QUARTERLY REPORT PandaLabs (JANUARY-MARCH 2011)

PANDA SECURITY

Index

Introduction

Q1 of 2011 is already behind us and the security landscape has evolved as expected. We have seen a number of attacks on cell phones and Facebook remains the king of all social networking sites, which has turned it into a lucrative draw for cyber-crooks aiming to trick users.

Additionally, some international events –like the civic rebellions sweeping across Northern Africa– have been largely reflected in the cyber-activism and security worlds. This first quarter has also seen cyber war and cyber-espionage in the spotlight, with China as the usual suspect in most cases

Cell Phone Malware

The first quarter of 2011 has been dominated by headlines with news about malware for cell phones. This could be for several reasons: firstly, smartphones exceeded PC sales in Q4 of 2010 for the first time ever. Secondly, Android is becoming the dominant platform of mobile computing and is likely to win the tablet market shortly. Additionally, there is increasing concern about cell phone security, and research studies and proof-of-concepts reporting security problems have multiplied over the last few months.

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.

A group of Russian cyber-criminals took advantage of Saint Valentine's Day to distribute an application that supposedly let users send romantic photos to their partners via MMS. The application offered a number of images that users could send to their loved ones, but actually sent SMS text messages to a premium rate number without the owner knowing.

Almost simultaneously, a new Android malware took the spotlight. The Trojan –detected as Trj/ADRD.A– stole personal information and sent it to cyber-crooks.

FIG.01
ST . VALENTINE´S DAY PICTURES USED BY CELL PHONE TROJAN.

FIG.02
ST . VALENTINE´S DAY PICTURES USED BY CELL PHONE TROJAN.

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 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 apps had been repackaged with the 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.

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, the infected applications had

been downloaded more than 50,000 times. This was a highly advanced Trojan, as it not only stole confidential information but could also download and install other applications without user knowledge. Google withdrawn all malware-infected apps from its store, and a few days later removed them from users' devices remotely.

In just 4 days the infected applications had been downloaded more than 50,000times.

This quarter has seen 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. This is actually the second variant of this malware strain. We already referred to a similar specimen in last year's report.

Malware on Facebook

As Facebook continues to be the most popular social networking site, cyber-criminals keep doing their best to exploit it in every imaginable way. We have seen a plethora of Facebook applications that post enticing messages on compromised accounts which, once clicked upon, prompt victims to install an application and take a survey to get a chance to win some kind of prize. This way, cyber-crooks obtain significant financial benefits and sometimes even phone numbers which they use to subscribe the unsuspecting victims to a premium rate service.

However, not all Facebook attacks are based on malware. As we have explained on a number of occasions, users sometimes give out too much personal information on social networking sites, which facilitates hacking their email and Facebook accounts. George S. Bronk has been recently **arrested in California** for these illegal activities. He used the information he found on Facebook to gain control of victims' email accounts. Once he had "kidnapped" the account, he looked for personal information he could use to blackmail the targeted user.

And it seems that anybody can actually become a victim of these attacks, as Facebook founder **Mark Zuckerberg** himself has seen his Facebook account hacked and defaced with a message saying "***Let the hacking begin***".

FIG.03

MARK ZUCKERBERG´S HACKED FACEBOOK PAGE.

Banking Malware

The term 'banking malware' normally refers to the many Trojans designed to infect online banking customers and steal their login credentials to access their bank accounts. However, not all attacks work like this. 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 respective for this type of scam. These two men are suspected to be members of a gang of Russian and American criminals operating all over the country.

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 Comission 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 represents 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 quarter 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.

Going back to Stuxnet

If you thought you already knew everything there is to know about Stuxnet, the worm designed to sabotage the Iranian nuclear program, you were wrong. Although there is still a lot more to be known about this case, new revelations have emerged about the infamous attack. Reports have appeared pointing to the USA and Israel as the culprits, although there is no solid evidence for that. However, it is with surprise that we have heard that General Gabi Ashkenazi, the Israeli Army chief of staff, took credit for the Stuxnet attack in his farewell party...

The Israeli Army chief, General Gabi Ashkenazi, took credit for the Stuxnet attack in his farewell party.

