ANNUAL REPORT PANDALABS

2013 SUMMARY

PANDA SECURITY

01| Introduction

In this report we will analyze the most important events that occurred in the computer security world in 2013. We will also look at the malware figures recorded by PandaLabs, the anti-malware laboratory of Panda Security, which offer an accurate picture of the most significant trends in malware creation as well as the global situation in terms of malware infections. Suffice it to say that malware creation hit record-high numbers during the past year.

The most important news stories of 2013 centered on the cyber-espionage activities conducted by governments around the world. China, a usual suspect when it comes to this type of activities, was overshadowed by the information leaked by former National Security Agency contractor Edward Snowden, who put this organization and the U.S. government in the eye of the storm, as the controversy surrounding the NSA's surveillance program continued to grow.

Additionally, we will describe the evolution of mobile malware and the attacks targeting mobile device platforms. In this respect, Android continued to be the number target for cyber-criminals to steal data and money, as the number of threats in circulation multiplied, reaching astronomical figures.

We will discuss social networks in a year in which the number of account hijacking attempts increased spectacularly, affecting companies, celebrities and even U.S. President Barack Obama, whose Twitter account was also hacked.

Finally, we will make a series of predictions about the security threats we can expect to face over the next 12 months.

02| 2013 in Figures

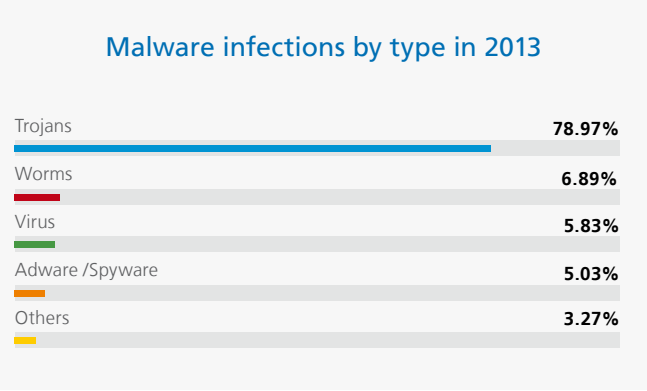
In 2013 alone, there were 30 million new malware strains in circulation, at an average of 82,000 per day. This has brought the grand total of all malware samples in PandaLabs' database to approximately 145 million. These numbers –which come as no surprise if we look at the trend set during the last 12 months– are certainly mind-blowing. Consider this: 20 percent of all malware that has ever existed was created in 2013. In a year that saw all kinds of cyber attacks, new waves of the infamous Police Virus and the resurgence of ransomware specimens such as CryptoLocker, Trojans continued to be the most common type of malware. Below are some interesting statistics about malware creation in 2013:

New malware strains in 2013, by type

Trojans	**71.11%**
Virus	**13.30%**
Worms	**8.49%**
Adware /Spyware	**6.93%**
Others	**0.17%**

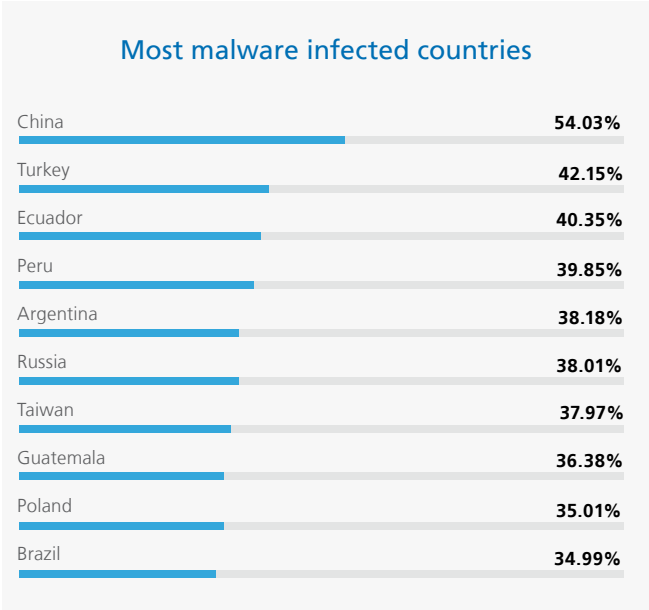
A comparison of these figures to those of last year reveals a significant growth in the number of viruses in circulation, rising from 9.67 percent in 2012 to 13.30 percent in 2013. This is mainly down to two particular virus families: Sality and Xpiro. The first virus family has been around a long time, whereas the second is more recent and capable of infecting executable files on 32-bit and 64-bit systems. One of the reasons why these viruses have become so popular in cyber-crime circles is that they can be used for data theft, which has led to big profits for malware developers.

