PandaLabs annual Report

2011 Summary

01| Introduction

Here you will find a summary of the most notable figures regarding malware creation and infections in 2011, a year that has set a new record for malware with 26 million new strains in circulation.

We also cover social networks, where Facebook is still king both in terms of users and the number of attacks suffered, and we take a look at the cell phone and tablet sector, where Android has become the number one target for cyber-crooks.

2011 has undoubtedly been the year of cyber-security awareness, with the headlines frequently featuring reports of serious cyber-attacks. We have seen the largest data breach to date, as Sony's PlayStation Network was hacked, affecting millions of users. In all, Sony suffered over a dozen attacks, with theft of over 100 million user details. Similarly, Steam, Valve's online gaming platform, was hit by attackers who stole personal information belonging to more than 35 million customers.

Cyber-war has also been one of the top stories of the year. There have been cases all over the world and numerous nations have been affected. This kind of attack not only affects governments, but also government contractors like weapons manufacturers.

This report recaps the major computer security events that occurred in 2011, and forecasts future trends for 2012.

02| 2011 at a glance

Social networks play a vital role in the life of Internet users, with Facebook and Twitter as the world's biggest social media sites. This year we have seen the launch of a new social networking service in a bid to rival Facebook: Google+ .

Social networks

GOOGLE+.

Despite its rapid growth, with more than 25 million users registered in just few weeks, Google+ is still far away from its direct competitor, Facebook, which makes it less of a target for cyber-crooks. However, we have seen a curious attack: Right after its launch, as invitations were not open to everyone and there was huge expectation and interest in getting one, Google+ became the subject of a scam… on Facebook. Fraudsters created a Facebook page titled "Get Google Plus Invitation FREE" where users just had to click the 'Like' button to get an invitation. Obviously, you also had to provide your email address to receive the invitation which, unfortunately, never came.

TWITTER

2011 has seen a reduction in the number of attacks on Twitter, the short-message social network, and despite there continues to be attacks based on exploiting Twitter's 'Trending Topics', they are decreasing probably due to better filtering by Twitter's own team. In any event, it continues to be exploited as a platform to send out spam and hack accounts, as shown in the following examples: On July 4, Fox News's Twitter account was hacked and started to post a series of alarming tweets reporting that U.S. President Barack Obama had been assassinated. In addition, the Twitter account of PayPal UK was hacked and used to criticize its poor security in offensive language.

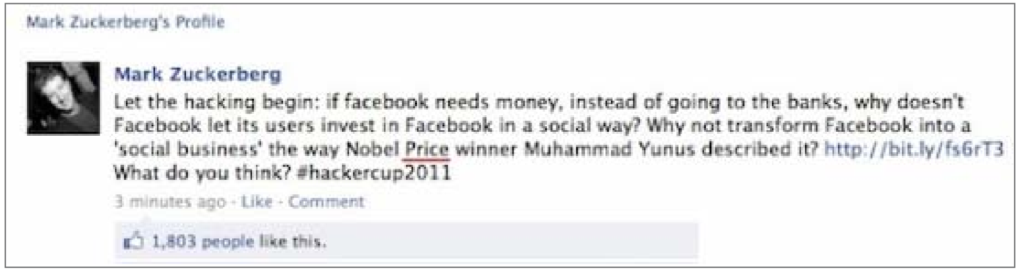
However, other attacks had far more serious consequences. A group of attackers hacked the Twitter account of a financial institution and started sending Direct Messages (DMs) to its followers instructing them to click on a link due to a security problem in their accounts. This link took users to a phishing page that imitated that of the bank and requested data that could then be used by attackers to impersonate the victims and steal their money.

FACEBOOK

When talking about Facebook attacks, most of us tend to think that cyber-criminals use the platform to spread their malware, but that is not usually the case. As we have said on many occasions, users give away too much information on their social networking profiles, which jeopardizes privacy and facilitates hacking of email and even Facebook accounts themselves. George S. Bronk was arrested in California for carrying out this type of illegal activity. Using information available on Facebook, he managed to gain access to victims' email accounts.

Having hijacked the account, he would search for personal information he could then use to blackmail the victim.

It would seem that anyone could become a victim of these types of attacks, as even Mark Zuckerberg –creator of Facebook– had his Facebook fan page hacked, displaying a message that started "Let the hacking begin".



Mark Zuckerberg's Profile

Mark Zuckerberg
Let the hacking begin: if facebook needs money, instead of going to the banks, why doesn't Facebook let its users invest in Facebook in a social way? Why not transform Facebook into a 'social business' the way Nobel Price winner Muhammad Yunus described it? http://bit.ly/fs6rT3 What do you think? #hackercup2011

3 minutes ago · Like · Comment

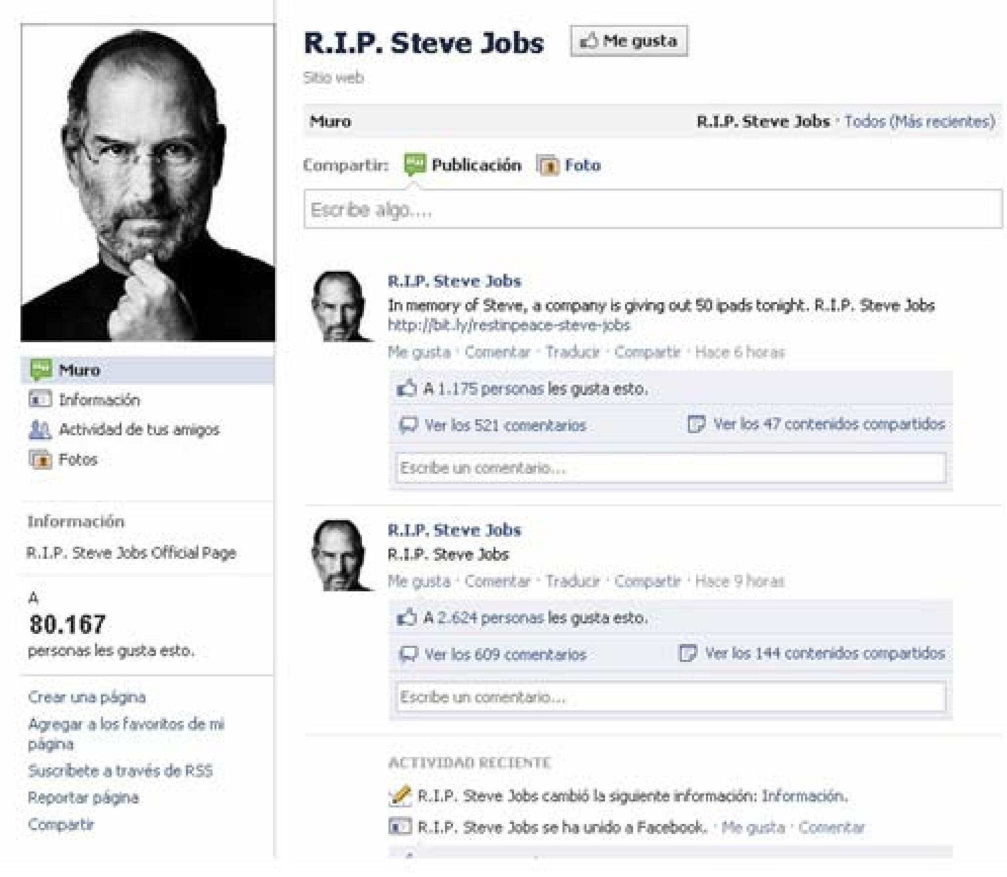
1,803 people like this.