Additionally, it has finally been revealed that Stuxnet hit its goal. Russian nuclear scientists have raised serious concerns about the extensive damage caused to Busher's nuclear power plant, and have tried to convince the Iranian government to delay its nuclear program until the end of the year. Finally, the reactor startup –scheduled for the end of January–, has been postponed.

Cyber-activism

When we published our malware trends forecast for 2011 and mentioned that cyber-activism was likely to take the spotlight this year, we could not imagine that it would do so so quickly. Even though this has been a consequence of the political revolts in Northern Africa, there is no denying that social media and the Internet have played an important part in the recent events.

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

FIG.04

ANONYMOUS GROUP POSTER ANNOUNCING THEIR CAMPAIGN IN FAVOR OF THE EGYPTÍAN PROTESTERS

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 have arrested scores of alleged participants in last year's cyber-attacks in defense of Wikileaks ("Operation: Payback"). 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 is 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.

But not only this, the contents of some of these messages have turned to be highly compromising for the U.S. company, as they have revealed a number of morally dubious practices (like a rootkit development proposal). As a result, the company was put in such a delicate situation that Aaron Barr was forced to resign.

Cyber war

Appart from Stuxnet, there is an increasing number of examples of cyber war (and cyber espionage).

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.

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 had been affected, and other French Ministries had also suffered unsuccessful intrusion attempts.

Frence´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.

Also in March, 40 South Korean government websites fell victim to a denial of service attack. This attack was very similar to another one that took place in 2009 and was blamed on North Korea, despite the fact that later investigations linked it to … China.

FIG.05

CYBER-WAR IS HERE

Our first quarterly report of 2011 has confirmed the huge amount of malware in circulation today. And even though this is starting to sound a bit repetitive by now, it is just plain reality.

PandaLabs has found an important increase in the number of new threats received at the laboratory every day: from 55,000 just a few months ago, to 63,000 at the end of last year and an average of 73,190 so far in 2011. That is, a 16 percent growth compared to Q4 last year.

All these figures refer to confirmed malware strains, that is, samples already analyzed by Collective Intelligence -our proprietary system for automated and enhanced malware collection, classification and remediation-, or by our lab technicians. In other words, in Q1 this year we have received an average of 195,463 files to analyze every day, 37.4% of which were new threats.

Overall, Trojans remain the most popular threat to computer systems, accounting for 70 percent of all new malware.

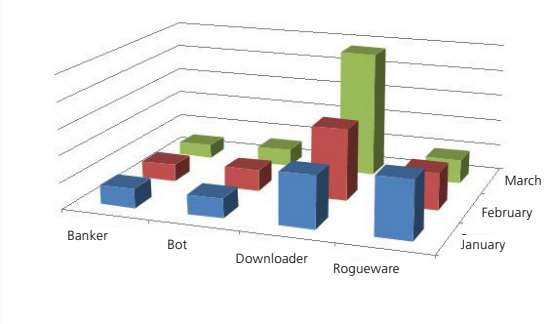


FIG.06

THE NUMBER OF DOWNLOADERS HAS INCREASED SIGNIFICANTLY IN THE 1st QUARTER

However, not all kind of Trojans have grown at the same pace. When investigating the subtypes of malware, PandaLabs found that banker Trojans have remained steady, whereas bots and fake antivirus or rogueware have decreased in popularity.
Contrary to this, the number of downloaders has risen significantly, which undoubtedly explains the increase in malware this year.

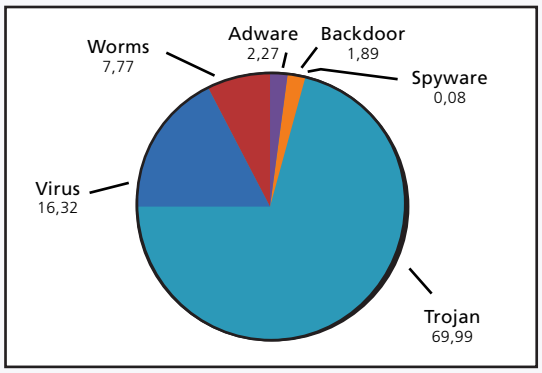


FIG.07

TYPE OF MALWARE

Downloaders are a particularly nasty type of Trojans that, once they have infected a user's computer, connect to the Internet to download additional malware. Hackers often use this method because downloaders are lightweight –only containing a few lines of code– and can go completely unnoticed unlike other Trojans.

