PANDALABS' ANNUAL REPORT 2015

panda

pandalabs

1. INTRODUCTION

1

Introduction

Last year saw one main protagonist in the world of cyber security. On the one hand, the number of malware created broke records, with more than 84 million new variants, while we saw that large businesses and websites of all types were attacked or had their clients' data stolen. This lead to millions of users across the world being affected by cybercrime.

Hotel chains get a special mention as they became a prime target for criminals, owing to the huge amount of information that they manage, such as credit card details.

Cryptolocker ravaged the corporate world, and due to many victims being willing to pay for the recovery of their information, we saw a huge increase in the number of attacks against businesses.

The Internet of Things (IoT) has begun to push itself to the forefront, as you will see in this report, as it seems that the security of these devices is relatively poor. During 2015 we saw how different specialists managed to hack cars, managing to remotely control them.

It isn't all bad news, however. Private businesses and security forces in various countries are working together more and more. Slowly but surely they are putting barriers up around the cybercriminals who are lurking online, and although there still remains a lot of work to be done, the fact that their crimes no longer go unpunished is a start.

Adobe Flash, a nightmare for the security world due to all of the vulnerabilities that it has which are used to infect millions of users worldwide, appears to have its days numbered as more and more systems prohibit its use.

Google is another company that has decided to no longer support Flash (via its Chrome browser), while Amazon no longer allows ads on its website that use the format.

2. THE YEAR IN NUMBERS

2

The year in numbers

Last year was, once again, a record year for the amount of malware created.

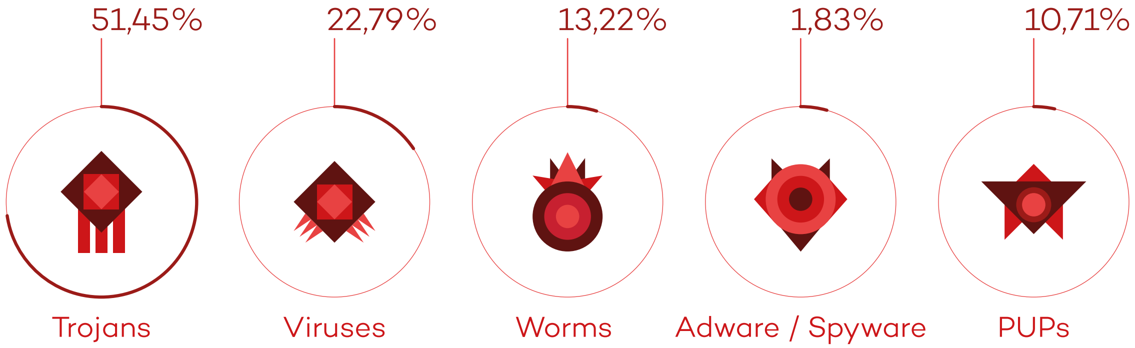
In total, more than 84 million new samples were detected and neutralized by PandaLabs, with an average of 230,000 samples daily.

We currently have 304 million samples of malware registered, which means that more than one in four of all samples ever recorded were registered in 2015 (27.36%).

Apart from Trojans, which are always the main creator of malware, PUPs (Potentially Unwanted Programs) and different variants of Cryptolockers (or ransomware) were big players last year, with the latter causing mayhem worldwide by kidnapping information in return for a ransom payment.

These are the figures for the different malware created in 2015:

NEW MALWARE CREATED IN 2015 (BY TYPE)



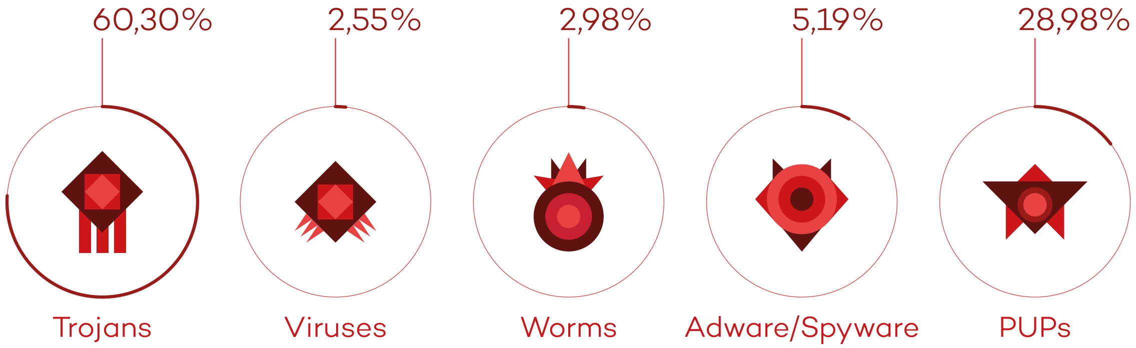
Trojans, as usual, are at the top of the list with more than 50% of the samples created during the year.

However, the figure is lower than the previous year's when compared to the rest of the categories, mainly viruses (22.79%), worms (13.22%), and PUPs (10.71%).

If we analyze infections caused by malware worldwide, thanks to the data provided by Collective Intelligence, we can see that Trojans caused the majority of infections (60.30% of all cases).

Let's take a look at how the infections are divided up:

INFECTIONS BY TYPE OF MALWARE IN 2015



We can see that PUPs are placed second, accounting for nearly a third of infections, and way ahead of Adware / Spyware (5.19%), worms (2.98%), and viruses (2.55%). Aggressive distribution techniques and software programs used by PUPs means that they achieve a high rate of installation in users' computers.

