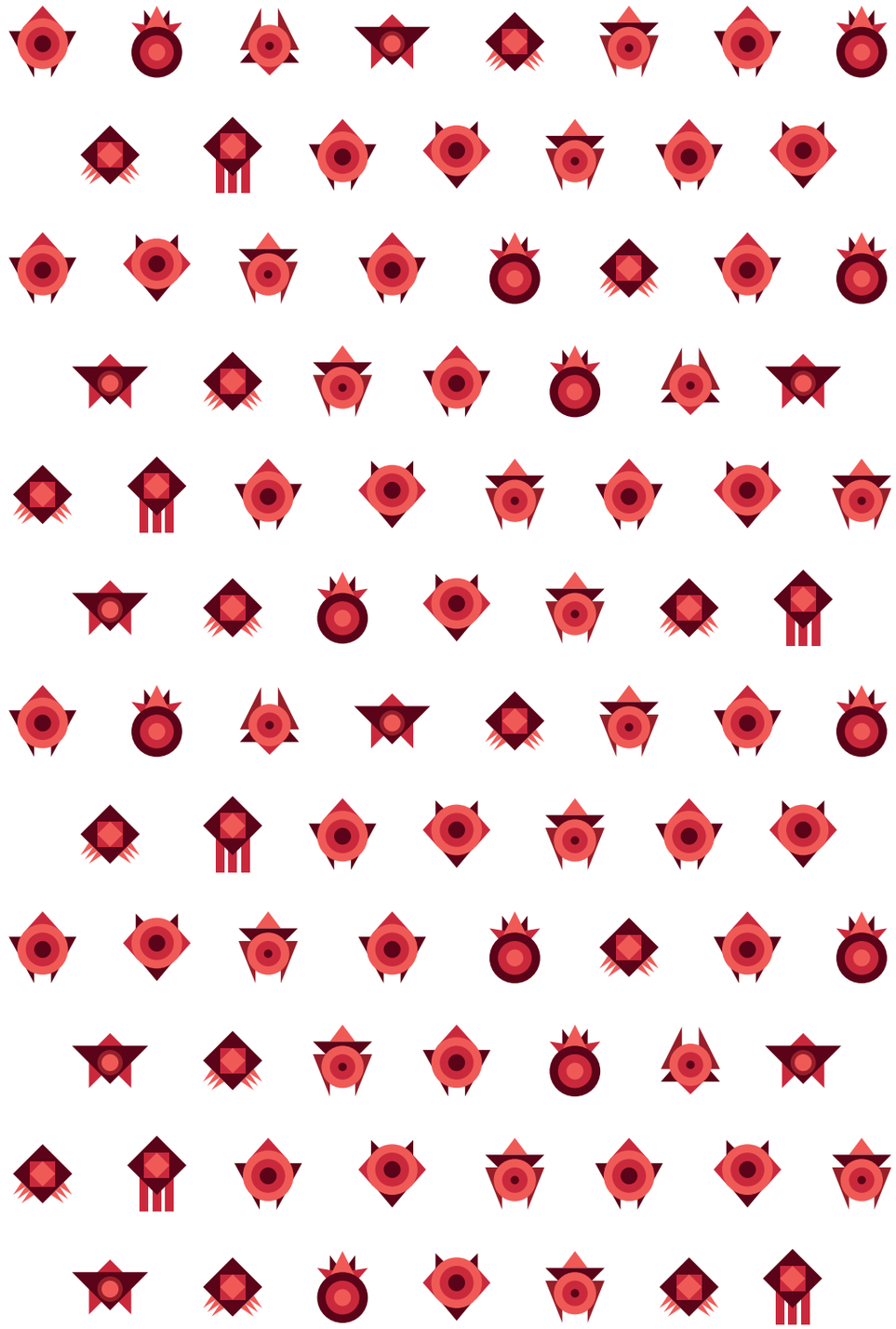
One of the most damaging attacks to occur last year was that of ransomware –with CryptoLocker as the most notable example–, a type of malware which encrypts users' files and requires a ransom in order to decrypt them.

Thousands of people have been affected by this type of attack -from home computer users to businesses and financial institutions-, who have seen their data held hostage with almost no chance of getting it back unless they had a backup or paid the ransom.

We'll analyze the most significant events that took place in the cyber-security field, the multiple cyber-attacks, and the alarming malware growth statistics recorded in this year.

In 2014 the malware creation broke new levels, with 200,000 new samples being spotted every single day.

Finally, we will discuss some of the attacks launched against mobile devices and evaluate each platform's security status. Android continues to be the leading platform in terms of market share and also cyber-criminals' favorite target, being hit by thousands of new malware strains.



2. 2014 IN NUMBERS

2014 in Numbers

We have just said goodbye to 2014, a year in which malware creation broke all records.

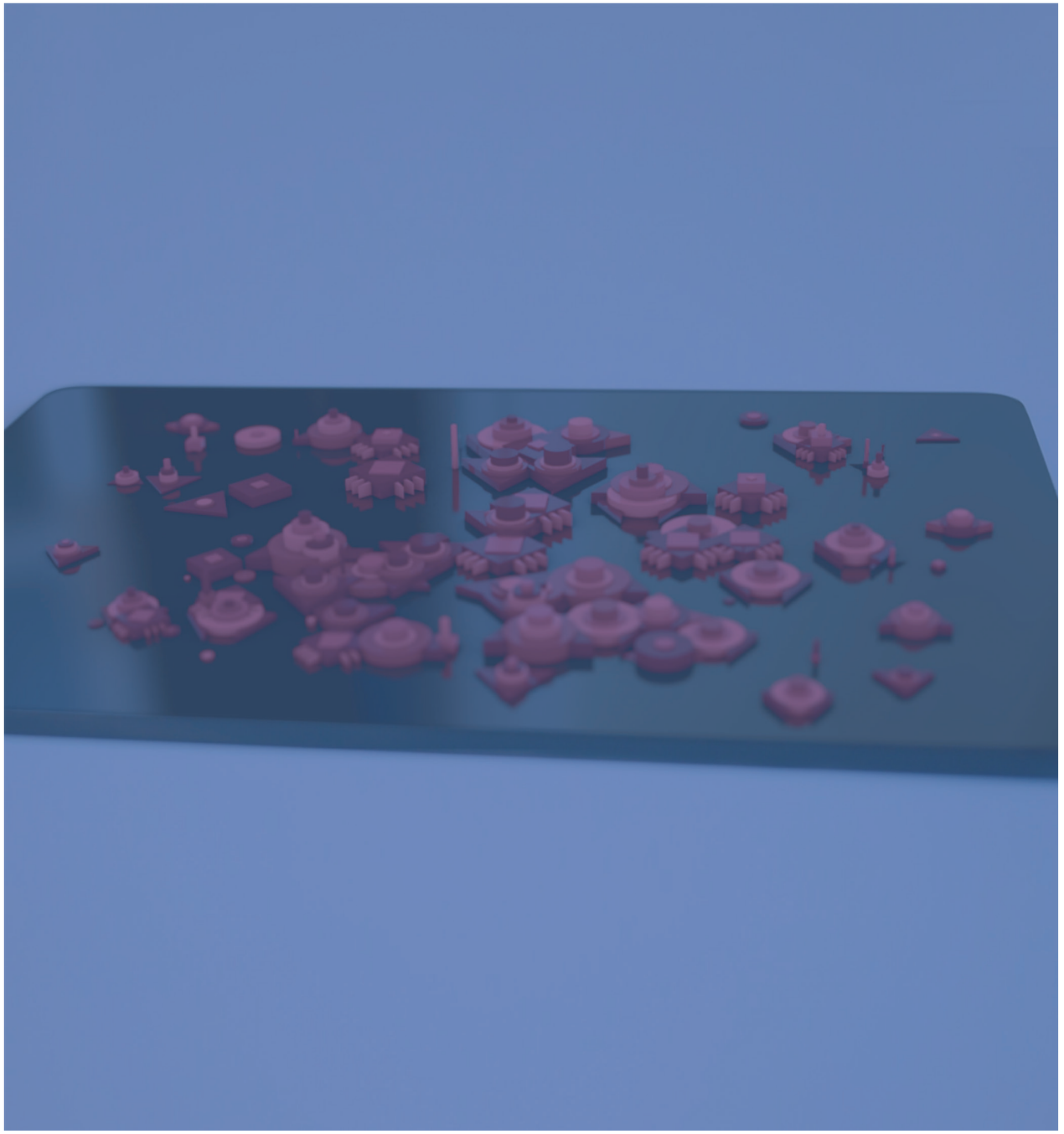
At PandaLabs, Panda Security's malware laboratory, we recorded more than 75 million new malware strains over the last twelve months.

This is 2.5 times the number of malware specimens detected in 2013, when the number of new strains unleashed by malware authors reached 30 million.