As for the least frequent malware categories, it is interesting to note that cyber-criminals are still creating large numbers of dialers mostly for developing countries (technologically speaking), where users still connect to the Internet by using a modem.

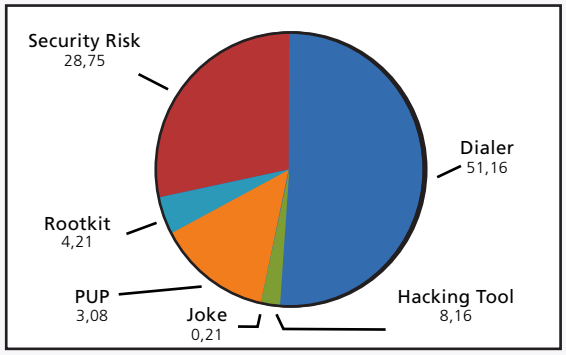


FIG.08

REST OF MALWARE TYPES

Most infected countries in Q1

There have been very few surprises with regard to the ranking of most infected countries in the first quarter of the year. The only thing worth mentioning is the fact that countries in the middle of the list still show infection levels of 50 percent or higher (even 70 percent in countries like China, Thailand or Japan).

This data has been obtained from users of Panda ActiveScan 2.0, our free online scanner. This tool keeps statistics of how many PCs worldwide are infected with some type of computer threat.