When it comes to the number of infections caused by each malware category, data gathered by our Collective Intelligence platform indicates that three out of every four malware infections were caused by Trojans (78.97 percent). It seems that cyber-criminals have managed to infect more computers with Trojans this year than in previous years. In 2011, Trojans accounted for 66 percent of all computer infections, whereas this percentage surged to 76 percent in 2012. The year 2013 confirmed this trend. Here is a graph showing these results:



The proportion of infected computers around the world was very similar to 2012 (31.53 percent). The countries leading the list of most infections are China (with 54.03 percent of infected computers), followed by Turkey (way behind at 42.15 percent), and Ecuador (40.35 percent).

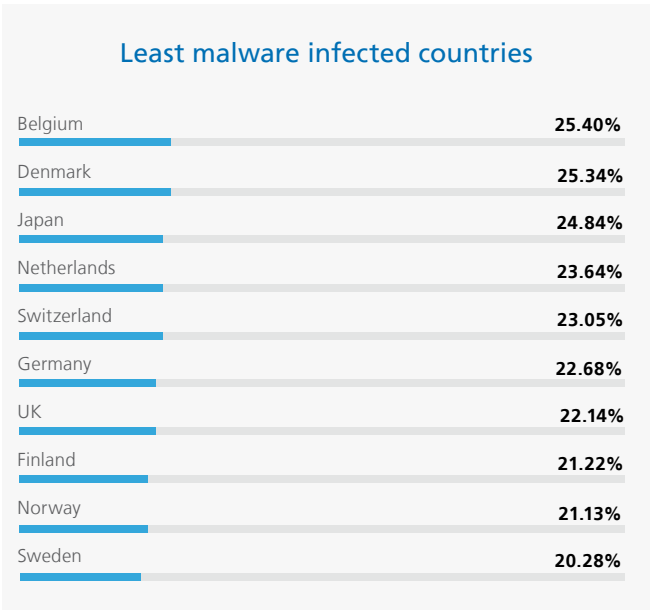
The graph below shows the ten countries with the most malware infections in 2013:



Asia and Latin America are the regions with the highest number of computer infections. Other countries with an infection rate over the global average include: Uruguay (33.64 percent), Chile (33.51 percent), Spain (32.72 percent) and Colombia (32.22 percent).

Nine of the ten least infected countries are in Europe with the only exception being Japan. The ranking is topped by Scandinavian countries: Sweden (20.28 percent of infected PCs), followed closely by Norway (21.13 percent) and Finland (21.22 percent).

Here's a graph representing the countries with the fewest infections in 2013:



Other countries outside this Top 10 but with infection rates below the average are: Portugal (25.28 percent), France (25.68 percent), Australia (26.84 percent), Austria (27.69 percent), Canada (27.82 percent), USA (28.96 percent), Venezuela (29.83 percent), Hungary (30.96 percent), Mexico (31.00 percent), Italy (31.47 percent) and Costa Rica (31.50 percent).

03| 2013 at a glance

Last year we saw many major companies fall victim to all kinds of cyber-attacks.

CYBER-CRIME

Last year we saw many major companies fall victim to all kinds of cyber-attacks. On February 1, **Twitter** published an article on its blog ("*Keeping our users secure*") detailing how the social network had fallen victim to an attack resulting in unauthorized access to the details of some 250,000 Twitter users.

A couple of weeks later, **Facebook** also released an article on its blog, entitled "*Protecting People On Facebook*". According to sources from the social network, user data was not compromised in this attack. The next victim was **Apple**. Just a few days after the Facebook announcement, spokesmen from Apple told *Reuters* that the company had also been targeted by the same attack.

And finally, of no less importance, **Microsoft** *admitted* that it too had been targeted.

An impressive list, isn't it? As far as we know, no other major company claimed to have suffered the same attack. In any event, there are some positives we can take from the situation:

- Companies are not shy to admit they have been targeted.
- Many companies have good security teams that have been able to identify the attacks as they happened.

Of course, all these attacks exploited a previously unknown security hole in Java for which no patch was available. This is known as a zero-day vulnerability.