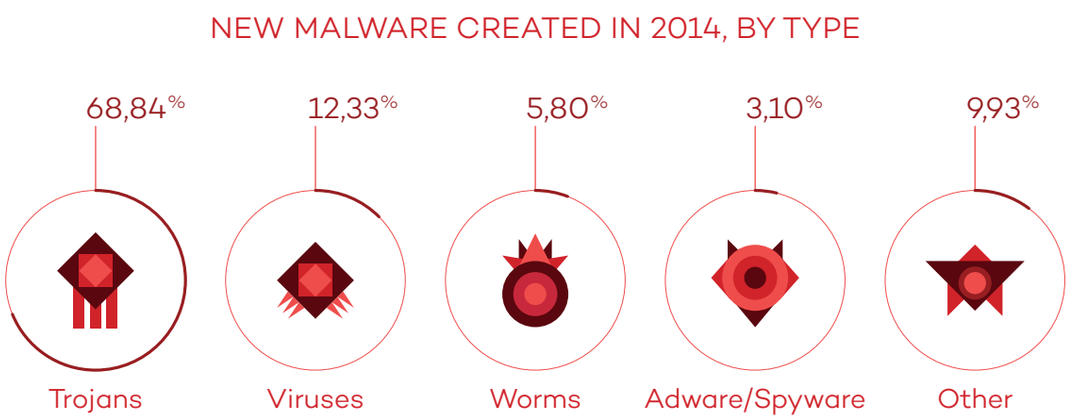
The total number of malware samples in our collection is 220 million, which means that 37.5 percent of all malware ever created was coded in 2014.

Despite 2014 was dominated by news reports of cyber-attacks on large companies, other threats also took the spotlight in what can be considered one of the worst years in computer security.

For example, ransomware like Cryptolocker, which encrypts users' files and requires a ransom in order to get a decrypter, infected thousands of people around the world.



Here is a graph that shows the types of new malware created in 2014:



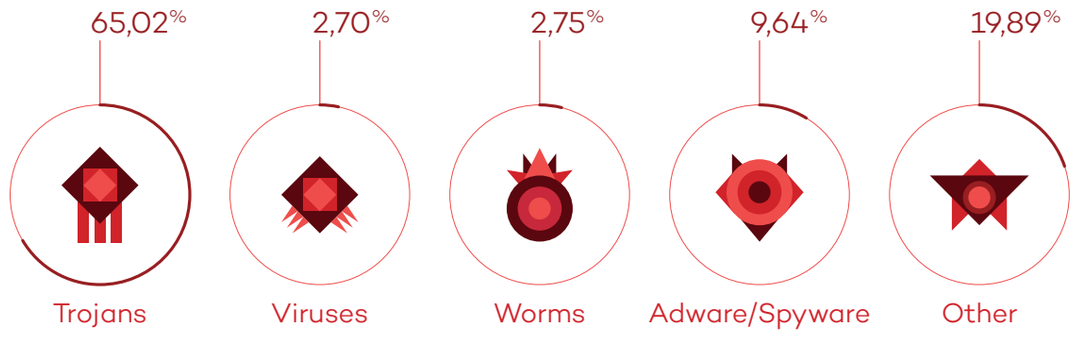
Trojans, as is usually the case, continue to top the ranking, accounting for nearly 70% of newly created threats.

Compared to 2013, there has been a significant rise in the “Other” category, with almost 10% of all new malware.

This is due, as already explained in previous reports, to the emergence of PUPs (Potentially Unwanted Programs): applications that, despite not being malicious per se, install unwanted software without properly informing the user.

When it comes to the number of infections caused by each malware category, data gathered by our Collective Intelligence platform shows that Trojans continue to top the infection ranking with a rate of 65.02%.

Here is a graph showing the infection statistics by type of malware:



Along with the usual presence of Trojans at the top of the ranking, it is worth mentioning the high position occupied by the ‘Other’ category, second, with a rate of 19.89%.

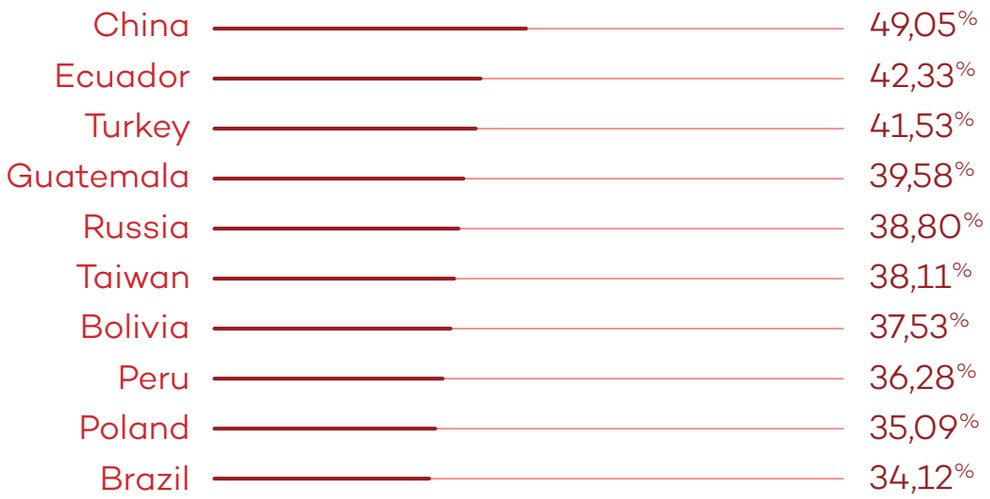
This category consists mostly of PUPs, unwanted programs that spread massively by installing themselves on computers along with the software that the user actually wants to install.

The global infection rate was 30.42%, a significant decrease on 2013.

Regarding the data across different countries, China is once again in pole position, with an infection rate of 49.05%, followed by Ecuador (way behind at 42.15%), and Turkey (41.53%).

Below we list the 10 countries with the highest infection ratios:

COUNTRIES WITH THE HIGHEST INFECTION RATES IN 2014



It's clear that the highest positions in the ranking are held by Asian and Latin American countries.

Other countries with rates above the global average include Colombia (33.27%), Uruguay (33.05%), Chile (31.27%) and Spain (30.90%).

In contrast, Europe in general is the area with the lowest infection rates and nine European countries figure in this ranking.

The list is topped by Scandinavian countries: Sweden (19.98%), Norway (20.31%) and Finland (21.21%). The only non-European country in the top ten most secure nations is Japan, which is in eighth place with 24.84%.

Below is a list of the countries with the least infections:

COUNTRIES WITH THE LOWEST INFECTION RATES

Other countries which, although they haven't made the Top 10, are still below the worldwide average include: Australia (25.28%), France (25.68%), Portugal (26.84%), Austria (27.69%), Canada (27.82%), USA (28.96%), Venezuela (29.83%), Hungary (30.96%), Mexico (31.00%), Italy (31.47%) and Costa Rica (31.50%).

3. 2014 AT A GLANCE

2014 at a glance

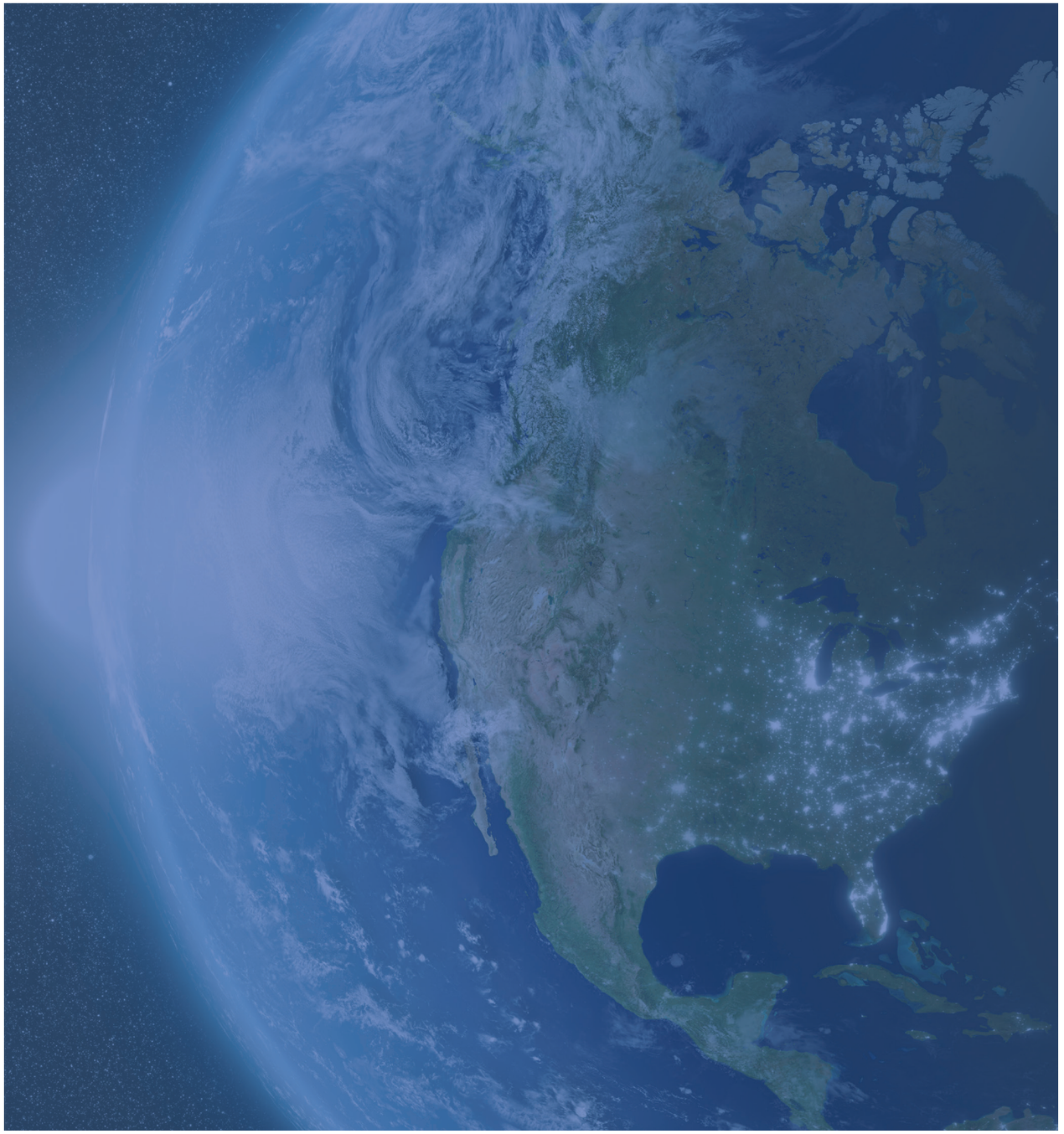
Cyber-Crime

At the end of last year, US retailer Target reported that hackers had stolen the credit and debit card details of some 40 million in-store shoppers. In this case, the breach did not affect online shoppers but customers who purchased products at the company's stores and paid with their credit cards. And not only was this information stolen but it was immediately sold on the black market.