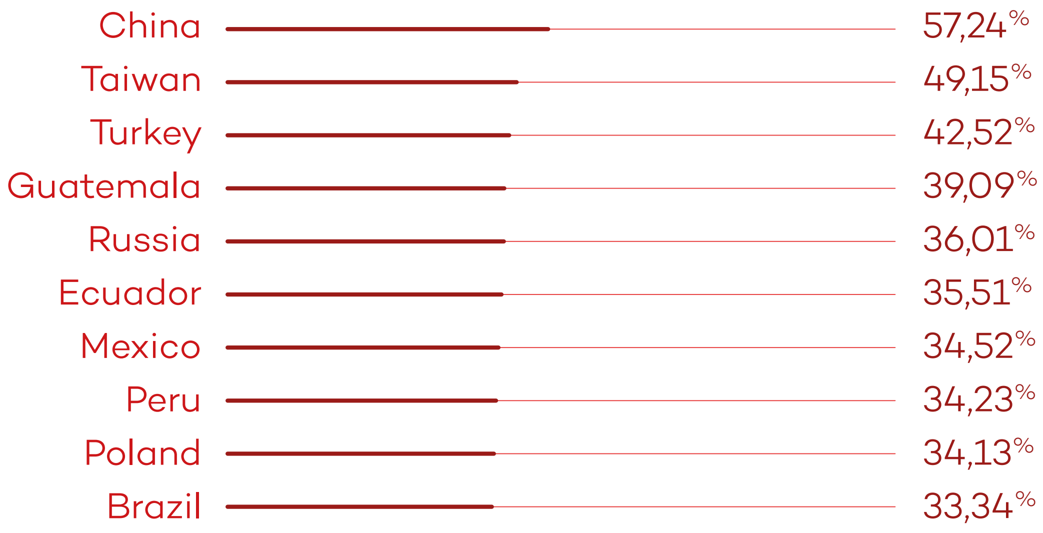
If we look at the global percentage of infected computers, which is 32.13%, we can see that it increased on the previous year, and this is mainly driven by PUPs.

We must point out, however, that this figure represents computers which have had any type of malware encounter, but doesn't necessarily mean that they became infected.

The countries with the highest infection rate are China (57.24%), Taiwan (49.15%), and Turkey (42.52%).

Below are the ten countries with the highest infection rates:

COUNTRIES WITH THE HIGHEST INFECTION RATES IN 2015

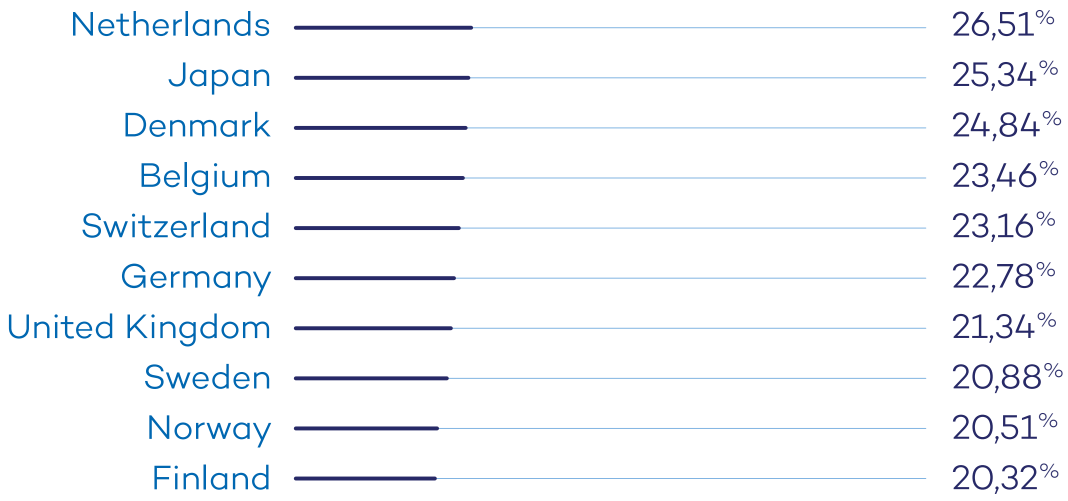


Asia and Latin America are the regions that register the highest infection rates. Other countries with an infection rate that is above the global average are Colombia (33.17%), Uruguay (32.98%), Chile (32.54%) y Spain (32.15%).

If we analyze the data of the countries with the lowest infection rates, we can see that nine of them are in Europe, with Japan being the only non-European country to feature in the top ten. The Nordic countries lead the way with Finland (20.32%), Norway (20.51%), and Sweden (20.88%) at the top of the list.

Below are the ten countries with the lowest infection rates:

COUNTRIES WITH THE LOWEST INFECTION RATES IN 2015



Other countries that registered an infection rate below the global average are Australia (26.87%), France (27.02%), Portugal (27.74%), Austria (28.96%), Canada (29.03%), United States (29.48%), Venezuela (30.11%), Hungary (30.23%), Italy (31.84%), and Costa Rica (32.10%).

3. THE YEAR AT A GLANCE

3 The year at a glance

Cybercrime

If we had to single out the most dangerous cyber-attack of Q1 2015, it would be ransomware, and CryptoLocker in particular.