Twitter, **Facebook**, **Apple** and **Microsoft** fell victim to a sophisticated attack that infected employees' computers by exploiting an unpatched Java vulnerability

Anyone who works in security knows that nothing is 100 percent secure. A number of preventative measures may work well most of the time. Yet there will always be weak points, a new vulnerability, human errors, etc. which may finally facilitate one of the thousands of attacks to which these companies are constantly subjected.

Here it is critical to be able to identify an attack when it is occurring. Twitter, Facebook, Apple and Microsoft were able to do this. All of them managed to gather data about the attack. All worked with the police to find out who was behind this.

Perhaps those running a small or medium-sized business feel they don't have to worry as much about security as these giants, given that they don't make such a 'sexy' target. And that's true to an extent. They probably receive a very small number of targeted attacks (if any), they will however be bombarded with the type of attacks from cyber-criminals that infect millions of computers. And these criminals like nothing more than an easy target. In short, all those with unprotected computers, with out-of-date software and without a serious security policy are surefire targets.

Most infections today occur through 'exploit kits', infecting users' computers through a vulnerability without their knowledge. More than 90 percent of these are through Java vulnerabilities in browsers. The attacks on Microsoft, Apple, Facebook and Twitter used Java. Most 'Police Virus' infections managed to reach victims' computers thanks to outdated versions of Java.

Java continues to be a major infection vector to compromise users' systems

What is the best way of preventing these infections? Simple: Just remove Java from the browser. If for any reason you need Java on your browser to use an application, use it on another browser set up specifically for this task.

Evernote was the victim of an intrusion that prompted the firm to release a statement calling on more than 50 million users to change their passwords. According to a statement from the **U.S. Federal Reserve** its website was also attacked, although it did not say whether any data was stolen. The incident coincided however with the publication, by Anonymous, of the personal information of 4,000 U.S. bank executives, suggesting that the attack on the Fed may have been carried out by this group. The NASA was also the victim of an intrusion. Internal information including email addresses, real names and passwords was published on the popular website Pastebin.

Cyber-criminals often try to exploit newsworthy events or notable dates to try to spread malware to new victims. This was apparent during the second quarter of 2013 when they used the terrorist attack on the Boston marathon. Similarly, the news of a fatal accident at a Texas fertilizer plant was used as a ruse to spread malware.

The news of the attack on the Boston marathon was used by cyber-crooks as a subject for spam messages

Another type of attack took advantage of International Workers' Day -May1- to compromise the U.S. Department of Labor website and spread malware.

When talking about how cyber-criminals infect computers to steal data and profit from it, perhaps the first thing that comes to mind is theft of online banking credentials in order to steal from bank accounts. However, there are other, more imaginative types of theft that take place in virtual worlds. For example, in World of Warcraft, the world's most popular MMORPG, cyber-criminals stole millions of 'gold' pieces from players' accounts. Investigations determined that this gold had been used to buy items in the game's auction house. It finally became clear that the attackers had exploited an error in the Web and smartphone app to enter the auction house.

An error in the smartphone app for the World of Warcraft Armory was used by cyber-crooks to steal millions of pieces of gold

The British Federation of Small Businesses issued a report revealing that 41 percent of small businesses had suffered attacks from cyber-criminals during 2012, with a cost of 785 million pounds.

The **LivingSocial** website was the victim of a cyber-attack that could affect as many as 50 million customers. Compromised information included names, email addresses, dates of birth and passwords.

The **Syrian Electronic Army** hacking collective continued their attacks against different institutions around the world. In July, they used phishing techniques to hack into the personal Gmail accounts of at least three White House social media staffers. Then, they used the compromised accounts to send phishing emails to other White House accounts. In August, the Washington Post reported being victim of a hacking attack, with readers of certain articles being redirected to the site of the Syrian Electronic Army.

Hacking group Syrian Electronic Army was particularly active last year, with victims including the New York Times, Twitter and even some White House employees

A few weeks later it was the New York Times and social networking site Twitter that fell victim to the hacking group. In this case the criminals didn't use a hacking attack, but a technique called DNS cache poisoning that redirected users who typed the Web addresses of these two organizations to another site. However, users who tried to access these Web pages via their IP addresses, could do so without problems.

DNS cache poisoning attacks are nothing new, although they have become more common in recent months. Several large websites hosted in Malaysia fell victim to this type of attack, including the local websites of companies such as Google, Microsoft or Kaspersky.

DNS cache poisoning attacks have been on the rise over the last few months

The "**Police Virus**" showed no sign of receding and continued wreaking havoc among users through new variants. Despite the arrest of one of the gangs behind the attacks, other criminals launched similar offensives. One of them was especially noteworthy for the high 'fine' it demanded from users ($/€300 instead of the usual $/€100).