Target Corp suffered a data breach compromising the credit and debit card details of 40 million in-store shoppers.

This year has seen some of the biggest data breaches since the creation of the Internet. At the beginning of 2014 new details emerged about the attack. According to information leaked to Brian Krebs, one of the company's Web servers was compromised. From there, a Trojan was distributed to Target's point-of-sale terminals.

The malware was specifically designed for point-of-sale systems and stole the credit card data directly from the card readers' RAM. The attackers then accessed the compromised server in Target's internal network to collect the information captured from the infected terminals.



How can companies protect themselves from this type of attack?

Antivirus solutions in this case are not the answer, as we are dealing with targeted attacks where the malware strain is specifically customized to avoid detection by the antivirus software in use.

As point-of-sale systems are usually closed platforms, you could think that a whitelisting solution would be extremely effective in such an environment.

Whitelisting solutions are designed to lock down a machine so that only certain trusted applications are allowed to run, whereas everything else is denied.

This could be a very effective means of neutralizing internal attacks in which, for example, an employee tried to infect a terminal by planting some type of malicious software in it.

However, whitelisting doesn't provide a universal solution. On many occasions malicious applications are installed by exploiting system vulnerabilities, and this is not necessarily detected by whitelisting programs.

Point-of-sale terminals are a highly prized target for criminals. Today it is not a question of 'if', but rather 'when' they will be attacked, that's why businesses need security solutions that are able to:

- Restrict software execution. Only trusted processes must be permitted to run.
- Identifity vulnerable applications, warning of any software that requires updating.
- Control the behavior of allowed processes , should there be an attempt to exploit a vulnerability in a trusted process.
- Traceability. If an incident occurs, the solution must offer as much information as possible in order to answer four basic questions: when did the intrusion occur, which users have been affected, what data has been accessed and what has been done with it, as well as knowing how and where the attack was launched from.

These are not all the security measures that could be implemented, but the four most important points to observe when securing a system.

If the Target data breach was huge, South Korea witnessed one of the largest ever cybersecurity attacks.

Credit ratings agency Korean Credit Bureau (KCB) was the victim of a cyber-attack that resulted in the theft of personal financial information from 105.8 million banking accounts. The stolen information included credit card numbers, names, phone numbers, home and email addresses and even passport numbers.

If you take into account that South Koreans on average have 5 credit cards, it means that at least 21 million users may have fallen victim to the attack, approximately 42 percent of the country's total population. In fact, the number of actual victims will probably be larger as not all users will have had all of their credits cards compromised. In this context, it may be harder to find people not affected by the data theft than the other way round.

Unlike the cyber-attack on Target, this time the criminals didn't use a particular strain of malware to steal the information. The theft appears to be the an inside job by a KCB worker –ironically enough, working at the company's anti-fraud department– who copied this information over a period of 11 months with the intention of selling to the highest bidder. The fact that the information stored by the company was not properly encrypted adds to the severity of the data breach. And the fact that an employee was able to steal information for more than 11 months also speaks volumes about the lack of proper supervision and access control mechanisms.

Nearly half the people in South Korea had their bank details stolen by a KCB worker.

There are a number of security measures that could have been implemented to prevent a situation like that, despite the fact that the thief in this case was a member of the company's anti-fraud department, and as such had access to sensitive information. What could have been done to prevent it? Well, as previously said, data encryption can be useful in situations like this, even though the attacker in this case may very well have had access to the data needed to decrypt the information.

Also, limiting the amount of information that can be accessed at a time can reduce the damage done by this type of data breach: If the attacker had been able to only access a limited number of records in the database –let's say, 10 records for example- he would have had to repeat the same operation more than 10 million times to achieve the same result.

And not only that, you can also limit the amount of data that can be accessed over a period of time, and better still: You can set alerts linked to a series of complex rules that trigger whenever some unusual activity takes place. This is something most financial institutions have already implemented, allowing them to detect cyber-fraud and data theft.

The first quarter of 2014 also also saw other, less notorious data theft attacks. For example, in Germany, the Federal Office for Information Security (BSI) released a statement saying that around 16 million email accounts had been stolen. In this case the criminals used a botnet to perpetrate the attack, which means that most probably the victims' computers had become part of a computer network controlled by the hackers.

Germany's Federal Office for Information Security revealed a data breach where 16 million email addresses were stolen.

The BSI created a website to help people find out whether or not their email account had been hacked. If you are among those affected, it is very likely that your computer is infected with malware. In that case, we advise that you use Panda Cloud Cleaner, a free tool that will allow you to scan your computer and remove malware threats.

Yahoo users were also affected by a security breach, although in this case the stolen data was not obtained directly Yahoo's servers.

Apparently, some users of Yahoo email informed the company that their user IDs and passwords had been compromised, and after further research, it was discovered that the information had been obtained from a third-party database.

In response to the attack, Yahoo reset the victims' passwords and used two-factor authentication to let users re-secure their accounts.

Unlike the Yahoo incident, an attack launched on Orange did affect one of the company's websites. More specifically, the breached site was affected by a vulnerability that allowed the attackers to gain access to personal data from hundreds of thousands of customers, including names, mailing addresses and phone numbers.

Orange confirmed hackers stole 800,000 customer records.

Fortunately, it seems that Orange's systems were configured in a way that prevented the customers' passwords from being compromised, which limited the damage done to the more than 800,000 users affected by the attack.

According to reports, the customers' passwords were stored on a separate server which was not impacted by the breach.

In any event, when it comes to protecting passwords from the eventuality of theft, the best policy is simply not to store them. If passwords are not stored, they can't be stolen, can they? It sounds quite obvious, but not many companies seem to apply this simple concept.

Germany's Federal Office for Information Security revealed a data breach where 16 million email addresses were stolen.

Now, the question is, if organizations don't store users' passwords, how can they validate users? Very simple. It would be enough to 'salt' the original password set by the user when signing up for a Web service, and apply a hash function to that 'salted' password. By salting the original password, what you actually do is generate a new, different password using a previously defined pattern (turn letters into numbers, change their order, etc).

Next, the system applies the hash function to the alternate password and converts it into a complex string of symbols by means of an encryption algorithm. It is this 'hashed' form of the password which is stored in order to validate the user.

From that moment on, every time the user types in a password, the system will apply the aforementioned pattern to it, calculate a hash value, and compare it to the hash stored in the password database.

If they match, it means that the user has entered the correct password and access is permitted. As you can see, the entire process takes place without the need to store sensitive data such as passwords.

Another measure that should be implemented on a massive scale is the use of two factor authentication. Even though it can be a pain at times, when applied, it makes compromising user accounts a lot more difficult. This is a system that financial institutions have been using for a long time, and which should also extend to other Web services as well.

The Syrian Electronic Army defaced Forbes' website, stealing more than 1 million user accounts.

The hacker collective known as the Syrian Electronic Army (SEA) managed to hack into Forbes' website, successfully stealing details from more than 1 million user accounts, including those of hundreds of the company's employees.

The stolen information included user names and email addresses as well as passwords (in encrypted form). To make things even worse, the SEA published this data online.

Cryptolocker, the notorious and dangerous ransomware that encrypts victims' files until a ransom is paid, struck again. One of its many victims was Goodson's law firm in North Carolina (USA), which admitted that every legal file on one of its main servers had fallen prey to the malware.

Incidents like this highlight once again the importance of backup policies in business environments, as the damage done by data breaches such as this would be clearly mitigated with a backup copy that allowed organizations to restore their information easily.

Cryptolocker continued to create havoc.