This type of attack is affecting all types of users, although companies seem to be the preferred target as they store valuable information that they are ready to pay ransom money for.

It is a known fact that some companies have finally succumbed to this form of blackmail, especially those that didn't have some type of backup system in place to protect their data. In February, it was made public that a police department in Illinois had paid a $500 ransom to unlock a computer after it was infected by ransomware.

Cyber-criminals use different types of techniques to infect systems and steal user information. One of the most common infection techniques is the use of exploits, which are programs that take advantage of software vulnerabilities on the victim's computer.

In January, it was revealed that cyber-crooks were actively exploiting a flaw in Flash Player. In this case, the security hole was a zero-day vulnerability, which is a previously unknown flaw for which no patch was available.

Flash is a prime target for cyber-criminals, just like Java, another software that is often compromised by attackers. When we talk about phishing we often think of email messages purporting to come from banks and financial institutions.

Although it is true that phishing attacks can be started like that and this technique is still used on many occasions, phishers no longer target the customers of banks and online payment services solely.

One of the "new" techniques (brought back from the past, as the first such attacks occurred almost 20 years ago) used by cybercriminals to trick users and infect them with ransomware is the use of macros in Office documents (especially Word).

Most users have a false sense of security that a text document will not contain any threat. Knowing this, and being aware that the perimeter filters do not act against such files, there has been a sharp increase in the types of attacks by this method.

The weak point of this attack is that the user must enable macros, yet cybercriminals are well aware of this and have successfully developed some ingenious social engineering techniques.

One such example which was discovered by PandaLabs was a Word document containing a blurred image.

At the top of the document in bold capital letters there was a message that indicated that the image was blurred for security reasons. If the user wanted access to the information then they had to enable the macros, with an arrow pointing to the button to be pressed. Once enabled, it showed you the clear image while simultaneously infecting you with a type of Cryptolocker.

Another ransomware which has proven to be popular, especially in Australia, although it had previously been seen in other countries, was one which used images from the popular television series Breaking Bad.

In January, a hacker group launched a phishing attack impersonating Apple. The malicious message came from "Apple Support" and used a recurrent tactic: citing a supposed security problem to scare the victim: "Your Apple ID has been suspended." The message warned the user that an unauthorized person had tried to access their account, and as a result the account had been disabled. The email included a link that took the user to a page that had Apple's look and feel and requested a lot of information: full name, address, phone number, credit card data, etc.

In February, U.S company Anthem acknowledged being victim to an attack that led to the theft of data from 80 million customers. In this case, the attackers managed to access one of the company's databases using a stolen name and password. It is estimated that the attack could cost Anthem over $100 million.

In March, U.S company Slack sent a message to all of its users informing them that it had detected unauthorized access to a database storing user profile information. Although no sensitive information was stolen (in fact, Slack informed users that it was not necessary to change their login credentials), the company immediately enabled a two-factor authentication system, encouraging users to use the security feature to improve protection.

Ryanair, the low-cost airline, was the victim of an attack which saw the company lose $5 million. Despite not revealing the details on how the perpetrators carried out the attack, it is known that it arose from a transfer to a Chinese bank. The company reported the crime and announced that it had managed to freeze the stolen money and was hopeful of recouping it soon.

CareFirst BlueCross BlueShield, a medical insurer, was the victim of a cyberattack in which information was stolen from 1.1 million customers.

With each day the threat of attack from these criminals is growing, and this is merely one example of the hundreds of information thefts happening around the world.

AdultFriendFinder, an online dating service, suffered an attack which saw the theft of private user information. The attackers offered the stolen information to the first one to pay them 70 bitcoins, equivalent to $17,000 at the time. Not long after, the complete database was published online.

LastPass, a leading password management company, was another victim of information theft. Luckily it seems that the attackers didn't get sensitive password information, but only the hashes of the users' master passwords. The complexity of these hashes (jumbled up and hard to understand) makes it very difficult for attackers to get the real password. Despite this, it is recommended to change the password if the one you are using is a weak one.

The Hard Rock Hotel and Casino in Las Vegas made it known that their security had been compromised during an eight month period in which the attackers were able to steal client information such as names, credit and debit card numbers, and the CVV of the cards. Those affected were the clients who used their cards in the complex's restaurants, bars, and shops, but did not affect those who made purchases in the hotel or the casino. This attack is reminiscent of others that we have seen in the past (Target, Home Depot, UPS, Neiman Marcus) where the sales point terminals were targeted with the aim of stealing the clients' credit card information.

There were rumors that Uber had been a victim of an attack after detecting that users of the service had witnessed unusual activity in their accounts. However, it appears that this was a case of phishing, whereby the users provided their ID to the attackers after being tricked.

At the end of June, 1,400 passengers of the Polish airline LOT were stranded in Warsaw Chopin Airport after an attack on the ground system that was used to make the flight plans.

One of the biggest attacks that took place in this period was, without a doubt, the one which affected Ashley Madison. The attackers, known as Impact Team, displayed a message on their website demanding the closure of the dating agency or they would publish all of the information that they had stolen.

Not long after they published a torrent with 10GB of information as the American company failed to give in to their demands.

Among the information that was released were the private details of 37 million customers, completed transactions, email address, sexual preferences, etc. Furthermore, the release also included internal documents relating to the business.