FIG.01.*MARK ZUCKERBERG'S FACEBOOK PAGE HACKED.*

Finally, if there is one thing that social networks prove, it is that users are very much capable of making the same mistakes over and over again. Malware campaigns fooling Facebook users into believing they will discover who is secretly viewing their profiles are still hugely successful, and infect thousands of computer users around the world.

These scams are actually quite frequent on Facebook, cyber-crooks' favorite platform for launching social engineering attacks by exploiting real or fake news stories.

For example, a few hours after Steve Jobs's death, scammers had created a Facebook page called R.I.P Steve Jobs, attracting thousands of users. The page gained five new fans every second and amassed more than 90,000 fans in just a few hours. It contained a malicious URL and a text claiming that 50 free iPads were being given away 'in memory of Steve Jobs'. Obviously, this was nothing but a scam, and once the user clicked the URL (which ended with "restinpeace-steve-jobs"), they were taken to a website offering prizes like iPads, Sony Bravia TVs, etc. However, in return users had to submit their personal details: name, telephone number, email address, etc.



R.I.P. Steve Jobs 👍 Me gusta

Sitio web

Muro R.I.P. Steve Jobs · Todos (Más recientes)

Compartir: Publicación Foto

Escribe algo....

R.I.P. Steve Jobs
In memory of Steve, a company is giving out 50 ipads tonight. R.I.P. Steve Jobs
http://bit.ly/restinpeace-steve-jobs
Me gusta · Comentar · Traducir · Compartir · Hace 6 horas

A 1.175 personas les gusta esto.

Ver los 521 comentarios — Ver los 47 contenidos compartidos

Escribe un comentario...

R.I.P. Steve Jobs
R.I.P. Steve Jobs
Me gusta · Comentar · Traducir · Compartir · Hace 9 horas

A 2.624 personas les gusta esto.

Ver los 609 comentarios — Ver los 144 contenidos compartidos

Escribe un comentario...

ACTIVIDAD RECIENTE

R.I.P. Steve Jobs cambió la siguiente información: Información.

R.I.P. Steve Jobs se ha unido a Facebook. · Me gusta · Comentar

Información

R.I.P. Steve Jobs Official Page

A
80.167
personas les gusta esto.

Crear una página
Agregar a los favoritos de mi página
Suscríbete a través de RSS
Reportar página
Compartir

FIG.02. *FACEBOOK PAGE EXPLOITING STEVE JOBS'S DEATH.*

Cyber-crime

Cyber-criminals' goal is to steal information they can turn into cash. This explains why banking Trojans, targeting financial institutions and their customers, are their weapon of choice, although there are also other types of attacks. In January, The Pentagon Federal Credit Union reported the fact that cyber-criminals had used an infected PC to access one of their databases containing confidential customer information. The stolen information included each individual's name, address, social security number and either bank account information or credit/debit card information.

Another frequent strategy is the use of ATMs equipped with duplicate card readers. In January, two men, aged 32 and 31, were sentenced to 7 and 5 years in prison respectively for this type of scam. These two men were suspected to be members of a gang of Russian and American criminals operating all over the U.S.

But it is not only the banking sector that is at risk. After a theft in the Czech Republic and attempted hacking in Austria, the European Commission was forced to suspend trading in CO2 emission credits. Of course as usual, the cyber-criminals were seeking to profit from the attack. There was a similar attack some months ago, when a hacker stole 1.6 million carbon trading credits from the Holcim cement company in Romania. At 15 euros each, that represented losses of some €24 million. These types of attacks, in addition to the financial loss, undermine the entire system.

This diversification is present in other areas as well. This year saw the appearance of a number of variants of the infamous ZeuS banking Trojan aimed at online payment platforms like Webmoney or MoneyBookers.

One of these attacks hit the UK Government, which admitted to having suffered a targeted attack with a ZeuS variant designed to steal not only bank account credentials but also all kinds of personal information.

RSA, the security division of EMC Corporation, announced in mid-March that they had suffered a breach on their network systems that had exposed proprietary information about their two-factor hardware-based authentication system "SecurID".

FIG.03. *RSA WAS ATTACKED IN MARCH.*

In May, Lockheed Martin, the largest provider of IT services to the U.S. government and military, suffered a network intrusion stemming from data stolen pertaining to RSA. It seems that the cyber-thieves managed to compromise the algorithm used by RSA to generate security keys, and the company had to replace the SecurID tokens of more than 40 million customers around the world, including some of the world's biggest companies. Some months later, RSA stated that they were convinced the hackers had been funded by a foreign government and, in October, security analyst Brian Krebs published a list of 760 other victims hit by the same attackers.

In June, the International Monetary Fund said it had been targeted by a sophisticated cyber-attack for months, even though the organization made no public statement about the motivation behind it. The nature of the information stored by the institution would seem to indicate that this was a targeted attack, however, we cannot rule out the possibility that it was just a common case of cyber-crime.

The website of the European Space Agency was also hacked into and a lot of information was stolen and made public. This data included user names, FTP accounts and even FTP login details stored… in plain text files!

Also in May Citigroup revealed that information for more than 360,000 U.S. credit card accounts had been compromised by a website hack. The worst thing about this attack is the fact that the data thieves did not even have to hack a server, but were able to penetrate the bank's defenses and leapfrog between the accounts of different customers simply by inserting various numbers into a string of text located in the browser's address bar.

Japanese video game company Sega also fell victim to a cyber-attack. The company confirmed that information belonging to 1.3 million customers was stolen from its database. Names, birth dates, email addresses and even encrypted passwords for Sega Pass online network were taken. The fact that the passwords were encrypted should minimize the impact of the hacking incident, but only if strong encryption was used, which is not always the case.