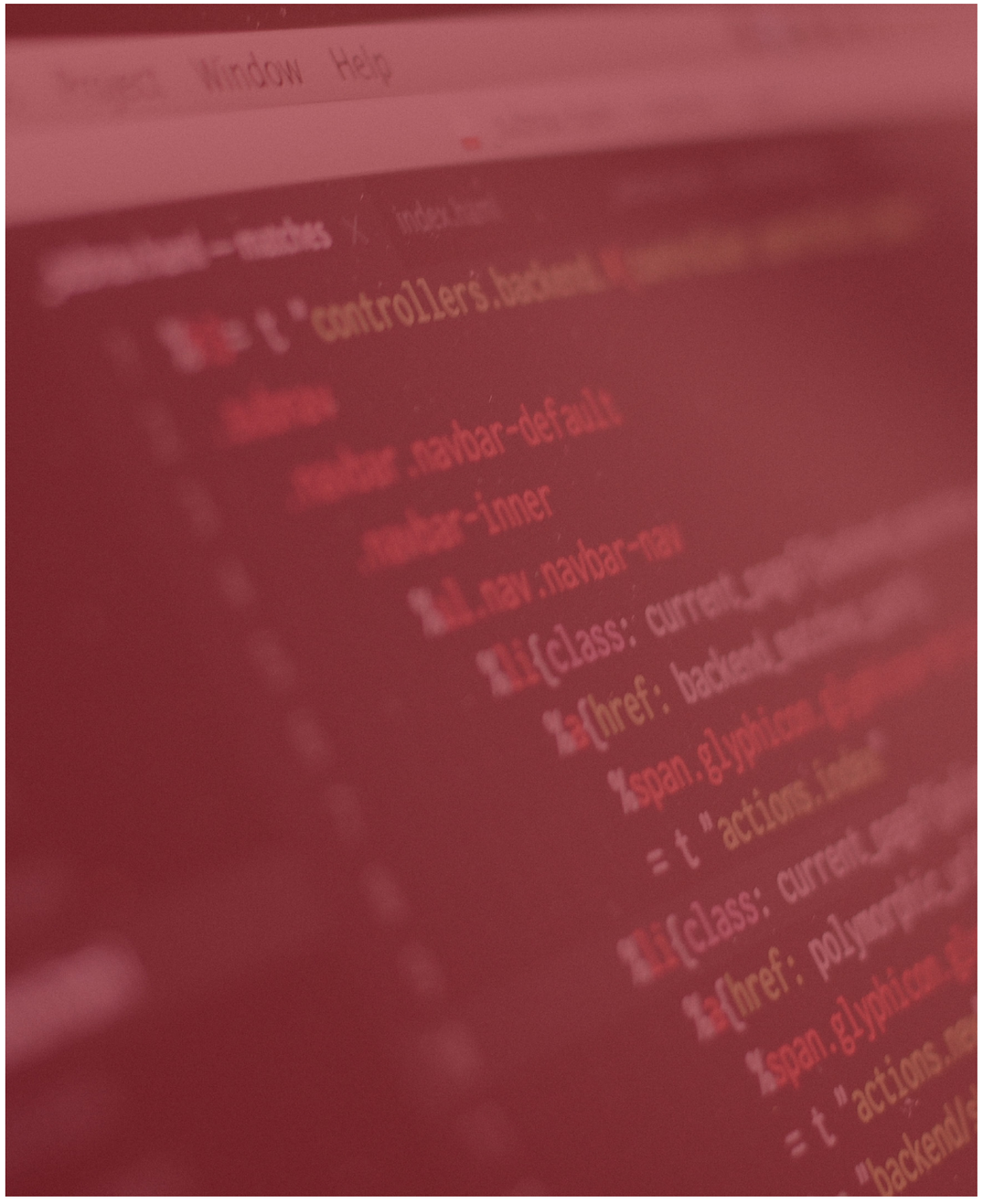
Its many victims included a law firm in North Carolina whose entire cache of legal files was encrypted by the malware.

When talking about cyber-attacks we normally think of computers, smartphones and tablets. However, other hardware devices can be affected as well.

A security flaw in Linksys routers could allow an attacker to perform actions such as changing the router's DNS settings -something quite usual in phishing attacks that redirect users to fake websites Banking Trojans are one of the most prevalent threats today. They are designed to gain access to victims' bank accounts and empty them, which makes them particularly dangerous and one of cyber-criminals' preferred weapons.

In January, the U.S. Department of Justice announced that Russian national Aleksandr Panin had pleaded guilty to conspiracy to commit wire and bank fraud for his role as primary developer and distributor of one of the worst banking Trojans ever: SpyEye.

Aleksandr Panin, the alleged mastermind behind the notorious SpyEye Trojan, pleaded guilty to bank fraud.



Last April 8 was the date set by Microsoft to cease offering support for Windows XP.

In short, this means that users of this operating system will no longer receive security updates, so any new security hole discovered will not be patched. However, this coincided exactly with the appearance of a serious security hole affecting Internet Explorer and which could allow an attacker to infect a computer simply when the user visited a website that exploited this vulnerability.

There was widespread panic, as attacks exploiting this flaw had already been detected, which led Microsoft to publish an update for the Windows XP version of IE even though it had stopped supporting the operating system.

Most security companies, including Panda Security, have opted to continue providing support and upgrades to all customers that still use XP. Nevertheless, users are strongly advised to consider migrating to a new operating system version that offers greater security, as it is not a question of 'if' new vulnerabilities will be discovered, but 'when'. And from that moment users will be running a risk that would be avoided if they were using a later version of Windows.

Heartbleed appeared in early April, just at the same time as support for Windows XP ended.

Basically, it was a security hole in the OpenSSL library, which is used for encrypting communications. Many Internet services, such as webmail, social networks, online banking, etc. encrypt communication to protect the data exchanged (bank login credentials, passwords, etc.).

Servers using the vulnerable library were vulnerable to attack. The problem involved a module that allows open connections to be reused (called 'keep alive'), enabling up to 64 KB of memory on the compromised system to be repeatedly available to an attacker. However, it wasn't a complete disaster, as at least attackers weren't able to choose which part of the memory they had access to, and also a library was released to fix this bug.

Some days later, a 19-year-old Canadian student was arrested for exploiting Heartbleed to steal the data of 900 Canadians from the country's tax office. The Canada Revenue Agency had blocked public access to their online tax service a day after the security flaw had been discovered and made public, yet they did not manage to prevent this attack.

One of the biggest and most controversial attacks during this second quarter involved eBay. The online auction company asked all its users to change their passwords as a result of a cyber-attack.

The attackers managed to obtain the credentials of eBay employees and used them to access the company's network.

They access to the database containing customer names, encrypted passwords, email addresses, postal addresses, phone numbers and dates of birth.

The controversy however was not due to the attack itself, rather how the company communicated it. At first it seemed that eBay was downplaying the attack, and the incident was not even mentioned visibly on its website.

Yet given the seriousness of events, the company was left with no choice but to change tack and release a highly visible notice on its home page asking all users to change their passwords.

PandaLabs detected that cyber-criminals, taking advantage of this incident, are sending phishing emails purporting to be from eBay notifying users of the security problem and providing a (malicious) link for them to change their passwords.

If users follow this link and enter their details, they will be handing over their eBay credentials to cyber-criminals.

Spotify, was also the victim of an attack that compromised its corporate network.

The interesting thing about this incident however was that it only targeted a single user, something really quite unusual. It either could have been an attack aimed at obtaining information from a single user or an attempt by cyber-criminals to see how far they could get.

The Reuters website was attacked by the Syrian Electronic Army.

In this case it wasn't a Reuters' security problem that led to the attack, instead the victim of the attack -and the route of entry for the hackers- was a service provider used by the company.

The Domino's Pizza fast-food chain was also targeted by a group called Rex Mundi.

Who stole the data of 650,000 customers in France and Belgium, and then asked for a ransom for the information. Company officials however said they refuse to give in to blackmail.

Hector Xavier Monsegur, alias Sabu, was arrested by the FBI on June 7, 2011. Many of you will remember him as one of the leaders of Anonymous and Lulzsec. Sabu pleaded guilty to a series of offences and is now facing up to 124 years in jail. Since his arrest however, he has been working with the FBI helping to collect evidence leading to the arrest of other cyber-criminals.

With the help of Sabu they have prevented some 300 cyber-attacks over a period of three years.

After his arrest he spent seven months in prison and is now awaiting sentence. In May this year Sabu was finally released, having repaid his debt to society thanks to the help he has offered security forces.

The second quarter had also witnessed one of the heaviest sentences handed out to a hacker. David Ray Camez, one of the ringleaders of a page which traded in stolen credit cards was sentenced to 20 years in prison and ordered to pay $20 million in damages.

A huge worldwide police operation, headed by the FBI, neutralized the Blacksades group.

This group used a RAT (Remote Access Tool) -of the same name as the group- to carry out a series of crimes related with stolen user credentials. This was one of the biggest security operations in history against these types of criminals.

Another major action against cybercrime, once again featuring the FBI, was the bringing down of the GameOver Zeus botnet.

These are a family of malware that used P2P communication, which made it really difficult to combat as it didn't rely on servers that could be neutralized.

Moreover, the FBI has now pressed charges against the person who controlled the botnet, Russian citizen Evgeniy Mikhailovich Bogachev. Bogachev, who is now on the Bureau's 'most wanted' list has also been accused of infecting systems with CryptoLocker.

iCloud was at the center of the much discussed #celebgate scandal. This hacking attack leaked private photos of more than 100 actresses and models to the Internet.