This quarter has also seen a whole host of new vulnerabilities used by cybercriminals as a means to access their victims. Apart from the typical Flash or Java attacks, the Apple Mac OS X operating system has also seen a couple of incidents. The first of these, which was discovered by Stefan Esser, allowed for access to the root and saw Adware being used to attack Macs.

The second vulnerability was discovered by investigators at MyK. It consisted of a vulnerability in the password administration system that allowed the attacker to obtain all of the stored information.

One of the methods of attack that is quickly becoming popular consists of intercepting routers, both in homes and businesses. By doing this, the routers remain under the attacker's control.

It was brought to light that routers in businesses such as ASUS, DIGICOM, Observa Telecom, PLDT, and ZTE had predefined information in their access codes. This allows attackers to take control of them without needing to enter the premises, and we have seen examples of this where the attackers used a DDoS against Xbox Live and PSN last Christmas.

Adobe Flash, known for its numerous security issues, is facing its demise soon. iOS didn't allow for it to be run on its operating system and Android followed suit. Now it's the turn of Google to put the final nail in its coffin, by banning it from its Chrome browser. Amazon has also announced that it is banning any advertisement that is based on this format from its website.

The FBI has detained 5 individuals that were involved in the hacking that JPMorgan suffered in 2014. In this attack that managed to get the credentials of an employee, and later used these to access 90 of the company's servers to steal information belonging to 76 million individuals and 7 million businesses, all of which were clients of the company.

Microsoft has decided to improve the security of its products and solutions by doubling the reward available to investigators that are able to discover critical new errors in its solutions. The amount has increased from $50,000 to $100,000.

Although this is becoming a common feature in IT companies, it hasn't yet filtered down to all sectors, although more and more businesses are offering incentives to their investigators in the hope that they will be informed first, as opposed to them selling the information to an outside source.

In the case of United Airline, which offers air miles as a reward, they have decided to offer up to one million air miles to their investigators who discover and inform them of errors.

The FBI also offers incentives, although in this case they are aimed at those who offer information on the suspected criminals. The highest reward offered is three million dollars for anyone who can help capture Evgeniy Mikhailovich Bogachev, the mastermind behind the network of Gameover ZeuS bots.

Hotel chains are also becoming targets for cybercriminals. Apart from the attack on the Hard Rock Hotel & Casino in Las Vegas, there were others: The Hilton chain, the Starwood chain (Westin, Sheraton, etc.), Las Vegas Sands Casino, Trump Hotels, Mandarin Oriental, FireKeepers Casino and Hotel, etc. This is a long list which will no doubt continue to grow, as hotels possess the information relating to millions of credit cards. It is unusual for a hotel to not ask a guest for payment by credit card, which means that attacks aimed at the points of sale (POS) are on the increase (something that we know has worked well in the past for criminals, as shown by the case of Target where they stole the information belonging to 46 million credit cards with a malware on the point of sale).

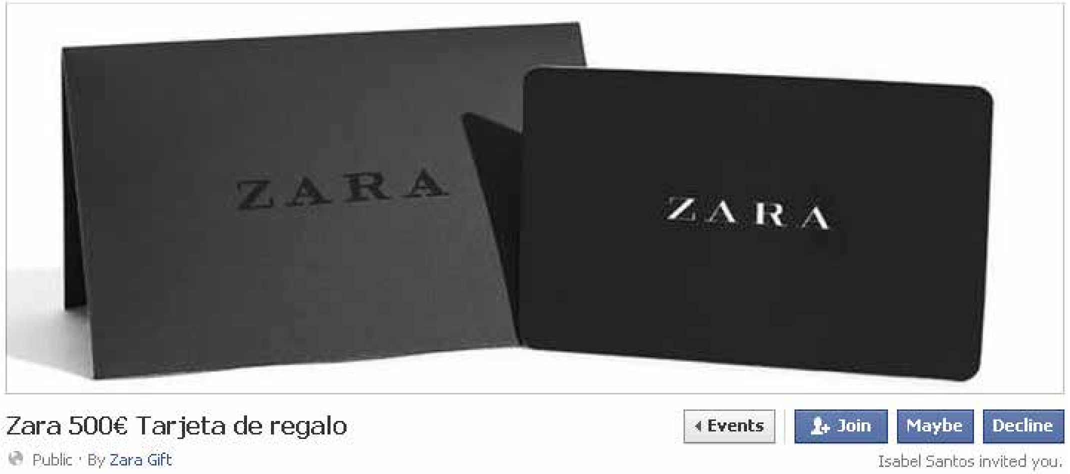
The toy company VTech also suffered a security breach which saw the data of 4.98 million parents and 6.37 million children affected. A few weeks after the attack, however, police in the UK arrested a suspect in relation to the attack.

Many businesses and websites have suffered similar attacks, such as T-Mobile, where 15 million customers had their data stolen, and sanriotown.com, which saw another 3.3 million customers have their data stolen.

Social Media

In January, at the same time that U.S. President Barack Obama announced a series of measures to combat cybercrime, a group claiming to be ISIS hacked the Pentagon's social media accounts.

On a different note, we'd like to draw attention to one of today's most common Facebook scams: bogus posts announcing giveaways of gift cards from popular companies. In January, a group of scammers created a Facebook event promising to give away 430 Zara gift cards valued at $500. To participate in the event, users simply had to join the event, write 'Thank you Zara' on their wall and invite 50 of their contacts to do so as well. The scam spread like wildfire. In just a few hours over 5,000 people had joined the event, and more than 124,000 invites had been sent out.