Perhaps the most infamous attack occurred this year was the one suffered by Sony. Everything started with the theft of data from their PlayStation Network (PSN), affecting 77 million users worldwide. Not only was this the biggest data theft ever, but the situation was also particularly badly handled by the company. They hid the problem for days, and when they finally made it public they simply said that there was evidence that some user data could have been compromised, even though they knew perfectly well that the situation was far more serious than that..

FIG.04. *DATA FROM 100 MILLION USERS WAS STOLEN IN 2 ATTACKS SUFFERED BY SONY.*

To make things worse, the stolen data was especially sensible, including users' names, billing addresses, email addresses, PSN IDs, passwords (apparently unencrypted), birthdates, purchase history, credit card numbers (from approximately 10% of users), credit card expiration dates, etc.

If this was not sufficient, Sony Online Entertainment was subject to another attack a few days later, a data theft that affected another 24 million users.

In July, Rogelio Hackett, 25, was sentenced to 10 years in prison and a $100,000 fine for stealing 675,000 credit card numbers and related information. The fact that there are tough sentences being handed out is very important as it sends out a strong dissuasive message to criminals: impunity is not as option.

Cyber-crooks continue to use social engineering techniques to deceive users and steal their data, taking advantage of headline-grabbing events such as the untimely death of singer Amy Winehouse or Steve Jobs.

In November, hackers broke into a database with customer information at Steam, the online platform of video gaming firm Valve, stealing information from over 35 million users, including credit card numbers and passwords. Fortunately, this information was encrypted, so the chances of thieves accessing the actual details are slim

One of the key instruments in the fight against cyber-crime is international cooperation. Cyber-crime is transnational and requires a transnational response to tackle it. In this respect, the collaboration agreement signed between the United States' and India's Computer Emergency Response Teams (US-CERT and CERT-In respectively) is very important. The generalization of this type of agreement represents a major step forward in the fight against cyber-crime.

FIG.05. *35 MILLION STEAM USERS HIT BY HACKERS .*

While a lot of data thieves are after money, that is not always the case. Last year we saw a number of celebrities who had personal photos stolen (the most notorious case being that of Scarlet Johansson, whose cell phone pics leaked to the Internet). There was speculation that an organized crime gang could be behind the attacks, but, in reality, everything turned out to be much simpler than it seemed. The culprit turned out to be a 35-year-old unemployed man named Christopher Chaney, who broke into the cell phones of starts by guessing their passwords. Chaney monitored social media sites and other online sources for personal information that would yield clues about potential passwords and, with a bit of patience, gained access to his victims' personal mail accounts. He also had a penchant for beautiful women, as some of his victims included Scarlett Johansson, Jessica Alba, Vanessa Hudgens, Miley Cyrus or Christina Aguilera. Unfortunately, the majority of users also use passwords which are very easy to guess –known as weak passwords-, which are strongly discouraged by security experts..

FIG.06. *CHRISTOPHER CHANEY, 35, STOLE PRIVATE PHOTOS OF OVER 50 HOLLYWOOD CELEBRITIES.*

Cyber-war

Cyber-war has been one of the top buzzwords for 2011. There have been so many cases of cyber-war and cyber-espionage this year that you could write a paper just on them. We live in a time where everybody and everything is connected to the Internet, which presents a world of opportunities for cyber-thieves while authorities and government entities work actively to tackle this problem.

In **January**, we learnt that Canada's Ministry of Economy had been hit with a sophisticated targeted attack. While the investigations seemed to indicate that the attack originated from China, it is actually very difficult to find the culprit. Also, no details have been released about the stolen information.

Back in **February**, U.S. security firm McAfee reported on "Operation Night Dragon", a case in which a number of energy companies had suffered cyber-espionage attacks for at least two years. Later investigations have revealed that the affected companies included the likes of Exxon Mobil, Royal Dutch Shell, BP, Marathon Oil, ConocoPhillips, and Baker Hughes. The attacks came once again from China, even though there is no direct evidence of involvement by Chinese authorities.

In **May**, the Norwegian military stated that it had been the victim of a serious cyber-attack that took place at the end of March. The attack happened when 100 senior military personnel received an email in Norwegian with an attachment. The attached file was in reality a Trojan designed to steal information. At least one person opened the attachment, but the attack was a failure and no data was lost.

At the beginning of **March** it was published that France's Ministry of Economy had been subject to a cyber-attack, linked to China yet again. The aim of this action was to steal information about the G-20 meeting held in Paris in February. Over 150 computers were affected, and other French Ministries also suffered unsuccessful intrusion attempts. Also in March, 40 South Korean government websites fell victim to a denial of service attack. This attack was very similar to one in 2009 and was blamed on North Korea, despite the fact that later investigations linked it to… China.

In **May**, China's defense ministry spokesman, Geng Yansheng, admitted for the first time that they had an elite unit of cyber-warriors in their army. British intelligence stated that the unit had been active for at least 2 years. At the end of the same month, the Pentagon declared that cyber-attacks that originated abroad could qualify as acts of war.

In July, the US Deputy Defense Secretary Bill Lynn revealed that foreign intruders had taken 24,000 files of classified information about a top secret weapon system during an attack suffered in March. Lynn said that a "foreign intelligence service" was most certainly behind the theft of the secret weapon blueprints, but declined to specify which nation had carried out the attack.

FIG.07. *24,000 PENTAGON FILES STOLEN IN MAJOR CYBER-BREACH.*

Some days later, U.S. Marine Corps General James 'Hoss' Cartwright stated that the DoD "was pretty much in the Stone Age".

If something can be said about cyber-war or cyber-espionage attacks is that most of them appear to originate from China. However, on one hand it is obvious that China is not behind every single attack and, on the other, China itself must be suffering attacks from others. One of the differences between a democratic and a non-democratic country is the amount of information they make available to the public. When, for example, the U.S. or a country in the European Union suffers a computer attack, as has happened so many times this year, it becomes public knowledge. However, this is not the case in other countries. Is it that some countries are never attacked? Absolutely not, it is just that they do not make attacks known. And China, for once, has opened to the rest of the world and has admitted that it was hit by nearly 500,000 cyber-attacks last year, about half of which originated from foreign countries.