This quarter we have seen the U.S. disappear from the Top 20 list of countries most affected by malware infections, whereas countries like France or Spain have re-entered it. The same can be said about Ireland, a country missing in previous lists that is now occupying one of the last places.

Peru and Ecuador close the list with infection levels between 30 and 40 percent, which nevertheless represents an improvement compared to previous rankings.

Finally, Trojans are the type of malware causing most computer infections in some specific countries, followed by traditional viruses and worms.

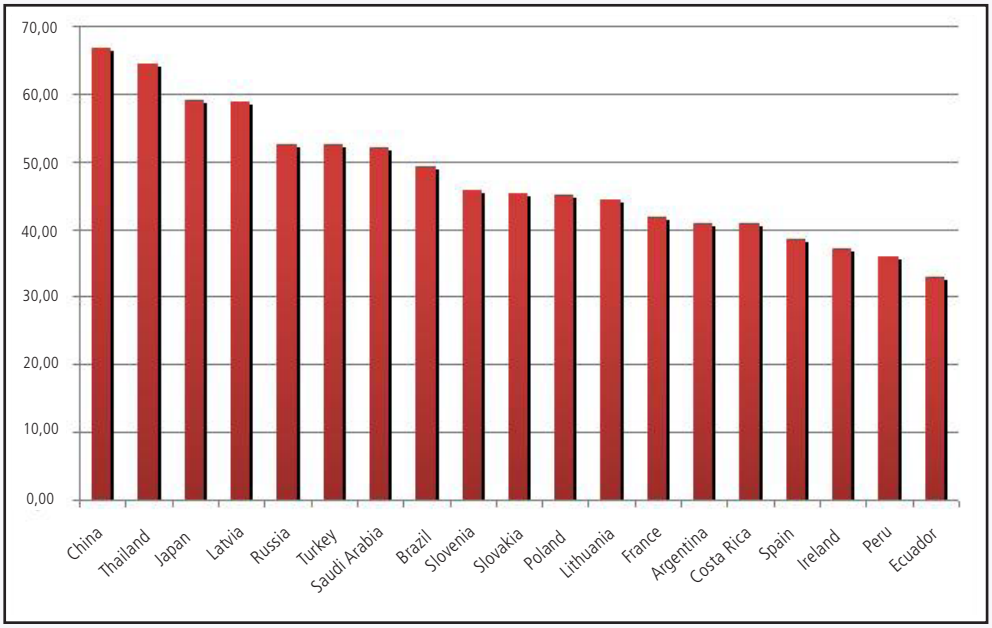
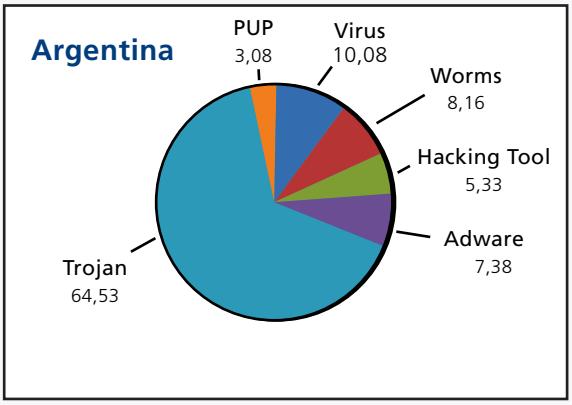
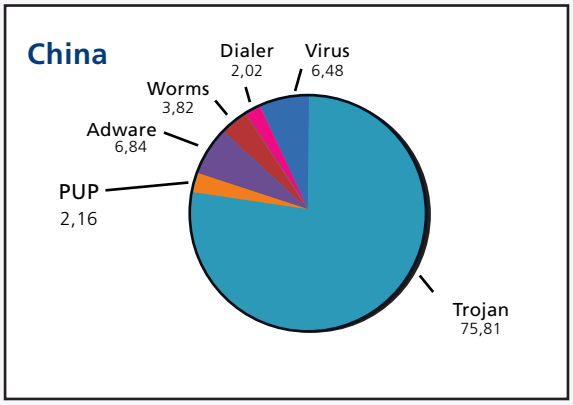
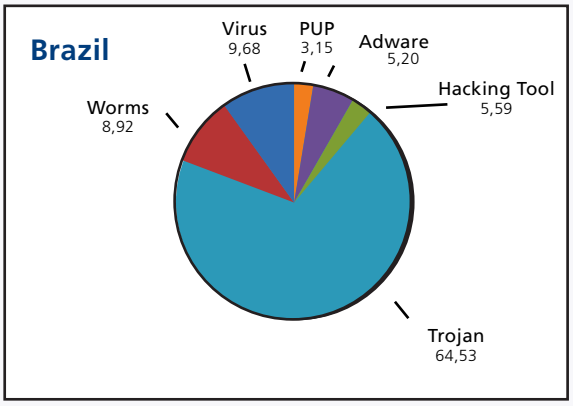