Zara 500€ Tarjeta de regalo

Public · By Zara Gift

Isabel Santos invited you.

All user connections to the servers of Facebook, including messages sent and received, are transmitted via secure HTTPS protocol. If this wasn't enough, the social media giant established a service on the Tor network so that users can be further assured of their online privacy. However, apart from the connections established by users via its own service, there are other indirect forms of communication carried out on Facebook by mail. They are the notifications that you receive when a friend sends you a private message (unless you have deactivated the feature).

Due to the security of these messages being at risk, Facebook has announced that from now on, all users will receive them – if they choose – protected by the popular encoding software Pretty Good Privacy (PGP).

PGP hides the mails from potential intruders with a system based on a public key (which the message sender must have) and a private key (which only the receiver must have).

The configuration process is easy – access your profile, enter into the part named "Information" and go to "Contact and Basic Information", where you will be able to enter your public PGP key (if you don't know what it is or how to get it, you can read the tutorial). It will then be visible on your profile, available for anyone who wants to send you a coded mail.

Underneath the chart there is a box that you will have to tick if you want all of the mails that Facebook sends you to be included in this new security measure. It is important to remember the key that you use to protect your mail with PGP. If you forget it, you won't be able to read your notifications and you may even lose access to your account on the social network.

WhatsApp is a popular way to attract and try to infect users. We have discovered a hoax, in which they try to trick users of the instant messaging application, called WhatsApp Trendy Blue. It passes itself off as a "new version" of the application with extra features when, in reality, the only thing it does is sign the user up to an expensive billing service.

This fraudulent program also asks you to invite at least 10 of your contacts to sign up for its services.

Facebook announced that it was looking into creating an "Unlike" button, and as expected, cybercriminals were the first ones to give us this option. In just a few hours there were a multitude of different scams featuring the supposed new button, each one looking to steal confidential information from the victims.

Mobiles

We began the year with a threat that reminded us of old-time email and instant messaging worms, conveniently modernized to make use of SMS messages.

The attack begins when the victim receives an SMS message with a link to a supposed picture of themselves. The problem with the link is that it actually downloads an APK (Android application package) file. If the victim installs it, the malicious app sends an SMS message just like the one received to all of the victim's contacts.

Fujitsu, in collaboration with the Japanese operator NTT Docomo, has launched Arrows NX F-04G, which is based on Android and is the first Android mobile to include an iris scanner as part of its security features. This is a measure that is a lot more secure than the fingerprint method that is popular with its rivals such as Apple's iPhone 6 or Samsung's Galaxy S6.

In June we detected a phishing campaign that was directed at Android developers who published their creations on Google Play, the official app store of the operating system. The message was sent from an entity named "Play Developer Support" and was titled "Update Your Account Information". Once the link was clicked, you were directed to a webpage that looks like Google, where they would ask you for your details.

Phishing attacks are designed to steal the user's identity and personal details, this is why attacks aimed at financial entities and any type of payment platform are so popular.

This case, however, is different because they weren't looking to empty the victim's bank account, but rather use their details to spread malware via the Google Play store.

The most worrying aspect of all this is how easy it would be for the criminals to automate the whole process.

All they need to do is the following:

- Create a spider or crawler (there are various open source projects available to help them with this) in order to download information in all of the apps published on Google Play.
- Analyze the information to get the email addresses of the different developers.
- Send a customized phishing campaign in which even the webpage is tailored to the developer. This makes the trick seem even more plausible and helps achieve a better "conversion rate".
- Because the attacker has information on all the apps published by each developer, it is possible to create a system that alerts him every time a publisher with a popular app (millions of downloads) falls for the trap.

With this in mind, one of the easiest and least sophisticated attacks would be the publishing of apps from that account. Imagine if someone managed to steal the details of one of the developers of Candy Crush and published Candy Crush 2 from the same account – if the attackers were cleverer and found a way to modify the application without using the private key (which can't be obtained with stolen ID information), they could publish and update any application they desire.

In the previous example, imagine that the attackers created an updated version of Candy Crush that contained a Trojan – millions of people would download and install it without realizing that they are being endangered.

Google has created a new program called Android Security Awards that will compensate those who investigate and discover new weaknesses in Android's security.

The amount paid depends on the seriousness of the security weakness with a sum of $2,000 for a critical weakness, $1,000 for a high-level weakness, and $500 for a moderate level weakness. That said, depending on the seriousness of the problem and the details of the finding, that figure could reach as much as $38,000.

In July, Zimperium recognized a massive vulnerability for Android that affected 950 million devices that used the operating system. The problem wasn't just the amount of mobiles, tablets, or other devices that were affected, but rather how easy it was to remotely endanger them. By just sending a malicious MMS it is possible to take control of any telephone just by knowing the victim's number. It isn't even necessary to open the MMS, as Android automatically processes images, meaning that receiving the MMS was enough to cause the damage.

Although the problem has since been corrected, the large number of manufacturers and versions of the operating system means that there could still be some versions out there that haven't been updated with the latest safety measures.

Google has since made a large number of the manufacturers (Sony, LG, Motorola, etc.) include the latest updates and Samsung announced that they would offer monthly updates to their customers to keep ahead of new vulnerabilities that keep on appearing.