One of the best ways to mitigate hacking risks is to use two-factor authentication. Most major online service companies (Facebook, Google, Microsoft, etc.) already have it, and Apple, which already utilized two-factor authentication in its iCloud services, extended the feature to its iCloud.com Web app suite, providing users who access their iCloud accounts from their iPhones or iPads with an extra layer of security.

iCloud was at the center of the much-discussed #celebgate scandal. This hacking attack leaked private photos of more than 100 actresses and models to the Internet.

Actresses such as Jennifer Lawrence, Kirsten Dunst or Kate Upton were among the victims of the mass photo hack, and the stolen images were obtained via the online storage offered by Apple's iCloud platform.

Initially it was thought that the leaks could be due to a potential security hole in iCloud, but Apple announced that, after a 40-hour investigation, they had discovered that the accounts of these celebrities "were compromised by an attack on the very specific user names, passwords, and security questions," adding that these attacks have "become all too common on the Internet." Obviously, the culprits of this type of hack are always the attackers who steal the victims' photos, however, there are also lessons to be learned:

› Never upload images that you don't want to share.

› Enable two-factor authentication in your online accounts.

A Russian hacker group that goes by the name of w0rm attacked technology news website CNET and stole user names, emails and encrypted passwords of over a million users. This is the same gang that claimed responsibility for hacking the BBC, Adobe and Bank of America websites in the past.

The third quarter of the year saw massive data thefts at major companies and institutions around the world.

Community Health Systems, one of the biggest U.S. hospital groups, announced that its computer network had been the target of a cyber-attack which saw the compromise of patient identification data for 4.5 million individuals.

In August, grocery store chain Supervalu announced that attackers had managed to compromise customer data at 180 of its stores around the country. Additionally, UPS acknowledged that credit and debit card information belonging to customers who did business at 51 of its offices had been compromised as the result of an intrusion into the company's networks.

U.S. bank JP Morgan Chase fell victim to a similar data breach. Hackers launched targeted attack at specific JP Morgan Chase employees to gain access to their computers, and from there to the bank databases.

The attackers modified and deleted some of the bank records yet the motive for these actions is unknown. Both the FBI and the Secret Service are investigating the case.

Home Depot was the victim of one of the largest attacks recorded. The home improvement retailer confirmed that its servers had been attacked and that 56 million credit and debit card details had been compromised. According to The Wall Street Journal, the company also acknowledged that, in some cases, the accounts associated to the cards were drained.

In addition, fraudulent transactions appeared across the USA as the criminals used the stolen card details to buy prepaid cards, electronic goods and even groceries.

This attack came just months after a similar attack on Target Corp., and there could be a connection, as the same tool – BlackPOS– was used to carry out the hack. It appears that the security breach may have affected customers who shopped in any of the almost 4,000 stores that the company has in the U.S. and Canada between April and September.

The news of a potential hack attack on Google hit the headlines after a list of almost five million Gmail user names and passwords was leaked online.

In a statement sent to the media, Google said it had no evidence that its systems had been compromised, adding that whenever they become aware that accounts may have been compromised, they take steps to help users secure their accounts.

Google said that 98% of the passwords did not work, and the leaked data seems to have been accumulated through phishing and other hacking attacks on users.

A security hole was discovered in Bash that jeopardized the security of Linux and Mac users.

This vulnerability, dubbed 'Shellshock', affected the command interpreter in these operating systems.

This flaw could allow a cyber-criminal to remotely access a system using Bash and insert spyware designed to steal confidential information or even take control of the system.

The affected systems include Mac OS X computers, many Web servers, and some home networking devices like routers.

The U.S. Postal Service suffered a data breach that compromised the personal information of 800,000 employees, which was rather surprising considering that the company only has half a million workers. It seems that the hacked server hosted data belonging to the company's current and former employees.

At the end of November, Sony employees were met with the nasty surprise of not being able to boot their computers.

At the end of November, Sony employees were met with the nasty surprise of not being able to boot their computers. A malware attack was deleting the contents of their hard drives. However, this was just the tip of the iceberg.

A group calling themselves the Guardians of Peace took responsibility for the attack, claiming to have stolen over 100TB of data from Sony. Shortly after, they started leaking personal information of the company's employees and their families, as well as email messages, salaries, copies of unreleased films, etc.

There was much speculation as to who was responsible for the hack, with the FBI pointing to North Korea as the perpetrator.

A few days after the attack, malware strains were detected with valid digital signatures stolen from Sony.

One of the last major attacks of 2014 affected Microsoft's Xbox Live and Sony's PlayStation Network.

These services were down for most of Christmas, probably the time of the year when they are more in demand, due to a string of denial-of-service attacks that prevented users from accessing the gaming platforms of these two industry giants.

However, what really caught our attention was the fact that the DDoS attack was not perpetrated using infected computers, as is often the case, but compromised routers.

Social Networks

The world was shocked with the recent mysterious disappearance of Malaysia Airlines flight MH370. Shortly after the news about the missing plane broke, cyber-criminals started preying on people's morbid curiosity through fake Facebook postings promoting a video of the plane. However, when users tried to watch the video, they were asked to enter their user names and passwords, compromising their accounts. Shortly after, the attackers carried out the same strategy on Twitter.

Cyber-criminals exploited the disappearance of Malaysia Airlines flight MH370 to launch attacks via Facebook and Twitter As well as on social networks, PandaLabs detected a malicious email message exploiting the same subject matter.

The message claimed to contain a transcript of the conversations held between the pilots and the control tower in the final minutes before ground controllers lost contact with the aircraft. The malware was attached to an executable file with a PDF icon to trick users into running it. Once run, the file infected the computer with a Trojan while at the same time opening a document with the supposed transcript so as not to raise suspicion.

The Syrian Electronic Army, already mentioned in this report, was particularly active in the social media arena, compromising the accounts of major companies worldwide.

Its victims included Microsoft, whose @XboxSupport and Microsoft News (@MSFTNews) Twitter accounts were hacked. However, these were not the only attacks suffered by the Redmond company. On January 1, Microsoft's Skype had their Twitter and Facebook accounts hacked by the same group.

Syrian Electronic Army compromised the Twitter and Facebook accounts of several organizations and attempted to gain control of the facebook.com domain in an attack stopped by MarkMonitor.

Unfortunately, these were not the only attacks perpetrated by the SEA. Actually, they tried to hijack the entire Facebook domain. They were able to gain access to an administrator panel at DNS provider MarkMonitor, but fortunately enough the hack was detected as it was taking place and MarkMonitor was able to regain control of the domain before the SEA was able to modify the Facebook.com DNS records.

The Syrian Electronic Army hijacked four Wall Street Journal (WSJ) Twitter accounts.

The accounts were those of WSJ Africa (@wsjafrica), WSJ Europe (@wsjeurope), WSJ Vintage (@vsjvintage), and WSJ.D (@wsjd). WSJ rapidly discovered the incident and deleted tweets published by the attackers.

The Twitter account for British Gas customer support was also hijacked. In this case the hackers started releasing tweets with links that took users to a replica of the Twitter page asking users to enter their login credentials.

If they entered them, they would be handing over their details to the cyber-criminals who could then access and use their accounts.

June 12 marked the opening of the World Cup finals in Brazil. A cyber-criminal took advantage of the opportunity to try to steal the Facebook credentials of players of Top Eleven: Be a Football Manager, one of the most popular fantasy football games, with over 10 million followers on Facebook.

The attacker used Windows malware disguised as an application. Supposedly, having downloaded the application users could earn tokens for Football Manager that can be used to buy players.

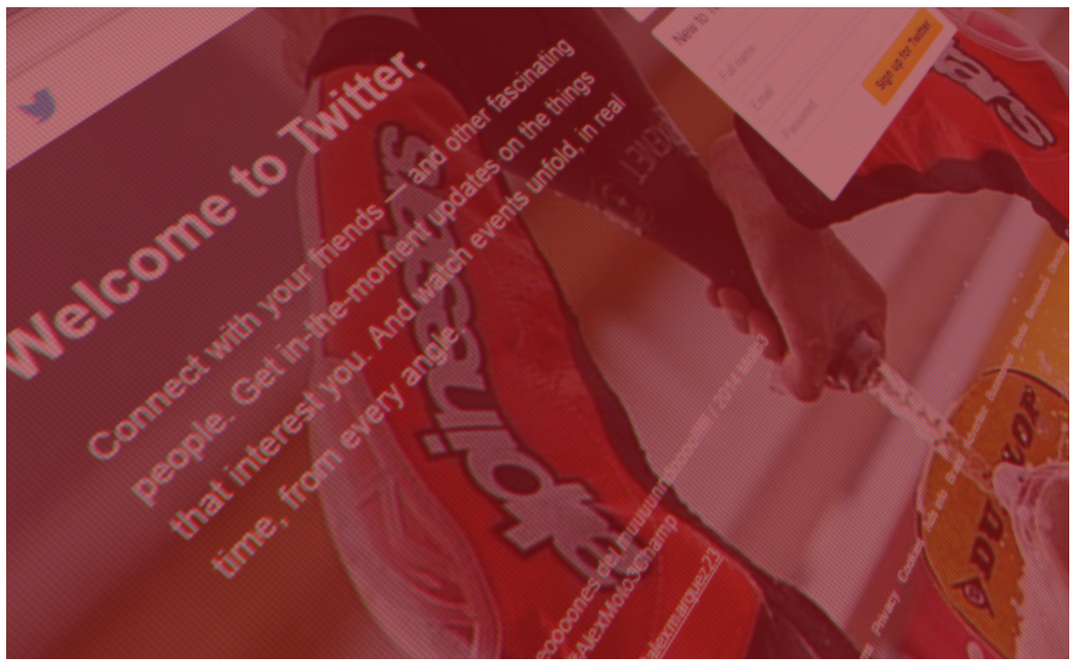
Obviously, this wasn't really the case, and those who followed the instructions in the application, apart from not earning tokens, would also risk losing access to their email or Facebook accounts.