In **September**, we learned that Japanese company Mitsubishi Heavy Industries had also been hit by a cyber-attack. Almost 100 computers had been compromised, despite the company claiming that no confidential information had been stolen. This company builds highly critical equipment, like guided missiles, rocket engines and nuclear-power equipment. Chinese language was found in one of the viruses used in the cyber-attack, so once again all eyes turned to the Asian giant. Finally, the worst fears became reality some time later, when it was confirmed that hackers had actually gained access to confidential information related to jet fighters and helicopters as well as power plants.

In **October**, it became known that several US Air Force's UAVs (unmanned aerial vehicles) had been infected with malware. After speculation of whether or not this had been a targeted virus attack, it was discovered that the infection was accidental and the drone software was infected through the use of USB drives used to share map updates.

In **December**, the Iranian government published images of a US drone they had captured unharmed. The interesting thing about the incident is that they managed to hack the drone's GPS signal, and landed it in Iran at what the drone thought was its home base in Afghanistan.

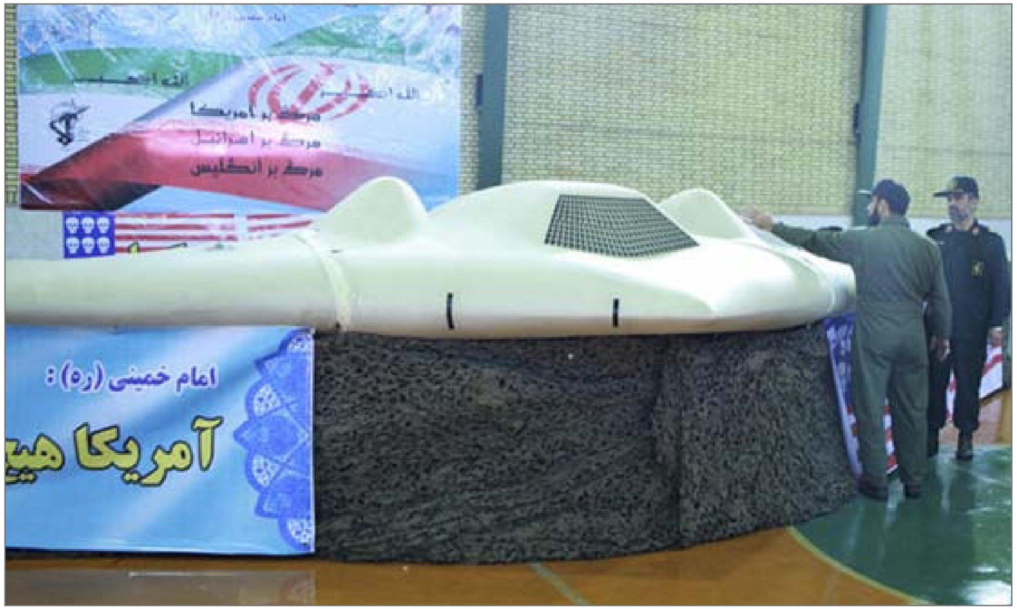


FIG.08. *IRAN HACKS AND CAPTURES U.S.'S DRONE.*

STUXNET

This is the first major cyber warfare attack by a nation state to date. Discovered in July 2010, the malware aimed at sabotaging Iran's nuclear plan. In 2011, new revelations emerged pointing to Israel as the culprit, as Israel Defense Forces Chief of Staff General Gabi Ashkenazi took credit for it in his farewell party.

Also last year, the DEBKAfile website published a report citing "intelligence sources" to claim that the Iranian government had had to replace an estimated 5,000 uranium-enriching centrifuges as a result of the attack, and that since then the country had not been able to return its uranium enrichment efforts to 'normal operation'. In fact, the foreign ministry of Iran acknowledged that they were installing "newer and faster" centrifuges to speed up the uranium enrichment process.

In July, the U.S. Department of Homeland Security said to the Congress that it was aware that a Stuxnet-like virus could be used to attack critical infrastructures in the country. Others have similar fears. Within DHS, many worry that other attackers could use 'increasingly public information' about the worm to launch variants that would target other industrial control systems.

2011 saw the appearance of Duqu, also called "Stuxnet 2.0" and "The Son of Stuxnet", a Trojan horse related to Stuxnet and created to steal information. It spread in Word files attached to emails sent to targeted victims and exploited a 0-day vulnerability for which there was no available patch.

Mac

This year has seen the first large-scale attack on Mac, using rogueware or false antivirus software. Despite thousands of users being affected by the fake antivirus program (called MacDefender), Apple very much tried to bury its head in the sand, denying that any attack ever took place. A few days later, however, they acknowledged it and released a "security update" to protect against the malware. But mere hours after the update, cyber-criminals had already released new variants of the malware, like MacShield, which easily bypassed Apple's security patch. This was rather logical if you consider the fact that the patch was based on 20-year-old technologies, fully obsolete and totally useless unless combined with modern techniques like behavior analysis.

Cyber-criminals are continuing to show increasing interest in targeting the Apple Mac community and have increased the number of attacks on this platform. We have seen the appearance of the first Mac-specific Trojan capable of detecting if it is being run on a virtual machine. This technique is commonly used in Windows-based malware to make detection more difficult, and the fact that it is being used on Mac platforms indicates that criminals are turning their attention to this operating system.

Mobile malware

2011 has been dominated by headlines with news about malware for mobile phones. Additionally, Android is becoming the dominant platform of mobile computing and is likely to win the tablet market shortly.

Cyber-crooks are beginning to realize the existence of an emerging market they are willing to exploit, and are trying new techniques while continuing to use proven strategies, like using malware to get infected phones to send SMS text messages to premium rate numbers

.

At the beginning of the year, a new Android malware took the spotlight. The Trojan –detected as Trj/ADRD.A– stole personal information and sent it to cyber-crooks. One of the most frequent recommendations to combat these threats is to avoid downloading applications from unofficial and questionable places. In this case, the Trojan was distributed from Chinese Android app markets (not from the official store) together with a series of games and wallpapers.

Unlike the iPhone's iOS, the Android OS lets you install applications from anywhere, an aspect cyber-crooks are beginning to exploit. However, this is not the only difference between both operating systems, as applications uploaded to Android's official store (Android Market) are not examined as scrupulously as Apple ones, which has already led to some nasty surprises.

A few days later, another Android Trojan started to spread from China once again. This time, the legitimate apps had been repackaged with malware, thus delivering a nasty present. This Trojan was designed to carry out a number of actions, from sending SMS text messages to visiting Web pages. It could also stop inbound SMS messages.