In fact, not long after, two investigators from IBM's XForce published another security problem that allowed an attacker to replace a legitimate application with a malicious one, which would then allow the attacker access to permission controls for the replaced app. Google has since updated its software to take care of this security problem.

We are now used to seeing ransomware attacks on PCs and it is becoming more common to see them taking place on Android, too. In fact, during the previous three months these attacks have been marked out for their originality and simplicity. What a malicious app does is change the PIN of the device and demand a ransom of 500 dollars.

For example, the users of our antivirus for Android can change the PIN code of their mobile from their web control panel, thus rendering this type of attack ineffective and saving themselves 500 dollars. Apple's operating system has also suffered various attacks during these months.

The company Appthority has discovered a vulnerability called Quicksand that affects corporations that use MDM (Mobile Device Management) services and could put confidential information relating to the company at risk. Apple has taken care of this vulnerability with its new version of iOS 8.4.1.

Another vulnerability that has been taken care of is ImsOmnia, which allowed a malicious app to avoid the running restrictions of Apple, permitting the activation of the microphone or camera and allowing the user to be spied on.

Apple had to remove a number of applications from its Apple Store owing to an attack known as XcodeGhost. The attackers published a modified version of the software that developed apps for iOS, which led to app creators using it to include malicious features in their apps without knowing.

Another attack targeted at Apple users managed to get off with iCloud credentials of more than 225,000 users. The attack affected users who had previously jailbroken their device so as to install apps without using the official App Store, but which resulted in the security controls installed on iOS being deleted.

Internet of Things

In July, HP Fortify published the results of a study on smartwatches which found that 100% of the devices analyzed were vulnerable to attack and shed light on the main problems that smartwatches face.

For example, none of the smartwatches offered a double authentication when linked to a mobile device and allowed for incorrect passwords to be entered repeatedly.

Security investigators Charlie Miller and Chris Valasek carried out a demonstration in July which left the world in shock.

They convinced Andy Greenberg, a journalist at Wired, to drive a Jeep Cherokee while the two of them hacked the car from their homes.

The attack started off with them taking control of things such as the air conditioning in the car, activating windscreen wipers, changing the radio station, and playing around with the volume… and ended with them taking complete control of the car, including its braking system.

They spent months working on these attacks and even informed the manufacturer before the test, hoping that they would install new security updates to cover this vulnerability. The pair gave more information on how they carried out the tests in an interview that they gave at the BlackHat conference in August.

Land Rover was also informed in July of a fault in software that affected 65,000 vehicles that had been on sale since 2013. The fault allowed for the unlocking of the doors by outside sources. Kevin Mahaffey and Marc Rogers, two investigators, showed how to hack a Tesla Model S. at the BlackHat conference. Despite needing physical access to the car to carry out this attack, they discovered 6 new vulnerabilities that allowed them to stop the engine when it was travelling at slow speeds. The manufacturer has since taken action to cover up this problem.

Hiroyuki Inoue, an associate professor at the Graduate School of Information Sciences in Hiroshima, carried out an experiment in which he connected a Toyota Corolla to the Internet and managed to hack it. He was able to remotely manipulate the windows of the car, change the speed limiter, and block the accelerator, among other things.

Although this experiment was with a car connected to the Internet – something which the model doesn't come with – it still raised alarm bells for manufacturers.

Cyberwar

For the first time, the United States imposed sanctions on a country in response to a cyber-attack.

The country in question was North Korea, and the sanctions were in response to the December hack on Sony Pictures over 'The Interview', a comedy film in which a couple of journalists are instructed by the CIA to assassinate the North Korean leader.

Additionally, new revelations came to light from the documents leaked by Edward Snowden to the press. In January, German magazine Der Spiegel published that China had stolen many terabytes of data relating to the F-35 jet fighter, including radar design information, engine schematics, etc.

Ben Rhodes, Assistant to the President of the United States and Deputy National Security Advisor for Strategic Communications and Speechwriting, stated that the White House had fallen victim to an IT attack. In an interview with CNN, Rhodes confirmed that the attackers obtained unauthorized access to an unclassified system of computers and stole highly important information, even though the classified system wasn't hacked. Despite not wanting to reveal whether the attack was perpetrated by Russian hackers nor when it occurred, Rhodes did give the impression that the attack hadn't taken place during the previous days. Without giving much more information, he stated that they had already taken "a series of security measures to evaluate and minimalize the damage caused".

In June we found out that the Office of Personnel Management (OPM), the human resources agency for the federal government of the United States, had been attacked and that confidential information relating to at least four million public sector workers had been stolen. This attack took place two months before then, at approximately the same time as the attack on the White House. However, it appears that the attacks weren't connected, given that the former appears to be linked to Chinese hackers, although the US government hasn't officially confirmed this.