Twitter joins the group of companies that reward the efforts of those users who dedicate to uncover security holes in their programs or platforms.

In the technology world, it is now quite common for companies to reward the efforts of those advanced users who dedicate some of their time to uncovering security holes in their programs or platforms.

Although there are still some who are yet to be convinced of the effectiveness of such 'bounty programs', many firms apparently see them as being extremely useful, not just to discover new bugs that have gone undetected, but also to get these expert users on their side. Twitter was still among those that had yet to take up the idea. The 140-character social network seemed reluctant to put its hand in its pocket to encourage experts to find bugs in its service.

Nevertheless, now the company has announced that it is offering a minimum reward of $140 for those who find security holes in Twitter.com, ads.twitter, mobile Twitter, TweetDeck, apps.twitter, as well as in the apps for iOS and Android. This sum is still way off what others are offering. Bounty programs at firms like Facebook or Google reward users that uncover vulnerabilities with amounts upwards of $500 and $1,000 respectively.



Mobile malware

In February, PandaLabs identified a number of malware apps on Google Play. Four apps (on subjects such as diet plans, hairstyles, workout routines and recipes) on the Google Play store were identified as subscribing users to a premium SMS service. Not only this, the SMS messages received were then hidden so that the victim was unaware that anything was wrong until they saw their phone bill.

PandaLabs identified four malicious apps on Google Play with somewhere between 300,000 and 1,200,000 downloads in a little bit more than one month.

A few weeks later, PandaLabs detected a similar attack, although this time, instead of using Google Play, cyber-crooks created a fake Web page designed to look like it, and spread the malware through malicious ads on Facebook. When we talk about security incidents affecting smartphones we normally talk about Android, as it is the most popular operating system. This quarter however we saw several notable attacks on the Apple operating system, iOS.

In April, a malware campaign was uncovered that targeted jailbroken iPhones/iPads.

It means, those ones that have been modified by their owners to install applications on them without having to go through the official App Store. The malware, apparently from China, is designed to steal user credentials.

Another case featuring Apple's mobile devices took place in Australia. An Australian newspaper reported that some of the country's Apple users had discovered that their devices had been hijacked, although it's not clear how many users were affected.

The story revealed that a number of users discovered a message asking them for $100 in exchange for handing back control of their devices.

YIt would appear that cyber-criminals had somehow managed to get hold of the Apple credentials of these users, and had impersonated them to remotely lock the devices using the Find my iPhone option which can locate and lock lost or stolen phones. The hackers would only send the new password needed to unlock the phone once the ransom was paid. What seems most likely is that cyber-criminals have hacked the database of the Apple fan forum, and, having stolen login credentials for the forum, have tried to see whether users had the same password for iCloud services. If the passwords matched, they hijacked the device and demanded a ransom.

In the world of Android there have been all kinds of stories and attacks, though the most striking are related to fake antivirus software and ransomware.

One so far unique case was that of an app called Virus Shield, which rose to the top of the most popular apps on Google Play.

It appeared to be a paid antivirus application, costing $3.99 However, it offered no protection whatsoever, but had an interface that simulated scans and smartphone protection. It reached more than 10,000 downloads before Google removed it and reimbursed the scammed users.

This quarter we also saw a new family of Android malware emerge, called Android/Koler. This attracted coverage in the media as it was an attack similar to that of the Police Virus that previously affected Windows computers In this case however the malware cannot encrypt data. It's still quite annoying nevertheless and difficult to remove if you don't have an antivirus on your phone, as the message it displays obscures everything else, and users only have a few seconds to try to uninstall it.

While we were analyzing it in PandaLabs, we came across a new variant, identical to the first one, but which connected to a different server.

And this server was still active... In this case the cyber-criminals had made a small mistake, and had left the door ajar while configuring it.

Sadly we couldn't access all the information there (a mysql database with data on infections, payments, etc.), though we were able to download files from the server and take a look at how it operates.

The way it works on the server side is similar to the malware that targeted Windows computers: several scripts geotag the device and display a message in the local language along with localized security force images.

Information from all infected devices is saved in the database along with the MD5 of the corresponding malware. This makes it possible to track the number of infections with each variant of the malware and measure the success of different infection campaigns.

The malware is designed to attack users in 31 countries worldwide, 23 of them in Europe: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Slovakia, Spain, Sweden, Switzerland and the UK. The remaining countries where users could also be targeted are: Australia, Bolivia, Canada, Ecuador, Mexico, New Zealand, Turkey and the USA.

Another type of ransomware appeared this quarter, this time originating in Russia.

This malware really did encrypt information (images and videos) on devices and demanded a ransom to release them.

As if it wasn't enough to have malware for smartphones lurking in app stores or on any web page, there has even been a case where the malware came pre-installed. This was the case with a Chinese manufacturer, who included a data-stealing Trojan that sent information to a server in China.

Android malware has continued to grow exponentially, and 2014 is already the year in which most mobile malware strains have been put in circulation.

Android was once again the main target for mobile malware creators. Adrian Ludwig, the lead security engineer for Android at Google, said there was “a bit of misperception” in how the company review apps for its Google Play store in comparison with other stores (a not-so-subtle swipe at Apple’s iOS App Store, which has a reputation of being much more demanding in this respect). In this context, he even proclaimed that mobile antivirus was not needed on Android.

Android malware, meanwhile, has continued to grow exponentially, and 2014 is already the year in which most mobile malware strains have been put in circulation.

Additionally, new vulnerabilities have emerged that could be exploited by attackers for malicious purposes:

- CVE-2013-6272: Exists in all Android versions through 4.4.2 (KitKat). It allows applications to make unauthorized calls to premium-rate telephone numbers.
- CVE-2014-N/A: Exists in Android 2.3.3 and 2.3.6, and has the same effect as the previous one.

WireLurker is a malware specimen for iPhone/ iPad devices

This malware employs an unusual infection technique. Once it infects a computer, it waits for the user to plug an iOS device into their Mac’s USB port. Once that happens, WireLurker seeks out three popular apps, uninstalls the legitimate version of those apps and replaces them with malicious ones without the victim’s knowledge or consent.

Cyber-War

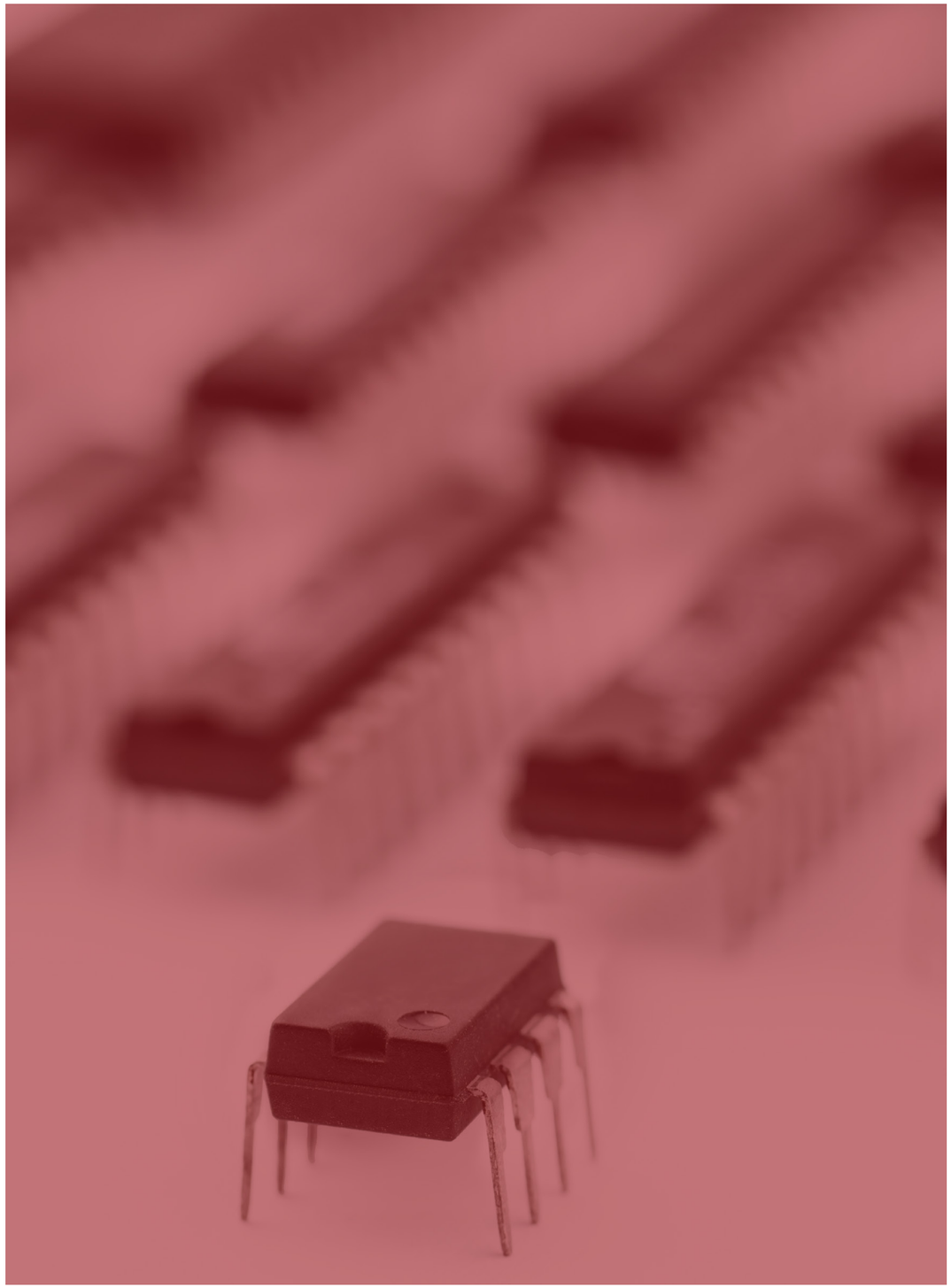
In the cyber-war arena, new revelations continued to surface about the cyber-espionage activities carried out by the NSA and uncovered by Edward Snowden. New reports revealed the collaboration between the NSA and the British intelligence agency GCH Q (Government Communications Headquarters).