One of the most notable –and notorious– threats over the past 12 months was CryptoLocker, a new Trojan that uses ransomware techniques, hijacking users' documents and asking them to pay a ransom for them.

CryptoLocker is a new family of malware that hijacks users' documents and demands a ransom for them

Even though this type of attack is nothing new, this new ransomware has some unique characteristics that made it a success for its creators:

- Instead of encrypting every file it finds, it focuses on those most valuable to users: photos, videos, text documents, etc.
- It not only encrypts files on the computer's hard disk, but also on every network drive the infected user has access to.
- It uses asymmetric encryption, which makes decryption impossible without having access to the actual key used by the cyber-criminal to encrypt the files. Neither is it possible to decrypt the files using any kind of forensic tools.
- The message displayed asking users to make the payment includes a countdown timer, pressing the victim into making a decision: pay the ransom or lose access to their files forever.

If we had to choose one attack from those occurred last year, it would be the Adobe hack. The company initially revealed that source code for its products as well as data of nearly 3 million Adobe customers had been stolen in a massive data breach.

Soon after these revelations became public, a file was leaked online which contained 150 million user names and passwords. Adobe was then forced to admit that the number of active users affected by the hack was at least 38 million, far bigger than initially reported.

Nearly 2 million of Adobe users used "123456" as password

This high profile hack revealed some interesting –and alarming– data about the most popular passwords used by Adobe users and their weakness. Here are the most common passwords, followed by the number of Adobe users who used that password:

"123456" (1,911,938 users)
"123456789" (446,620 users)
"password" (345,834 users)

THE FIGHT AGAINST CYBER-CRIME

The year started with good news. On January 11, the European Commission inaugurated the European Cybercrime Center (EC3) in order to support member states in the fight against cyber-attacks. The truth is that cyber-criminals have often benefited from the difficulty in coordinating the police effort across different countries, and therefore such initiatives are always welcome.

The European Commission inaugurated the European Cybercrime Center (EC3) in order to support member states in the fight against cyber-attacks

In January, the FBI published details of an investigation that began in 2010 and thwarted a gang of cyber-criminals who had infected more than a million computers since 2005. This operation stands out not least because of the coordination between security forces in different countries. The FBI had the support of police in Moldavia, Romania, Holland, Germany, Finland, Switzerland and the UK.

One of the most infamous cases of the last year or so was the '**Police Virus**'. In February this virus once again hit the headlines, but this time for a very different reason. Our friends in the Technological Investigation Division of the Spanish National Police, in collaboration with Europol and Interpol, dismantled the gang of cyber-criminals responsible for the virus. According to a statement from the *Spanish Interior Ministry*, ten individuals were arrested from the group's financial cell, which generated a million euros a year from victims of the malware. Six of those arrested were Russian citizens, two were Georgian and two Ukrainian.

The Technological Investigation Brigade of Spain's National Police, together with Europol and Interpol, broke up one of the cyber-crime gangs responsible for the 'Police Virus'

The head of the whole operation –a Russian resident– was also detained while on holiday in Dubai.

Russian and Ukrainian police arrested the cyber-gang leader responsible for the Caberp botnet, along with 20 other individuals who were part of the malware development team. The gang leader (28) was a Russian citizen living in the Ukraine.

The U.S. government was responsible for a major blow to the financial structure used by cyber-criminal gangs around the world when it shut down Liberty Reserve, the 'favorite bank of cyber-crooks'. This company enabled anonymous cash transactions, and investigations led to some of the owners being arrested. It's not yet clear what will happen to the money of the bank's legitimate customers who were not involved in any illicit activities.

After several years of investigation, Liberty Reserve was shut down by the U.S. government and the owners arrested

The European Parliament passed a bill imposing harder sentences on cyber-criminal activities. For example, simply creating or using a botnet may be punished with a minimum of three years in prison, excluding other crimes that may have been committed using the botnet.

One of the highlights in the fight against cyber-crime was the arrest at the end of the year of "Paunch", the author of BlackHole, perhaps the most popular exploit kit among cyber-criminals.

SOCIAL NETWORKS

Social networking sites have become a hub of social interaction in today's digital world. They have given millions of people the ability to stay in touch with family and friends and keep up-to-date with everything that happens in the world. Most companies today have their own Twitter and Facebook accounts, and major brands attract thousands of followers, which has put social media sites in the crosshairs of cyber-criminals. One of the most notable cases was that of **Burger King**, with attackers seemingly managing to work out the account password and take control of the account. They changed the background image to that of McDonalds and claimed that the company had been taken over by its main rival.