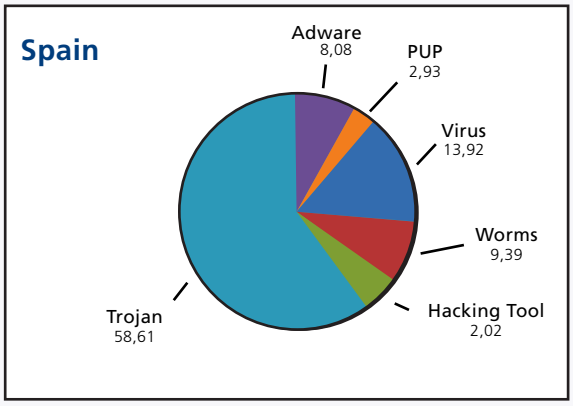
FIG.09

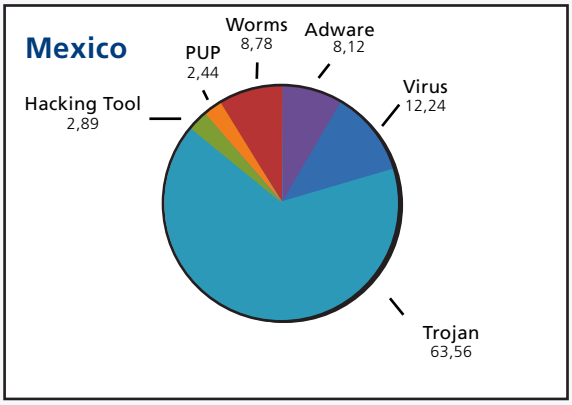
INFECTION RATE PER COUNTRY











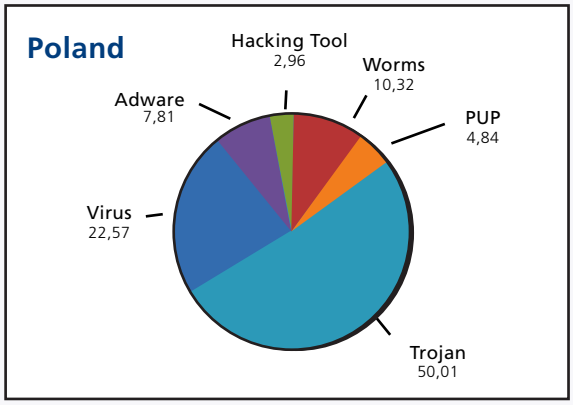


FIG.10

TYPE OF MALWARE PER COUNTRY

This quarter's vulnerability summary deals with the PWN2OWN contest organized by the ZeroDay Initiative [1] team at security researches TippingPoint.

The name 'WN2OWN' means pwn (= hack) to own (you can go home with one). In other words, contestants are challenged to exploit specific software, and winners receive the device/computer that was successfully exploited and a $15,000 cash prize, besides the obvious recognition and quite possibly, an exciting job offer.

All the operating systems and applications used in the contest are fully patched.

The 2011 contest took place in Vancouver between March 9 until 11 during the annual CanSecWest [2] security conference.

The contest began in 2007 and brings together the best vulnerability researchers, who try to get past the latest security protections in the most important operating systems and mobile devices. Actually, all the operating systems and applications used in the contest are fully patched. It is quite usual that a few days prior to the competition, vendors release their latest fixes and security patches to prevent their products from being hacked.

Apple was the first to fall on the first day of the contest. VUPEN researches took advantage of a security flaw in the latest version of Safari's WebKit [3] engine to bypass the ASLR [4] and DEP [5] protection in the 64-bit version of a fully patched MacOSX Snow Leopard. Consequently, the contestant winners received the $15,000 cash prize and an Apple MacBooc Air for the two weeks spent to find the vulnerability and to write the exploit. After this, many Apple users started complaining on Internet forums about Apple's lack of commitment towards operating system and application hardening, as their system has also been the easiest to exploit in past editions of the contest. We can imagine that Apple users will be looking forward to seeing what happens next year with Lion, the new Mac operating system, and see it if eventually takes out its claws and manages to leave the contest unharmed for the first time ever.

The second system to go down was Internet Explorer 8 (32-bit) running on a Windows 7 computer with Service Pack 1. It took Stephen Fewer, a security researcher at Harmony Security, almost a month and a half to prepare an advanced exploit that took advantage of three vulnerabilities to compromise it. Stephen exploited two flaws to run code on the browser and then one more to bypass Internet Explorer Protected Mode.

Day two pitted the mobile devices against hackers. Apple fell to attackers again as the iPhone 4 was quickly hacked by the famed security expert and former NSA employee Charlie Miller. Miller had also developed a functional exploit for MacOS X, but the VUPEN researchers were faster than him. Charlie Miller has already proven in this competition that he can break into all Apple operating system and mobile devices. Nevertheless, the researcher has acknowledged that preparing a functional exploit for IOS version 4.3, the new operating system for the iPhone 4 and iPad, will be much more difficult due to ASLR implementation. ASLR has been developed together with DEP to prevent successful exploits and arbitrary code execution vulnerabilities, as previously mentioned in one of our past quarterly reports. It is interesting to note that Charlie Miller took advantage of a vulnerability found on the mobile version of the Safari browser, managing to access confidential information stored on the phone.

RIM's Blackberry OS 6 was also hacked into. Once again, a vulnerability in the WebKit engine (used by Google for Android, and by Apple for IOS and MacOSX) was exploited in the attack. Unlike the iPhone, Blackberry devices include ASLR and DEP protection in their operating system, but this protection was not good enough for security researchers, who managed to compromise them and access their confidential information.

We can conclude that security and software vendors are making major efforts to enhance the security of their operating systems and applications in order to better protect customers.

The implementation of DEP and ASLR has been a major advancement in the prevention of vulnerability exploitation and code injection attacks. Nevertheless, there is still a long way to go as shown by the PWN2OWN contest. Initiatives like this are very positive for software vendors to gain insight into their products' weaknesses and realize the need to invest in security.

Panda Security provides you with the necessary products and tecnologies to protect your system.