One of the most controversial cases has to do to do with the “Optic Nerve” program, which accessed and collected webcam images from Yahoo users around the world. Although it’s impossible to know the precise number of people that were spied on, it is estimated that in just six months, the webcams of more than 1.8 million users were hacked.

The NSA and GCHQ intercepted the webcam images of millions of Internet users through the “Optic Nerve” program.

Instead of capturing whole video chats, the program randomly stored an image every five minutes. It is important to bear in mind that the victims were not suspected of any crimes. These were indiscriminate interceptions of individual users. It is also estimated that between three and eleven percent of the documents contained images of nudity. Yahoo accused British and U.S. intelligence of taking the violation of user privacy to a “whole new level.”

In March, German newspaper Der Spiegel revealed how British intelligence agency GCHQ and US agency NSA had been spying on a number of German companies and individuals, including German Chancellor Angela Merkel.



The USA, Germany, Belgium and the UK are some of the countries that confirmed different attacks durign 2014.

One of the most interesting cases that occurred during the last quarter was in Belgium.

In March, German newspaper Der Spiegel revealed how British intelligence agency GCHQ and US agency NSA had been spying on a number of German companies and individuals, including German Chancellor Angela Merkel. One of the most interesting cases that occurred during the last quarter was in Belgium.

The Ministry of Foreign Affairs had been compromised by hackers Russia was once again suspected of being the source of the attack, though we have to reserve judgment, as the investigation is still ongoing and it may take time to find out what really happened.

In the UK, a senior government official confirmed that an attack originating from a ‘foreign power’ had been detected. The attackers managed to access the account of a system administrator of the Government Secure Intranet, although the attack was nipped in the bud and no data was stolen.

Regarding internal espionage, Charles Farr, Director General of the Office for Security and Counter-Terrorism has said that communications over social networks or foreign search engines are understood by the British Government as being “external”, meaning they don’t need a court order to obtain access to information or communications across Google, Twitter or Facebook.

Such statements, along with all the recent scandal regarding the NSA is leading to a change in the way users behave. In fact, according to a recent study, there is now more than twice the amount of encrypted traffic circulating on the Internet than there was before these massive espionage cases were leaked. And this is not the only consequence, the German Government has canceled a contract with US company Verizon, as part of its reshaping of internal communications, after revelations of spying by the US government, who had even tapped the phone of Chancellor Angela Merkel.

In July, U.S. newspaper The New York Times revealed that alleged Chinese hackers gained access to some of the databases managed by the Office of Personnel Management to house the personal information of the federal employees who apply for top-secret security clearances. The U.S. Government acknowledged the attack but denied the possibility that any classified information had been compromised. Despite the attackers were tracked back to China, there is no conclusive proof that they were working on behalf of the Chinese government.

In the cyber-espionage arena, new top-secret documents from the NSA and the British agency GHCQ revealed the existence of "Treasure Map", a secret operation aimed at mapping the entire Internet, including end-user devices.

The documents leaked by former intelligence service employee Edward Snowden revealed how the NSA and its intelligence partners had illegally penetrated the internal networks of different companies. One of these companies is German firm Deutsche Telecomm which, after been alerted to the possibility of this attack by German magazine Der Spiegel, scanned its network without being able to find any evidence of intrusion.

Other classified documents revealed by Snowden showed how British intelligence agency GHCQ had the ability to actively monitor Skype users in real time without their knowledge. In August, a hacker claimed to have stolen 40 GB of internal documentation from Gamma International (http://en.wikipedia.org/wiki/FinFisher), a German-UK technology company that develops spying software for governments and police agencies around the world. The attacker created a Twitter account (@GammaGroupPR) through which he began posting links to the stolen documentation.

CVE-2014-4114 is the identifier of a vulnerability discovered last October by security consultants iSIGHT Partners. This flaw affects the most recent versions of Windows and could have been used in a Russian cyber-espionage campaign called 'Sandworm'. This campaign targeted institutions such as NATO, European telecom companies, U.S. universities, and the Ukrainian government.

This security hole allows an attacker to remotely run code if they can convince a victim to open a specially crafted PowerPoint file via social engineering methods. According to iSIGHT, the vulnerability exists because Windows allows the "OLE packager" (packager.dll) to download and run INF files, which in this case could contain malicious commands.

This vulnerability affects all versions of the Windows operating system, from Windows Vista (Service Pack 2) to Windows 8.1, as well as Windows Server versions 2008 and 2012.

Microsoft's Security Bulletin MS14-060 includes a security update that resolves this vulnerability:

https://technet.microsoft.com/library/security/ms14-060

4. 2015 SECURITY TRENDS

2015 Security Trends

Cryptolocker

This type of malware has been in the spotlight in 2014, and these attacks are set to increase in 2015.

The functioning is quite straightforward: once it gets into a computer, it encrypts all types of documents that could be valuable to the user (spreadsheets, documents, databases, photos, etc.) and blackmails the victim into paying a ransom to recover the files.

Payment is always demanded in bitcoins, so that it cannot be traced by the police, making this type of attack very attractive to cyber-criminals, as many users decide to pay in order to recover the hijacked information.

APT

APTs (Advanced Persistent Threats) are a type of targeted attack aimed at companies or institutions. Behind these attacks are usually countries that invest huge sums of money in ensuring that the target attack goes undetected for a long time.

They are the virtual version of James Bond. Although we will not see mass APT attacks in 2015, new cases will be discovered that will have probably been around for years but will only just start coming to light.

Targeted Attacks

Although the majority of malware attacks are within the millions of malware samples that appear every month, a small percentage of these are created to attack previously defined targets. These attacks known as targeted attacks are getting more common and will be very significant during 2015.

One of the greatest risks to tackle is that many companies do not think that they could be the target of targeted attacks, and therefore do not have appropriate measures for detecting them and stopping them, or at least for detecting any anomaly and mitigating any damage as soon as possible.

Smartphones

Smartphone attacks, or more specifically cell phones running Android, are going to reach new heights. Not only will the attacks increase but so will their complexity, with a single goal: to steal login details.

We store a growing amount of data on our smartphones and cyber-criminals are going to try to get it at any cost.

Although malware on cell phones was somewhat anecdotal a couple of years ago, more malware samples for Android have appeared in 2014 than all of the malware targeting any mobile device ever.

It seems that in 2015 growth will skyrocket, the number of victims also increasing, and therefore it will be essential to use antivirus products for these devices.

Internet Of Things

The number of Internet-enabled devices is increasing dramatically, and we are not just referring to computers or cell phones but other devices.

From IP cameras to printers, all of these "new" devices that form part of the Internet share a feature that makes them very vulnerable to becoming a target for cyber-criminals: they are devices that users do not pay much attention to and therefore, they are rarely updated, for example.

As a result, as soon as a security flaw is found in the software on any one of these, compromising the device will be child's play for any cyber-criminal. To make matters even worse, these devices are connected to internal networks, home or corporate, making them ideal entry points for carrying out all types of wide-scale attacks.

Point-Of-Sale Terminals

During the year, attacks on POS terminals, used by all stores to take their customers' payment, have increased.

Cyber-criminals are effectively attacking these environments, allowing them to steal the credit card details of the customers of these stores. As a result, an activity that users did not think of as a risk, such as paying at a supermarket, gas station, clothes store, etc., is starting to pose a potential threat to which hundreds of millions of people around the world have already fallen victim.