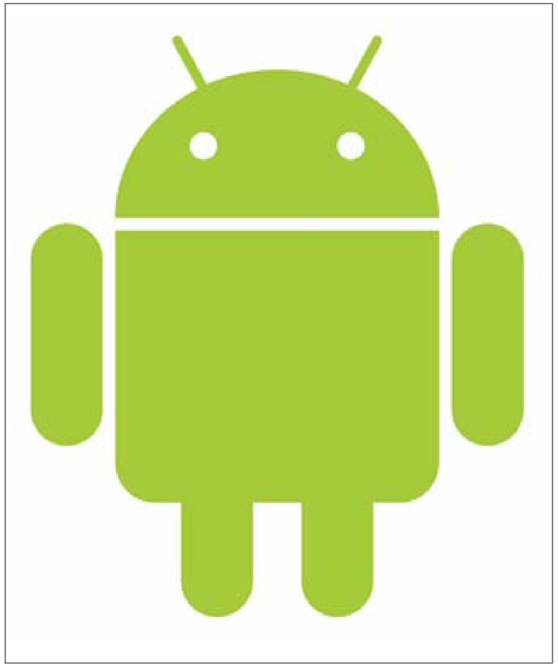


FIG.09. *ANDROID HAS BECOME A FAVORITE TARGET FOR CYBER-CROOKS.*

The beginning of March saw the largest malware attack on Android to date. On this occasion, the malicious applications were available in the official Android Market. In just four days these applications, which installed a Trojan, had racked up over 50,000 downloads. The Trojan in this case was highly sophisticated, not only stealing personal information from cell phones, but also downloading and installing other apps without the user's knowledge.

Google managed to rid its store of all malicious apps, and some days later removed them from users' phones.

The first months of this year saw another major attack engineered by the writers of the infamous Zeus banking Trojan. The attack was designed to bypass the double authentication system implemented by banking institutions for mobile devices. If your PC was infected and you tried to make an online transaction, the bank would display a page (modified by the ZeuS Trojan) prompting you to enter your phone number and model in order to send you a message to install a "security certificate" on your phone. However, this certificate was in reality a Trojan designed to intercept all messages you received.

If this was not enough, we learned that Android has some very basic security holes, as shown by the fact that it stores the passwords for email accounts on the phone's file system in plain text, with no encryption. This makes it an easy target for criminals, who can easily extract all passwords once they have hacked into the device.

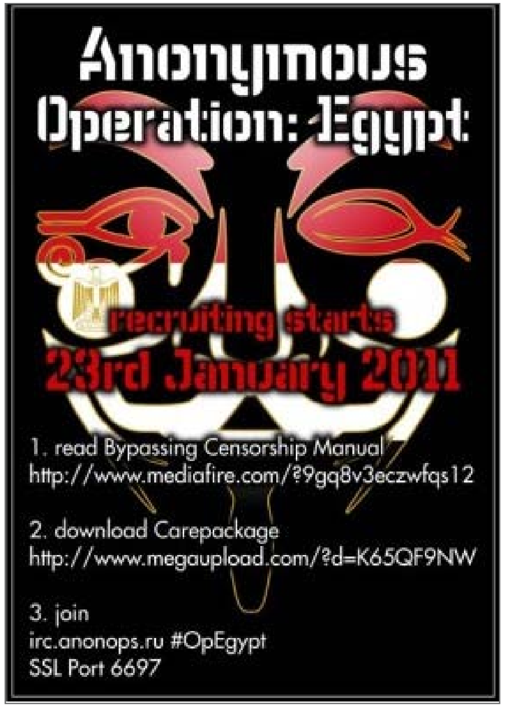
The appearance of new Android malware is becoming increasingly frequent, and the final objective is always the same: to steal users' data. Thus, we have seen malware which not only copies data from the device and sends it to cyber-crooks, but also records phone calls.

In all, Google has removed about 100 malicious applications from its Android Market app store throughout 2011, which has undoubtedly delivered a blow to the confidence of Android users.

Cyber-activism

In 2010 we anticipated that cyber-activism would be one of the major stories in the coming year and our predictions have been confirmed.

In Egypt, the Internet became almost a battlefield between the Egyptian government and protesters, especially on Facebook and Web pages like that of the Anonymous group.



The Egyptian government was so desperate that it took the unprecedented step of shutting down the country's Internet connection and mobile phone network.

Similarly, police in several European countries arrested scores of alleged participants in 2010's cyber-attacks in defense of Wikileaks ("Operation: Payback").

FIG.10. *ANONYMOUS GROUP POSTER ANNOUNCING THEIR CAMPAIGN IN FAVOR OF THE EGYPTIAN PROTESTERS.*

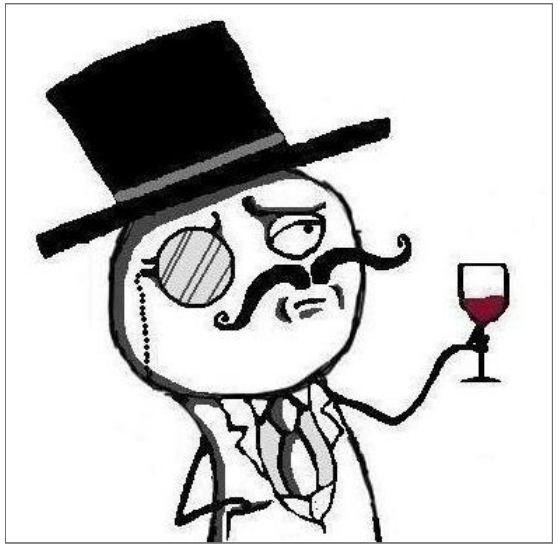
Those arrested were mainly teenagers that used the LOIC tool to take part in the attacks without using any kind of anonymous proxies or virtual private network to cover their tracks. Everything seems to indicate that this was a retaliatory action from governments (Holland, United Kingdom and the USA) wanting to scare off protesters.

Another 'battle' worth mentioning is the one waged between the U.S. security firm HBGary Federal and the Anonymous group. Everything started when Aaron Barr, CEO of the American company, claimed to know the names of the Anonymous group leaders and said he was going to make them public. Anonymous then threatened to hack into the company... and managed to do so in less than an hour. They not only hacked into the company's Web page and Twitter account, but managed to steal thousands of emails that they later on distributed from The Pirate Bay site.

If that were not enough, the content of some of these mails was highly embarrassing for the company, as they brought to light unethical practices (such as the proposal to develop a rootkit) forcing Aaron Barr to stand down.

This was only the tip of the iceberg of a series of criminal activities perpetrated by Anonymous, as it seems that the only way they can protest is by committing illegal acts. However, as stated in previous reports, if the members of the group were smart enough, they would realize that their constant breaking of the law undermines the legitimacy of their protests. Over the last few months they have launched attacks on Sony and the websites of the U.S. Chamber of Commerce, Spain's national police force, several governmental institutions, etc.