Burger King's Twitter account was compromised and had its profile image changed to McDonalds

The Twitter account of Jeep was also the victim of a similar attack, in this case stating that the company had been bought out by Cadillac. Other attacks on Twitter accounts had a more political slant. A group of cyber-crooks calling themselves the "Syrian Electronic Army" managed to hack accounts belonging to several organizations. From what we can determine, phishing attacks were launched to get the passwords and then the accounts were hijacked. Their victims included Human Rights Watch, the French news channel France 24 and the BBC weather service.

On many occasions we are not fully aware of the consequences these attacks may have. Let's see some examples: The 'Syrian Electronic Army' which was responsible for several attacks earlier in the year, hacked the Twitter account of the **Associated Press**. Once it had taken control of the account, it published a fake breaking news story: 'Two Explosions in the White House and Barack Obama is injured.' Immediately, numerous followers of the account helped the story to spread like wildfire, resulting in the Dow Jones index dropping 145 points.

Dow Jones industrial average tumbled 145 points after **Associated Press** hack attack

It was discovered that the attackers had sent a malicious email to the AP staff claiming to be a news item from a major American newspaper. Recipients were encouraged to click a link in the email. Anyone who followed the link would be taken to a fake Twitter sign-in page, and asked to enter their login credentials.

This was how the 'Syrian Electronic Army' managed to take control of the AP Twitter account. This same group continued to launch attacks, with victims including **CBS**, who had three Twitter accounts hacked, including the '60 Minutes' account, and satirical news site The Onion.

The Syrian Electronic Army stroke again in October, managing to hack the T**witter account of U.S President Barack Obama,** and posting two links to videos with Syrian pro-government propaganda.

In October, U.S **President Barack Obama's Twitter account** was hacked by the 'Syrian Electronic Army'

However, not all news regarding social networks had to do with cyber-attacks originating from external sources: Facebook acknowledged that it had inadvertently exposed six million users' phone numbers and email addresses as a result of a technical flaw. Additionally, Facebook announced it had finished its migration to secure browsing, with all active users of the most popular social networking site now accessing it over HTTPS. This means that all traffic between users' devices and Facebook is now encrypted to prevent data theft.

Facebook users now connect to the social media site via HTTPS

MOBILE PHONE MALWARE

Practically all news regarding malware attacks on mobile platforms involved the Android operating system, which has the largest share of this market. In addition to the usual attacks, last year we saw new techniques that deserve mention. A strain of Android malware -hidden inside Google Play- not only infected cell phones but could also infect computers via smartphones or tablets. The technique was very simple: Once it run on the phone, it connected to the Internet to download files which it stored in the root directory of the device storage card, so then when it connected to a computer via USB, it automatically run one of the files, a Windows Trojan.

In April, a new type of attack on Android operating systems was discovered. In this attack, malware was being spread through non-malicious apps. Many free apps include some kind of advertising as a way of financing the app, instead of charging for it. In this case, cyber-criminals apparently offered apps that were not in themselves malicious, but they controlled the advertising displayed. Once they had enough users of these applications, they began to display ads with fake app update notifications, which if installed on the device, used a Trojan to send SMS messages to premium-rate numbers. There were 32 apps in all, and the total number of downloads through Google Play reached nine million.

2013 saw a large number of Android scams using malicious ads in legitimate apps

While the amount of malware for Android is still low compared to Windows, it is definitely on the increase. We are no longer talking about sporadic attacks or a few dozen malware strains doing the rounds: In 2013 alone there were over two million new different strains of malware for **Android** in circulation.

Google's Android security chief Adrian Ludwig reported that "less than an estimated 0.001% of app installations on Android are able to evade the system's multi-layered defenses and cause harm to users." Despite these statistics, there is no denying that Android is the mobile platform most targeted by cyber-criminals.

While it is true that Android attacks are normally carried out employing social engineering techniques, this doesn't mean that the platform is free from vulnerabilities that could be exploited by an attacker. In fact, in 2013 we saw a new form of attack that involved modifying a legitimate APK file (Android app installer) to install any type of malicious code in an undetected way.