5. CONCLUSION

Conclusion

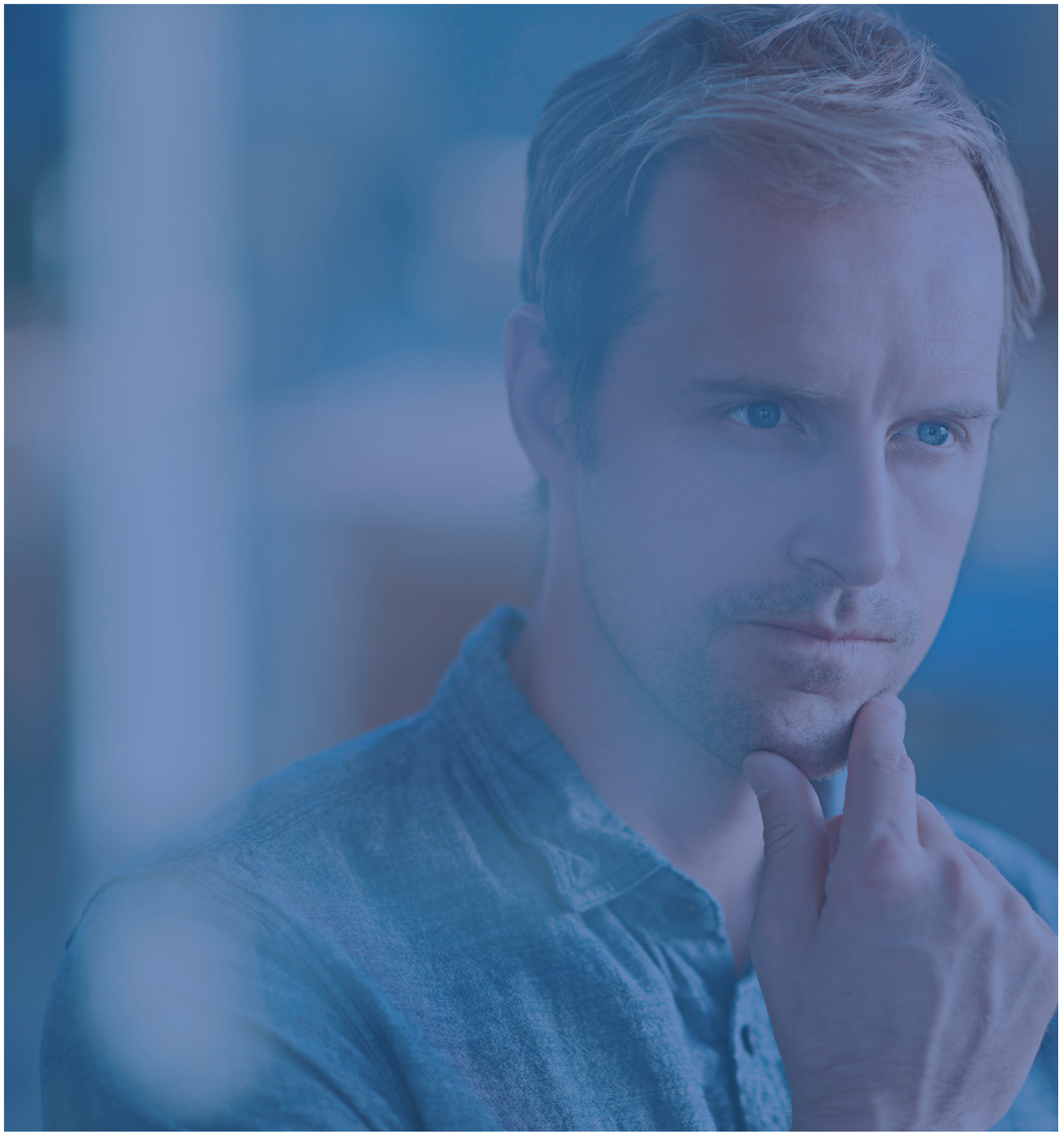
We live in an Internet-connected world, and as such we are exposed to cyber-attacks now more than ever before.

As risks increase and cyber-criminals are more active than ever, anticipating cyber-attacks is key to staying ahead of danger.

Companies must take an active, not passive stance. They cannot simply wait to be notified of data breaches on their own networks by a third party months or even years after they actually occurred. Companies must take responsibility and learn to monitor and control their own IT networks to stop computer security threats.

We hope you have found this report useful and informative, and we'll keep you updated on our activity via our next reports and our blog:

http://www.pandasecurity.com/mediacenter/



6. ABOUT PANDALABS

About PandaLabs

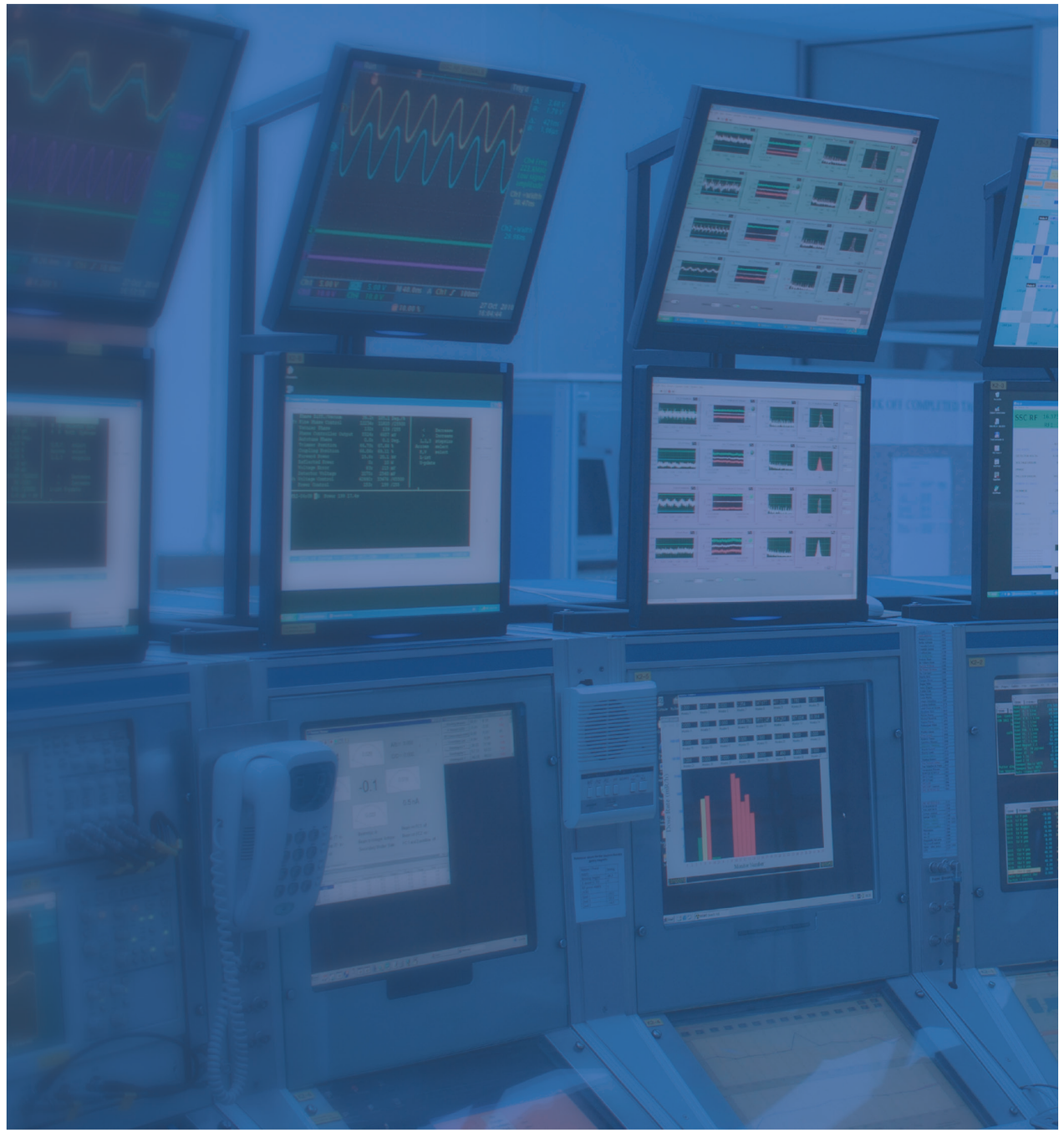
PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

PandaLabs creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.

PandaLabs is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.

Likewise, PandaLabs maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security.

Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.

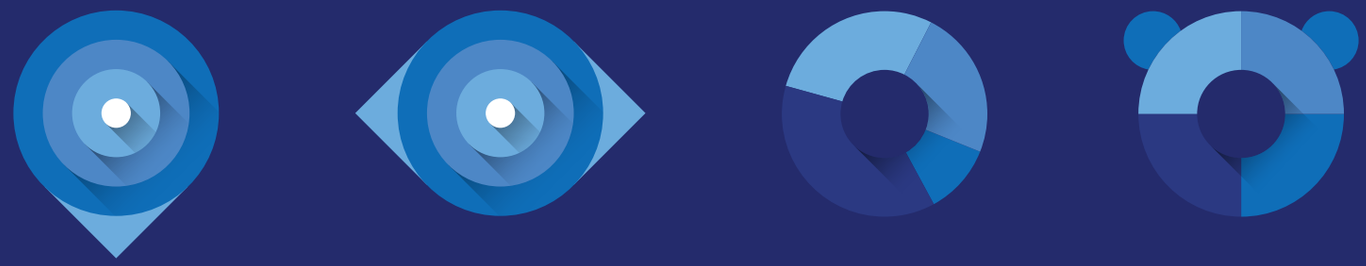


panda

pandalabs

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Panda Security.

© Panda Security 2015. All Rights Reserved.



panda

pandalabs