In any event, it is important to remember that security's weakest link is people. Only a few months ago, many Android users became infected with malicious software when downloading certain applications from a dubious site. There was no need to exploit any vulnerabilities to perform this kind of attack, as sometimes it is just enough to trick users into visiting an infected Web page, etc. That is, it is not only companies that must tighten security measures, but users must also be cautious when downloading files online.

As we have already said on other occasions, a fully patched operating system is not enough. Other technologies and applications must come into play to combat intrusions and system infection. No matter if you are a Microsoft Windows or Apple MacOSX user, Panda Security provides you with the necessary products and technologies to protect your system.

1 http://zdi.tippingpoint.com/
2 http://cansecwest.com/
3 http://www.webkit.org/
4 http://en.wikipedia.org/wiki/Address_space_layout_randomization
5 http://en.wikipedia.org/wiki/Data_Execution_Prevention

Cyber-activism and Cyber War

The 3rd Security Blogger Summit, held in February in Madrid, focused on cyber-activism and cyber-war as well as on the new dangers posed to users and institutions on the Internet. The roundtable discussion centered around the most recent examples of these emerging phenomenons, international cooperation and the limits to these activities on the Web. The discussion also centered on the new trends for 2011 and the legal framework against this type of Web activity.

This year, the meeting organized by Panda Security, has placed itself among one of the main events for bloggers worldwide as shown by the more than 300 technology and computer security experts and bloggers that attended it.

The Summit gathered an impressive line-up of renowned speakers and journalists such as Enrique Dans, Chema Alonso and Rubén Santamarta, as well as Elinor Mills and Bob McMillan, two of the most prominent IT security journalists from the US. All of them coincided in underlining the importance of these coordinated worldwide attacks on international institutions.

Cyber-activism: Internet protests and demonstrations

The 3rd Security Blogger Summit kicked off with a keynote by Enrique Dans, well-known blogger and professor at the IE Business School, which focused on the part played by cyber-activism in recent revolts like those in Iran, Tunisia or Egypt. He also insisted in the concept that social media have taken down the barriers of activism as "You can retweet a message and believe you're already part of a cyber-activist movement."

As for recent events regarding WikiLeaks and Web attacks in defense of Julian Assange, Enrique Dans explained that "There is no way to stop a phenomenon like WikiLeak. In the future anybody will be able to disclose relevant information from a website, as contaminated as this might be."

Bob McMillan, a San Francisco-based computer security journalist explained that, in his opinion, "WikiLeaks is as important as The New York Times". "WikiLeaks has helped those who wanted to expose sensible information, and to think of changing the legislation in the wake of a denial of service attack like those in the "Operation Avenge Assange" is very difficult, even though these examples of cyber-activism may seem legitimate to you".

During the course of the debate moderated by Josu Franco, Corporate Strategy Director at **Panda Security**, Elinor Mills, senior writer at CNET News on security issues with over 20 years of experience in the security field indicated that "People have replaced neighbor meetings with Internet-based tools".

WikiLeaks has helped those who wanted to expose information, and to think of changing the legislation.

Chema Alonso, a URJC University Computer Engineer, postgraduate in Information Systems and author of the blog "*Un Informático en el Lado del Mal*", added that "Technical evolution has changed the way people express themselves and now it is no longer necessary to gather 3 million people to attract some attention". Rubén Santamarta, an IT researcher with over 10 years of experience in the reverse engineering and IT security fields, indicated that "Cyber-activism was born from the global situation we live in".

When asked by the audience, Santamarta questioned the legality of cyber-activism vs. the apparent legitimacy of the initiatives behind it. "Users want honesty, and that's the key of WikiLeaks". "The worrying aspect is the lack of reaction from governments throughout the world after all the information disclosed by WikiLeaks", said Enrique Dans.

Cyber-war: Reality versus sensationalism

The Summit participants discussed some of the most relevant examples of cyber-war, such as the alleged attacks targeting Iran's nuclear plants using the Stuxnet Trojan, as well as Operation Aurora, concerning attacks on Google from China in order to steal corporate secrets.