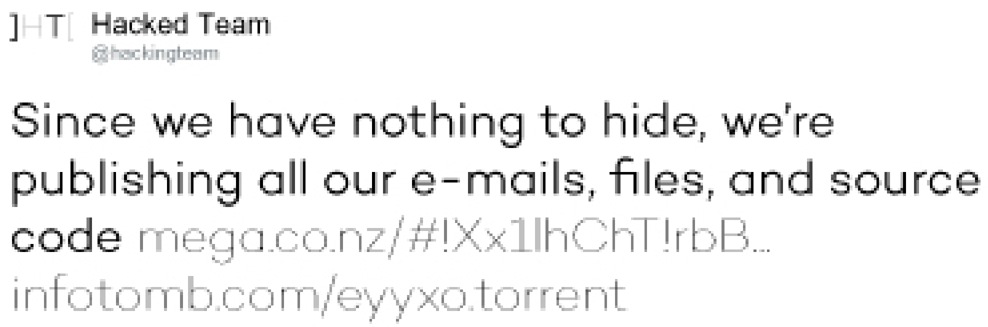
ISIS sympathizers attacked the French television station TV5MONDE, managing to sabotage its transmission. On top of that, they also took over its Facebook page and website.

The well-known group Syrian Electronic Army managed to infiltrate the website of the US Navy, publishing propaganda promoting Bashar Al-Assad and his regime in Syria.

The German parliament was the victim of an attack in which they managed to infiltrate and steal information from various computers. It is believed that the attack came from Russia, but it is difficult to prove exactly who was behind it. We already know that the NSA used a modified version of Stuxnet to try and sabotage a nuclear program by North Korea. Although on that occasion they weren't successful, it must be noted that with Stuxnet they managed to destroy at least one thousand centrifuges of uranium in a plant in Natanz, Iran, a few years ago.

Hacking Team is a business known for providing cyberespionage and cyberattack tools to a multitude of governments worldwide.

In July it suffered a massive hack which saw the theft of all types of data. The attack was made known via the Hacking Team's Twitter account, which was also taken over by the attacker who changed the name of the account to Hacked Team and attached a link to download all of the stolen information:



]HT[Hacked Team
@hackingteam

Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB… infotomb.com/eyyxo.torrent

They made public lists of clients (police and intelligence agencies of various countries, from the United States to Uzbekistan). They also made public a corporate certificate used by Hacking Team, passwords they were used on their most protected systems, lists of products that they sold, source codes for their applications, financial data, etc. They even published a website with a search function that allowed for all of the email addresses stored by Hacking Team to be searched through.

A few days later a Zero-Day was discovered on Adobe Flash thanks to the information stolen from Hacking Team.

James Comey, the director of the FBI, spoke at a security forum and told of how they had detected a growth in interest on behalf of terrorists in strategies for launching cyberterrorist attacks against the United States.

He didn't specify the types of attacks and said that they still appeared to be in the planning stages and that the terrorists were still looking into how effective they could be.

On July 25, Russian hackers managed to access a non-classified email system pertaining to the Pentagon. Official sources have stated that it was a sophisticated attack and that they were sure there was a government entity behind it.

In September, investigators at DGI published a study on the 78020 unit of the Chinese army, where they showed that it was behind a group known as Naikon, which was responsible for different military, economic and diplomatic cyberespionage attacks in the area. Its victims included Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, Vietnam, The United Nations Development Program, and the Association of Southeast Asian Nations..

Anonymous launched a campaign against ISIS, hacking and releasing websites and social media accounts of thousands of its members.

4. TRENDS FOR 2016

4

Trends for 2016

Below we will look at what we believe to be the main IT security trends for 2016.

1.- Exploit kits

They will continue to be the favored tool of cybercriminals, as they look to achieve massive infections. Exploit kits can be bought on the black market and come with updates, allowing attackers to find new victims with new methods of attack. Many security solutions still aren't capable of effectively combatting this type of attack, which means that the success rate is high for attackers.

2.- Malware

The number of new malware samples keeps rising. Although the majority of samples will continue to be PE types (https://es.wikipedia.org/wiki/Portable_Executable), we foresee a growth in non-PE malware, mainly scripts. It won't just be the well-known javascript, but rather there will be a growth in the use and abuse of Powershell, a tool that comes by default with Windows 10, which allows for the running of all types of scripts. It will combine itself with known attacks such as Fileless Attacks, where, instead of the malicious code being on a physical file on the computer, it will be a parameter in the execution of a command, or an entry in the register that contains the script to be executed.

3.- Direct attacks

There will be a growth in direct attacks. The use of rootkit techniques, which allow the attack to hide itself from the view of the operating system and security solutions, will intensify. Companies will be obliged to take security measures to be protected against these attacks as they can seriously damage the company, both financially and in terms of reputation. Keep in mind that these attacks look to steal both confidential company data (financial data, strategic plans, etc.) and that of their clients.

4.- Malware for Android

Malware for mobiles will increase, especially for Android as it is the most popular operating system on the market. We will see that more threats will root the device, meaning that eliminating it will be nearly impossible for antiviruses, except for those that come installed from the factory.

5.- Mobile payment platforms

It still isn't clear if 2016 will be the year in which these platforms become truly popular, but what we do know is that their use is going to increase and that they will become targets for cybercriminals due to them being a direct way of stealing money. If any of the platforms becomes the first to breakthrough and become popular, it will be a prime candidate for attackers looking to see any weakness that they can abuse in the system.

6.- Internet of Things

We know that 2016 won't be the year of the Internet of Things, but we will have more and more devices connected to the Internet and we will see many tests that show how different attacks can be carried out. We have already seen many such tests in 2015, like those on automobile software, which allowed for the cars to be remotely controlled while travelling.