Well, if you didn't have enough already of Anonymous, a new hacker collective called LulzSec emerged, whose claimed main motivation is simply 'to have fun by causing mayhem.



LulzSec has specialized in stealing and posting information from companies with poor security (PBS, Fox, etc.), as well as carrying out denial of service attacks (against the CIA website, for example). They also released a full list of user data they had previously stolen such as email addresses, passwords, etc. which has led to account hijacking and other forms of identity theft..

FIG.11. *LULZSEC'S TWITTER PROFILE PICTURE.*

At the end of June, LulzSec teamed up with Anonymous for "Operation: Anti-Security", encouraging supporters to hack into, steal and publish classified government information from any source.

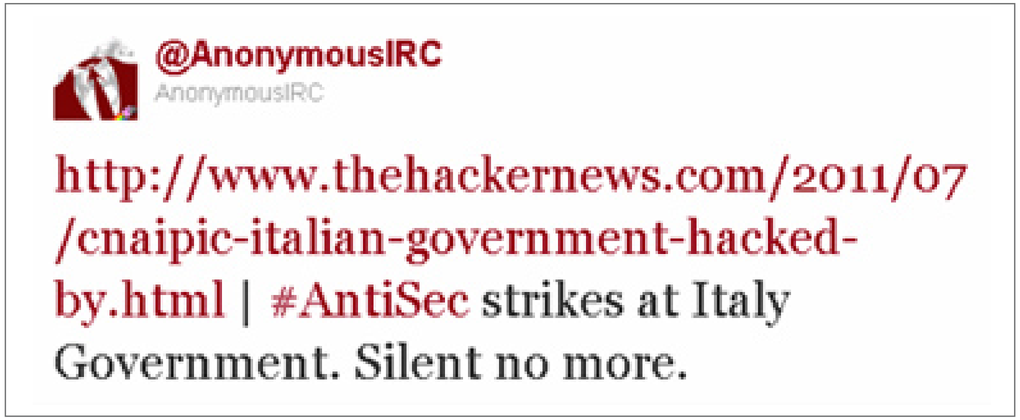
But not everything has been bad news: a significant number of suspected members of the Anonymous group were arrested during 2011.

In the United States, Anonymous went one step further and hacked into the systems of Booz Allen Hamilton (a government contractor with strong ties to the US Department of Defense – DoD), stealing 90,000 military email addresses and passwords. They managed to enter the system through an outdated server with no antivirus protection at all.

Soon after these attacks, the FBI arrested 16 Anonymous members in the US. All of these people could face 5 to 10 years in jail if found guilty.

However, none of these actions seem to have stopped Anonymous, who actually seems to have redoubled its efforts. Just days after the arrests, Anonymous posted links to two NATO confidential documents, and claimed to have one more gigabyte of confidential data which they refused to publish as it would be "irresponsible".

Meanwhile, Anonymous stroke once again in Europe, stealing over 8 gigabytes of data from Italy's CNAIPIC (National Center for Computer Crime and the Protection of Critical Infrastructure).



@AnonymousIRC
AnonymousIRC

http://www.thehackernews.com/2011/07/cnaipic-italian-government-hacked-by.html | #AntiSec strikes at Italy Government. Silent no more.

FIG.12. *MESSAGE POSTED BY ANONYMOUS, BOASTING OF THEIR LATEST ATTACK.*

In addition, they released the stolen personal data of thousands of U.S. law enforcement officers, including their email addresses, user names, passwords and in some cases even their social security numbers. And they did it again a few weeks later, as they exposed personal data of San Francisco-area subway police officers. But, if this was not enough, the group hacked yet another U.S. Department of Defense contractor (this time Vanguard Defense Industries), stealing 1 gigabyte of data such as emails and confidential documents from one of the company's top executives.

At the end of the year, Anonymous hacked thousands of credit card numbers and other personal information belonging to customers of the U.S.-based security think tank Stratfor to donate to charity. They also published a small slice of the 200 gigabytes of data that they claimed to have stolen. The list of Stratfor's customers includes entities ranging from Apple Inc. to the U.S. Air Force, which gives an idea of the seriousness of the attack.

03| Malware figures in 2011

26 million new malware samples have been identified in 2011, some 73,000 strains per day; quite a frightening number, the highest ever. This could pretty much sum up the malware situation in 2011, however, let's look beyond the numbers to know exactly what is happening. Firstly, let's take a look at the type of malware created in the last 12 months:

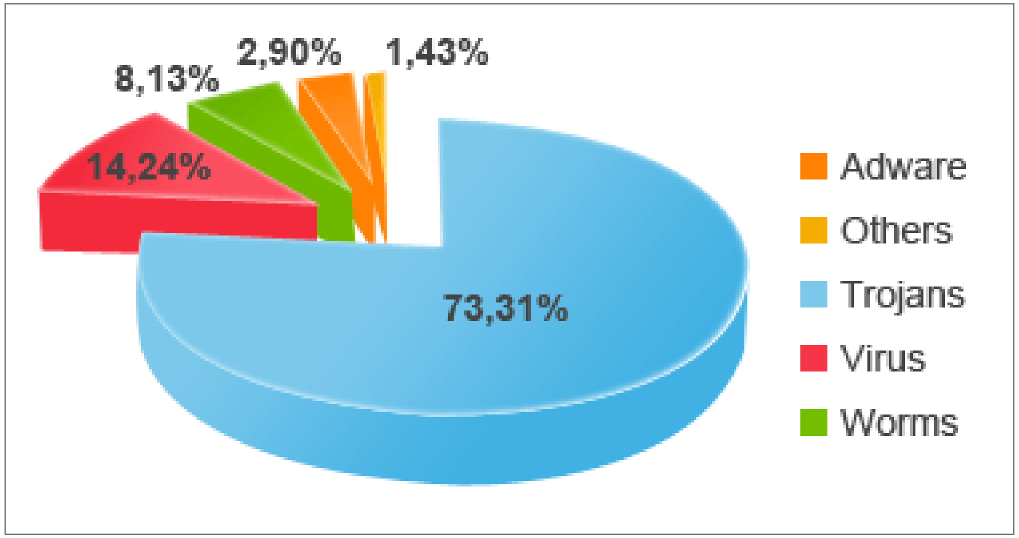


FIG.12. *NEW MALWARE CREATED IN 2011, BY TYPE .*

Trojans continued to account for most of the new threats, growing spectacularly. In 2009, Trojans made up 60 percent of all malware, whereas the percentage dropped to 56 percent in 2010. This year they have jumped up to 73 percent, so that nearly three out of every four new malware strains created in 2011 were Trojans. All other malware categories have lost ground with respect to Trojans, once again the weapon of choice for cyber-crooks' intrusion and data theft efforts.