However, this platform is not the only one subjected to attacks. Platforms such as iOS, Apple's operating system for smartphones (iPhone) and tablets (iPad) were also in the crosshairs of criminals. In July, a group of researchers from Georgia Tech Information Security Center (GTISC) revealed how they were able to hack into an iPhone using a malicious charger.

Fake chargers can infect iPhone devices with malware

In September, **Apple** launched the new iOS 7 which, in addition to an all-new design and all-new features, included fixes to 80 different vulnerabilities, including the fake USB charger flaw. However, just a few hours after its release, new security flaws had been reported in iOS 7. One of them, for example, allowed attackers to bypass iOS 7's lock screen. November was the month when the "Mobile Pwn2Own 2013" took place, an event in which participants compete to uncover new vulnerabilities in mobile devices. The event saw all kinds of attacks: from capturing Facebook credentials on an iPhone 5 with the latest iOS version installed, to exploits against several apps installed by default on the Samsung Galaxy S4, attacks via Chrome on a Nexus 4, exploits against Internet Explorer 11 on a tablet with Windows 8.1… No one survived the hacker jungle.

CYBER-ESPIONAGE

China often gets a mention in this section, and it did earn all the headlines at the start of the year before being overshadowed by the information leaked by former National Security Agency contractor Edward Snowden. In any event, let's take a look at the stories that involved the Asian giant before analyzing the scandal surrounding the **NSA** cyber-espionage programs.

On January 30, the **New York Times** ran a front-page article explaining how they had been victims of an attack that had allowed their computers to be accessed and spied on for months. Coincidentally, the attack came just after the paper released an article describing how Chinese PM, Wen Jiabao, and his family had amassed a billion-dollar fortune.

> The New York Times, The Wall Street Journal and The Washington Post were the target of a politically-motivated attack originated in China

A day later, The **Wall Street Journal** declared that it had also been the victim of a similar attack by Chinese hackers. The Chinese government protested against these 'unjustified attacks' and Hong Lei –Chinese Foreign Minister- claimed it was "…unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence."

Interestingly, in both incidents the attackers were able to access all types of data (customer details, etc.), yet only focused on information about journalists and employees, trying to find any reference to investigative journalism regarding China, and in particular, looking for the papers' sources.

The day after the Wall Street Journal's revelations, another U.S. media giant, The Washington Post, announced they had suffered a similar attack in 2011, also originating in China.

Some weeks later, Mandiant published a damning 76-page report (APT1: Exposing One of China's Cyber Espionage Units, *http://intelreport.mandiant.com*/) explaining how Unit 61398 of the Chinese army has specialized in cyber-espionage. The report reveals more than 3,000 pieces of evidence showing how this unit has been running since at least 2006, stealing information from no less than 141 organizations worldwide.

We may not truly appreciate the importance of the Mandiant report and the impact it may have in the mid to long term. Proving who is behind any attack is highly complex, even in normal cyber-crime cases. When it comes to cyber-espionage things are further complicated by the simple fact that whoever is behind the operation is highly qualified and adept at covering their tracks. For some years now, people have turned their gaze to China whenever this type of incident occurs, yet without any real evidence that the Chinese government is behind such attacks. Now, for the first time, it has been proven that the Chinese army is actively involved in espionage on a global scale, infiltrating companies across many sectors and stealing information.

A week after the Mandiant report was published, several other stories of cyber-espionage emerged that also pointed towards China: EADS (European Aeronautic Defence and Space Company), manufacturer of the Eurofighter and owner of Airbus, was attacked by hackers according to Der Spiegel (*http://www.spiegel.de/international/world/digital-spying-burdens-german-relations-with-beijing-a-885444.html*). The article also mentioned another similar attack on the German company ThyssenKrupp.

It was revealed that Chinese hackers gained access to plans of more than two dozen U.S. weapons systems. The Washington Post obtained an internal report of the Pentagon's Defense Science Board (DSB) detailing how they gained access to plans of Patriot missiles or fighter aircrafts such as the F-35.

> Chinese hackers stole plans for the F-35 fighter as well as other weapons systems

In any event, there is nothing new about such attacks aimed at the United States clearly originating from China. In fact, the Pentagon itself in its annual report to Congress accused China of being behind numerous attacks on U.S. intelligence data.

According to a report by Taiwan's National Security Bureau, the Chinese cyber-war machine continues to grow and now has about 100,000 personnel.

All these attacks have led to serious concerns from numerous governments, who are trying to implement security measures. Indonesia, for example, has recently announced the setting up of a military cyber-unit. The country's defense minister said that the main objective of the new unit would be to protect government portals and websites from cyber-attacks.