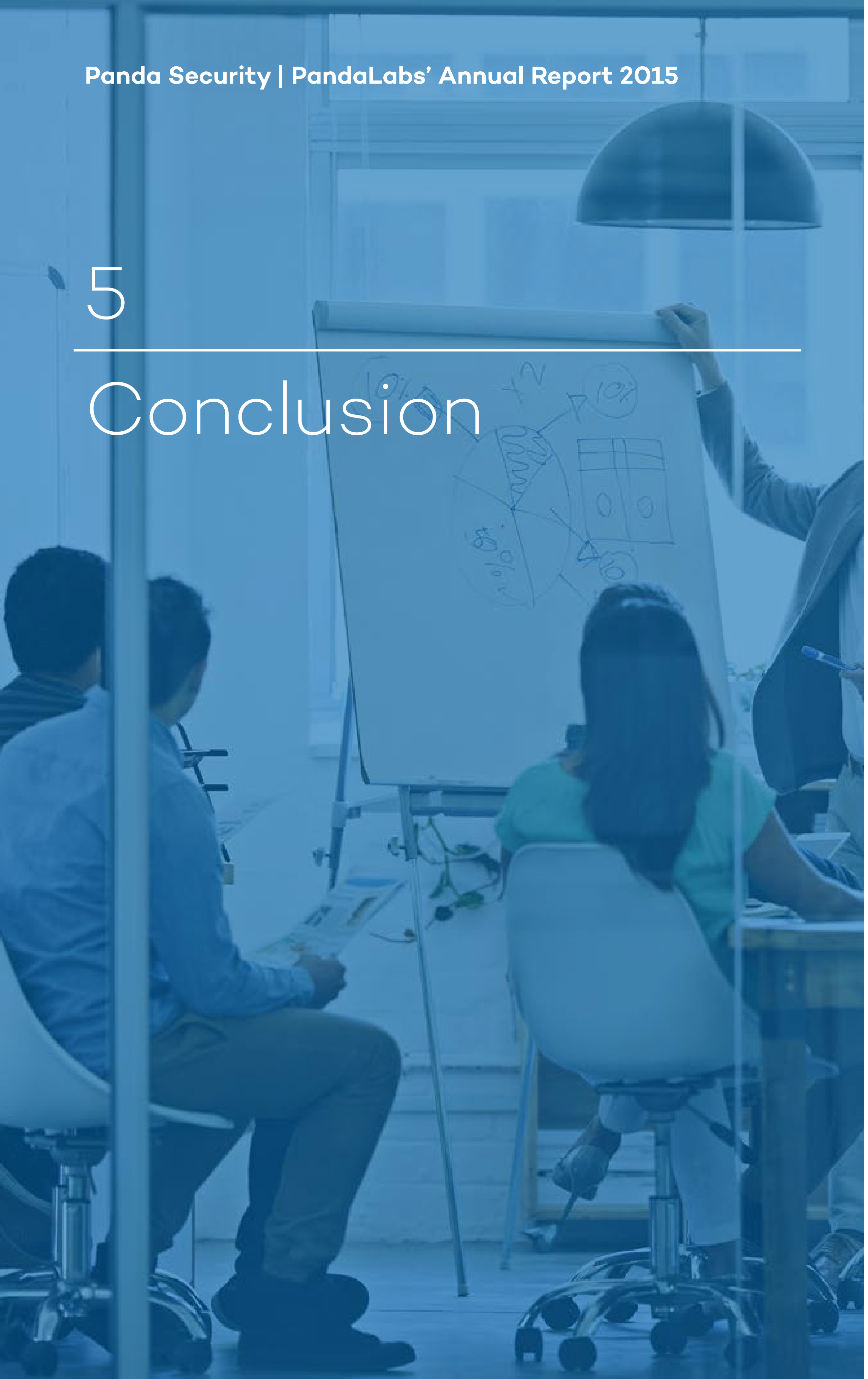
7.- Critical infrastructure

It won't be a target for regular cybercriminals, but in the area of cyberwar, the power to remotely sabotage the critical infrastructure of another country is something so valued that intelligence services from the world's most powerful countries will try to achieve it. It takes a lot of money and planning to carry out this type of attack, as we saw in the case of Stuxnet.

8.- Threat Intelligence for businesses

The growth in the number and complexity of attacks is changing the use of information, and also how it is shared. Even though companies that offer security solutions and services usually share information to be better able to protect their clients, the set up will change dramatically. We will have large companies asking their security provider to give them all of this information while also collecting all of the information that is on their networks and sharing it with other businesses.

5. CONCLUSION



5 Conclusion

2015 was a difficult year, one in which attacks grew at a rate never before seen, and the truth is that 2016 is going to be even harder. Many of the attacks that we saw last year will continue to be seen in the next 12 months, like Cryptolocker which has yielded so much rewards for cybercriminal gangs.

We must pay special attention to the Internet of Things, as we have more and more devices with Internet connection that could be turned into a tool for cybercriminals to get their hands on any information that they desire about us, both on a personal and corporate level. Although these devices don't usually store a lot of information, they can serve as an entry point for criminals to get onto our network, whether it be at home or at work.

Having seen the data thefts that have taken place, it is clear that businesses have a protection deficit that they need to work on immediately. Nobody should assume that they are protected and safe, it is better to behave as if you were already attacked, instead of waiting to find out months or years later. Keeping track of everything that happens on your network is essential.

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

6 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.