As for the number of infections caused by each malware category, it is worth remembering that Trojans cannot replicate automatically, so they are less capable of triggering massive infections than viruses or worms, which can infect a large number of PCs by themselves. The graph below shows the distribution of malware infections this year.

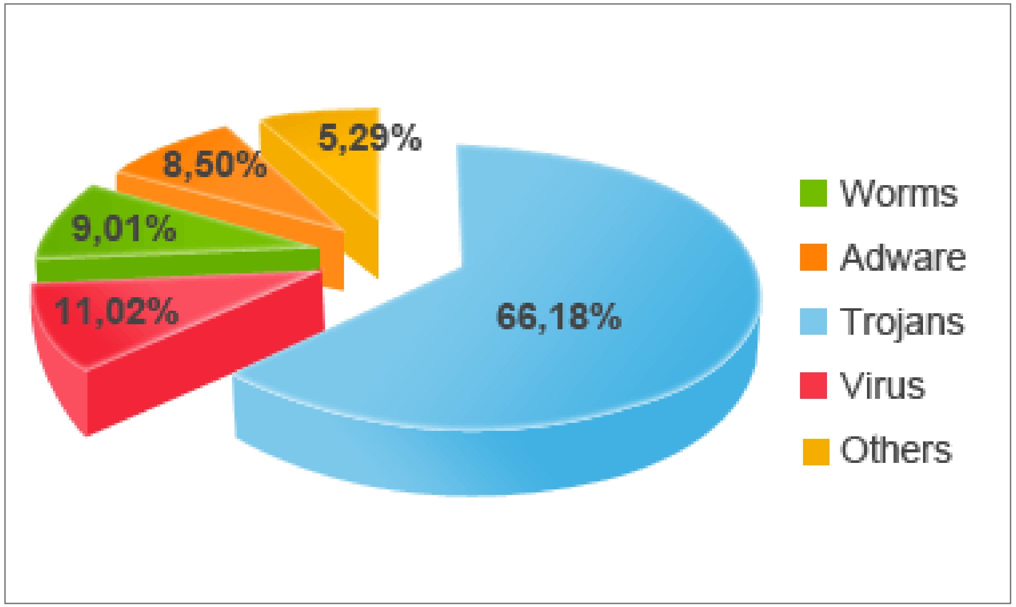


FIG.13. *MALWARE INFECTIONS BY TYPE IN 2011.*

As you can see, there is not a big difference between the different types of malware created and the infections caused by each of them, with one exception: the percentage of computers infected by adware/spyware almost triples the percentage of new adware/spyware strains created.

What is the reason for this 'anomaly'? This category includes fake antivirus software or rogueware: applications created by cyber-crooks that try to pass themselves off as legitimate software applications in order to trick users by falsely informing them that their computers are infected, and prompting them to buy a program to disinfect them.

Rogueware is ideal for cyber-criminals, who no longer need to steal users' information to make their money; instead, users part with their cash voluntarily. This is why computer criminals are spreading rogueware to as many people and as quickly as possible. The more infections, the more profit.

Let's look at the geographic distribution of infections. Which countries are most infected? Which countries are best protected? The average number of infected PCs across the globe stands at 38.49 percent, with the most infected country being China (60.57 percent of infected PCs), followed by Thailand (56.16 percent) and Taiwan (52.82 percent). These are the only countries that exceed 50 percent of infections. The graph below shows the 10 countries with the highest malware infection rates in 2011.

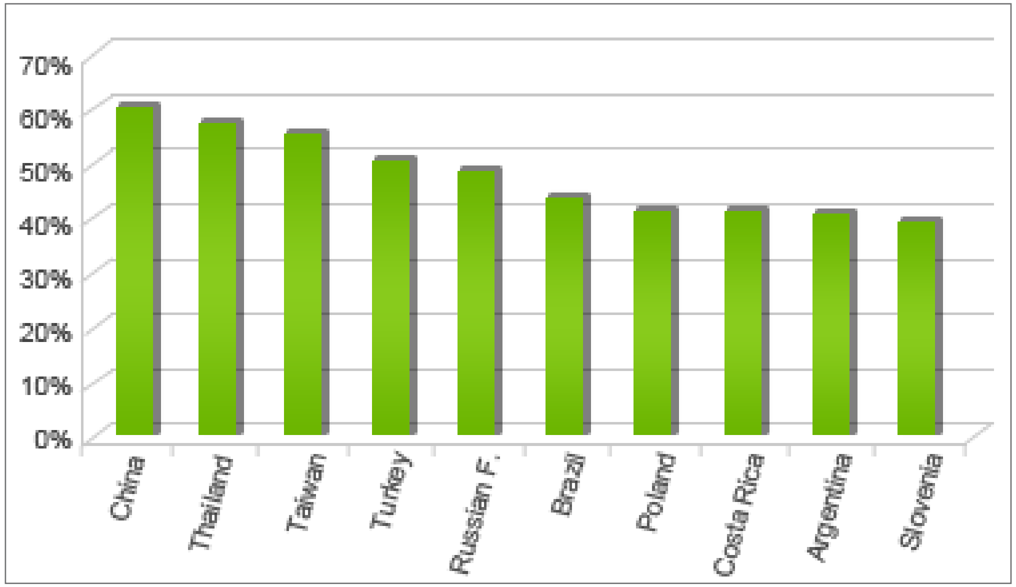


FIG.14. *COUNTRIES WITH THE HIGHEST MALWARE INFECTION RATES.*

As the table shows, there are high-infection countries in almost every continent. The U.S. barely escaped the list, as they ranked 11th with slightly more than 39 percent of its PCs infected, also above world average.

The list of least malware infected nations is topped by European countries, with the exception of Australia and Japan. Sweden came in lowest with only 24 percent of its PCs attacked by malware.