The NSA and Privacy Violation in the Name of Safety

On June 6, a story emerged that spread around the globe in just a few minutes: the U.S. National Security Agency, the **NSA**, had been indiscriminately spying on individuals and businesses around the world. And there was evidence of it.

According to the Washington Post, the NSA had been spying on 'everyone' using a program called PRISM with the voluntary assistance of nine technology sector giants. Microsoft, Apple, Google, Yahoo, Facebook, YouTube, Skype, AOL, and PalTalk. The NSA had supposedly obtained any data they wanted on all of these companies' customers. This story was immediately echoed by media around the world.

NSA was reported to have used its PRISM program to obtain data from users of online platforms

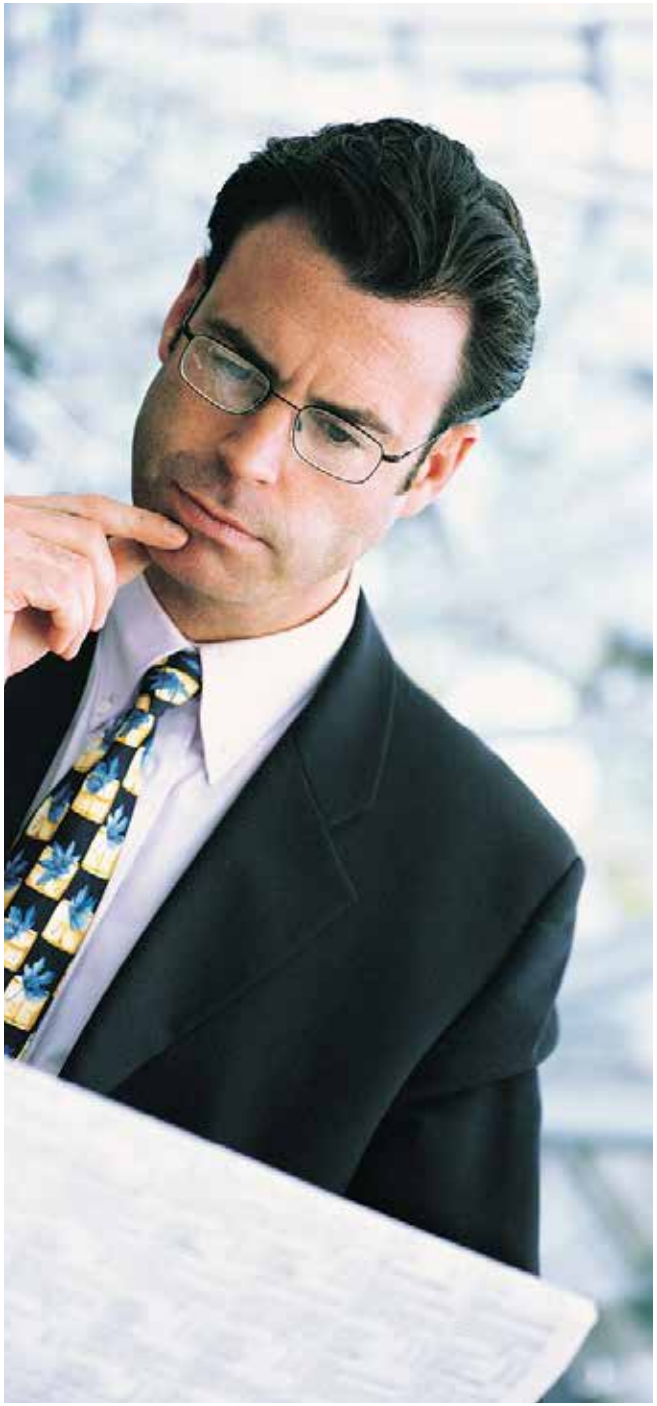
These companies categorically denied the accusations. In fact, the Washington Post edited the story the following day, changing the title and deleting references to how the companies were voluntarily releasing all kinds of customer data to the NSA.

After the repercussions of the NSA spying scandal, major communication companies have asked the U.S. government for greater transparency in surveillance programs. More specifically, they are asking the government to allow them to make public the data request received from the NSA, as well as additional information in relation to these requests.

The NSA inserted a backdoor in a popular pseudo-random number generator endorsed by important official institutions

According to new revelations, it has emerged that the NSA put a backdoor in Dual EC_DRBG, a pseudo-random number generator algorithm certified by the most important international bodies. In fact, some days after this information was made public, computer security company RSA issued an advisory telling its customers to stop using the algorithm, which was included by default in two of its products. But there was more: The scandal reached epic proportions when it was revealed that the RSA received US$ 10 million from the NSA for implanting the aforementioned backdoor in the algorithm.

But the scandal continues: If we had to detail every privacy violation that this surveillance program has led to we would need a book. And just when you think it can't get any worse, along comes a new story to prove you wrong. According to the information leaked to the public, the NSA monitored billions of phone calls, hacked into companies such as Google to collect user data, infected tens of thousands of computer networks around the world to steal information, and even tapped the phone calls of German chancellor Angela Merkel… The NSA knows no boundaries, and the impact of this massive surveillance program will linger for years.



04| 2013 Security Trends

Malware Creation. Malware creation will hit a new record high in 2014. Actually, such was the case in 2013, 2012, etc. Most new malware will be variants of known malware conveniently modified to bypass security products.

Vulnerabilities. Security holes in Java have been responsible for most infections detected throughout 2013, and this is not likely to change during 2014. The fact that Java is installed on billions of computers (and some other type of devices) and is apparently affected by countless security flaws has made it a favorite target of cyber-criminals. There is no exploit kit on the market worthy of that name that doesn't exploit a set of Java vulnerabilities.

Social Engineering. Social engineering is a field that gives cyber-crooks freedom to show their creativity. After vulnerabilities, the second most frequent cause of computer infections is… users themselves, who many times fall into the trap set by cyber-criminals. Despite many scams propagate via email, most of them occur on social networking sites, a meeting place where users share information, but also the perfect place for malware to spread.

Mobile Malware. Android will continue to be the number one mobile target for cyber-crooks in 2014, and the coming year will set a new record for the number of threats targeting this platform.

Ransomware. In addition to banking Trojans and bots, ransomware will be one of the most pervasive threats in 2014. Get ready for new waves of malware asking victims to pay a ransom to unlock their computers, access their files (CryptoLocker), remove supposed threats (fake antivirus software), or even pay a 'fine' for supposed illegal activities (Police Virus). Ransomware allows criminals to obtain money directly from users, and so we can expect it to soar and extend to other types of devices, like smartphones, for example.

Corporate Security. As malware attacks become increasingly aggressive (look at CryptoLocker for example) and the number of targeted attacks suffered by companies rises, there will be a demand for extra-tight security measures that go beyond the protection provided by a "traditional" antivirus. Traditional perimeter solutions are still a necessity, but they have become obsolete in some of the new scenarios companies have to face: users who bring their own devices to work and connect them to the corporate network… Not to mention the espionage operations conducted by governments themselves (NSA, etc.). It is for all these reasons that new solutions will be released capable of responding to these needs and offering protection levels that ensure data security and integrity much more effectively.

Internet of Things. The number of objects and devices connected to the Internet is ever-increasing, and will continue to do so. IP cameras, TVs, multimedia players are now an integral part of the Internet, and often share a characteristic that sets them apart from other devices such as laptops, smartphones or tablets: Users rarely update them. As a result, they are extremely vulnerable to security flaw exploits, and so we are likely to see attacks that target these devices as well.

05| Conclusion

Over the next 12 months we will have to pay special attention to Android threats, as they are clearly on the rise all around the world. In this context we can expect to see new waves of attacks aimed at stealing data and money.

Edward Snowden will continue to leak NSA surveillance information, and new stories will emerge about other operations to spy on citizens massively and indiscriminately. This continuous violation of people's privacy will continue to grab headlines, although its consequences are yet to be seen.

Businesses are cyber-brooks' favorite 'victims'. Today, companies not only have to worry about infections resulting from an employee's careless behavior, they also know that they are in the crosshairs of attackers looking to steal sensitive data. For this reason it is essential for them to deploy comprehensive security solutions that allow them to have complete control over everything that happens on their network, control software execution, and monitor who and when accesses corporate data.

Visit the PandaLabs blog *http://pandalabs.pandasecurity.com/* to stay up to date with the latest discoveries made at the laboratory.

06| 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.

For further information about the last threats discovered, consult the PandaLabs blog at:
http://pandalabs.pandasecurity.com/

07| Follow us on the web

facebook
https://www.facebook.com/PandaUSA

twitter
https://twitter.com/#!/Panda_Security

google+
http://www.gplus.to/pandasecurity

youtube
http://www.youtube.com/pandasecurity1

linkedin
http://www.linkedin.com/company/panda-security