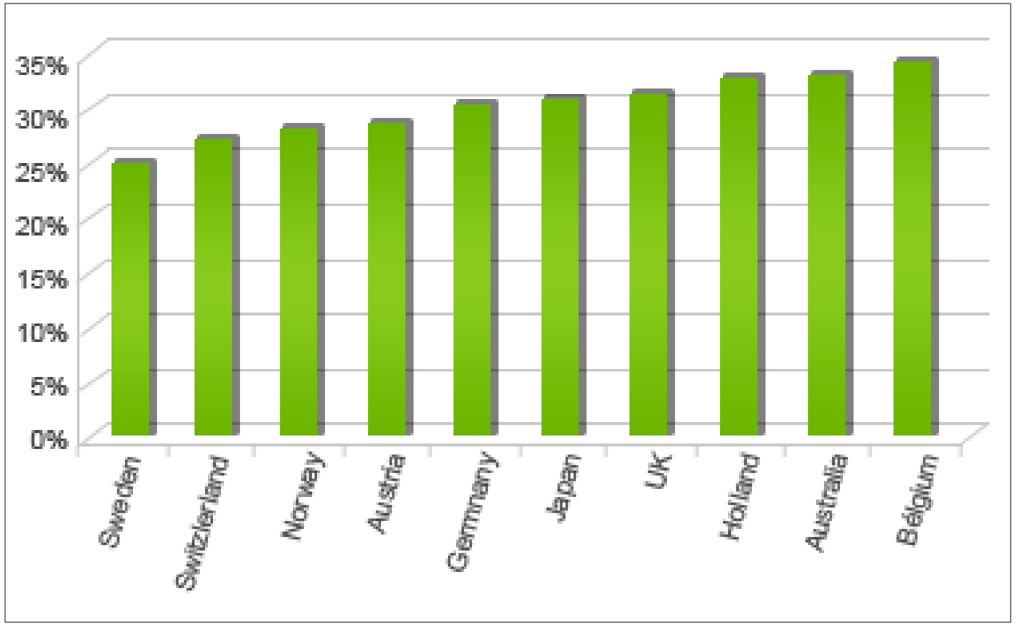


FIG.15. *LEAST MALWARE INFECTED COUNTRIES.*

04| 2012 Security Trends

We have seen what has happened in 2011: malware creation record, highest number of Trojans ever, attacks in social networks, cyber-crime and cyber-war everywhere. What do we have to expect for the next 12 months?

Social networks

Social engineering techniques exploiting users' weaknesses have become the leading attack method in social networks. Trending topics such as the Olympics or the next US Presidential elections will be used as a bait. Cybercriminals will continue to target social media sites to steal personal data.

Malware increase

In the past few years, the number of malware threats has grown exponentially, and everything seems to indicate that the trend will continue in 2012. In fact, malware is the weapon use by cybercriminals to carry on their attacks.

Troyans

they are cyber-crooks' weapon of choice for their attacks, as shown by the fact that three out of every four new malware strains created in 2011 were Trojans, designed to sit silently on users' computers and steal their information.

Cyberwar

or maybe it is more accurate to say cyberespionage. 2011 has been the year with most intrusions ever aimed at companies and government agencies. From New Zealand to Canada, from Japan to the European Parliament, there have been countless attacks aimed at stealing secret or classified information. We live in a world where all the information is in digital form, so modern-day spies no longer need to infiltrate a building to steal information. As long as they have the necessary computer skills, they can wreak havoc and access the best-kept secrets of organizations without ever leaving their living-rooms. In 2012 we will see these kind of attacks even more.

Mac malware

As the market share of Mac users continues to grow, the number of threats will grow. Fortunately enough, it seems that Mac users are now more aware that Mac is not immune to malware attacks and they are increasingly using antivirus programs, hindering cyber-crooks. The number of malware specimens for Mac will continue to grow in 2012, although much less than for PCs.

Mobile malware

Over ten years ago, antivirus companies started making dire predictions of a mobile malware epidemic. Years later, as the situation was not as apocalyptic as predicted, they started claiming that the installation of antivirus software on mobile phones had prevented the catastrophe. Well, they were wrong again. If having an antivirus solution were enough to solve all types of malware problems, the world would be a happier place. Unfortunately though, both users and security vendors alike are in the hands of cyber-crooks, who are the ones who decide which platform to target. In this context, last year PandaLabs predicted a surge in cyber attacks on mobile phones, and the fact that Android has become the number one mobile target for cyber-crooks in 2011 confirms that prediction. In 2012 there will be new attacks on Android, but it will not be on a massive scale. New mobile payment methods –via NFC for example– could become the next big target for Trojans but, as always, this will largely depend on their popularity.

Malware for tablets

The fact that tablets share the same operating system as smartphones means that they will be soon targeted by the same malware as those platforms. In addition, tablets might draw a special interest from cyber-crooks as people are using them for an increasing number of activities and they are more likely to store sensitive data than, say, a smartphone.

Cybercriminals targeting small to medium-sized companies

Why do cybercriminals target online banking customers instead of directly attacking banking institutions to steal money? The answer to this question has to do with the cost-benefit ratio of the attack: Financial entities are usually very well protected, and the chance of launching a successful attack is remote and very costly. However, attacking their customers to steal their identity and impersonate them is much simpler. The security of small to medium-sized companies is not that strong, and this makes them very attractive for cyberthieves, who can steal data from hundreds or thousands of users in one go. On many occasions, small to medium-sized companies do not have dedicated security teams, which makes them much more vulnerable.

Windows 8

The next version of Microsoft's popular operating system is scheduled for November 2012, so even though it is not supposed to have much on an impact on the malware landscape in the coming year, it will surely offer cyber-crooks new opportunities to create malicious software. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smartphones) running Windows 8, so it will be possible to develop malicious applications like those for Android. This, in any event, will probably not take place until 2013.

05| Conclusion

Last year we finished our report by commenting on the bleak future that laid ahead for the security sector in 2011. Unfortunately we were right, and cyber-attacks and data theft have dominated headlines all through the year. We do not want to be pessimistic, but 2012 does not look much better.

Cyber-espionage and social networking attacks will be the predominant threats to safeguard against this year. The rise of social media, which has increased communication between people all over the world, has its own disadvantages too. Cyber-thieves can infect and steal data from thousands or millions of users in one go. You no longer need to be a computer whiz to gain control of a system or edit malicious code to generate new malware strains.

The growing number of Internet users means there is no shortage of potential victims. Cyber –criminals are just like pickpockets in a busy city square during the Christmas shopping season. The problem is that today the number of cities and squares (platforms, social networking sites, cell phones, tablet computers, etc.) has multiplied and they are busier than ever, leaving you with more chances of exposing your wallet and its contents (credit cards, photos, money) to thieves. There are more potential victims for more pickpockets.

But this rather bleak outlook should not stop you from enjoying the benefits of the Internet: online banking and shopping, instant communication with friends and relatives all around the world, the ability to read books on your phone or tablet… You just need to take a few precautions.

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/**

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