Elinor Mills and Bob McMillan coincided in pointing out that the term 'cyber-war' was 'too exaggerated' for the actual events talking place. "We still do not know the real dimensions of cyber-war and it is easy to confuse it with espionage or even cyber-crime" explained Elinor Mills. Bob McMillan added that "Even though Stuxnet has been used as a cyber-weapon, that does not mean that we are already knee deep in a cyber-war. If there really was a cyber-war, it would be on a global scale, as the two Great Wars of the 20th century."

Rubén Santamarta however insisted on the idea that the cyber-war phenomenon is at its early stages and it will probable become a reality in 10 years' time. "We are talking about a war without an army. It is a fourth-generation war where it is possible to damage a country without having to invade it with soldiers. A country can have another one under control through the Internet even before they have declared war on each other."

Santamarta also expressed his hope that "Not everybody is willing to launch attacks such as these". Finally, Chema Alonso stated that "Fortunately at present, the people that can do such a thing are very few and must be extremely knowledgeable".

FIG11

SECURITY BLOGGER SUMMIT ROUND TABLE

In this quarter we have released an investigative report on the current cyber-crime black market. We discovered a vast network selling stolen bank details along with other types of products in forums and more than 50 dedicated online stores. This is a rapidly growing industry and cyber-criminals are aiding and abetting each other's efforts to steal personal information for financial profit. After posing as a cyber-criminal to infiltrate the network, we made some alarming discoveries which are available in the full report here: **http://press.pandasecurity.com/press-roomreports/#monographs**

The cyber-crime black market, which has traditionally centered on distributing bank and credit card details stolen from users around the world, diversified its business model in 2010, and now sells a much broader range of hacked confidential information including bank credentials, log-ins, passwords, fake credit cards and more. But as openly available as this information is, PandaLabs discovered that it can only be accessed by personally contacting the hackers who are promoting their information for sale on forums and in chat rooms.

Making the Sale

By having access to bank credentials, criminals can easily defraud any bank or credit card account long before the hack is discovered. Alarmingly, this data can be purchased for as little as $2 per card, but this level does not provide additional information or verification of the account balance available. If the buyer wants a guarantee for the available credit line or bank balance, the price increases to $80 for smaller bank balances and upwards of $700 to access accounts with a guaranteed balance of $82,000.

Prices are higher if the accounts have a history of online shopping or use payment platforms such as PayPal. For a simple account without a guaranteed balance, PandaLabs found prices starting at $10 and increasing to $1,500 depending on the platform and the guarantee of available funds. Similarly, these cyber-criminals also offer cloned credit/debit cards (from $180), card cloning machines ($200-1,000), and even fake ATM machines (from $3,500 depending on the model). Additional products such as money laundering services (bank transfers or cashing checks) are available for a commission ranging from 10 to 40 percent of the operation. If buyers want to use stolen bank details to buy products online, but are wary of being traced through the delivery address, the cyber-criminals will make the purchase and forward the goods for a fee of between $30 and $300 (depending on the chosen product).

For more sophisticated cyber-criminals who want to set up their own fake online stores and use rogueware techniques to obtain both user details and also reap the money these unsuspecting victims pay for fake antivirus products, there are also teams available to deliver turnkey projects, design, develop and publish the complete store, even positioning it in search engines. In this case, the price depends on the project.

Prices for botnet rental for sending spam (using bot-infected zombie computers, for example) vary depending on the number of computers used and the frequency of the spam, or the rental period. Prices start at $15 and rise to $20 for the rental of a SMTP server or VPN to guarantee anonymity.

PRODUCTS	PRICE
Credit card details	From $2-$90
Physical credit cards	From $190 + cost of details
Card cloners	From $200-$1000
Fake ATMs	Up to $35,000
Bank credentials	From $80 to 700$ (with guaranteed balance)
Bank transfers and cashing checks	From 10 to 40% of the total
Online stores and pay platforms	From $80-$1500 with guaranteed balance
Design and publishing of fake online stores	According to the project (not specified)
Purchase and forwarding of products	From $30-$300 (depending on the project)
Spam rental	From $15
SMTP rental	From $20 to $40 for three months
VPN rental	$20 for three months

FIG.12

BRIEF OVERVIEW OF SOME OF THE TYPICAL OFFERS AVAILABLE ON THE BLACK MARKET

Big Business

This cyber-criminal black market caters to buyers' needs just as any other business, and functions in similar ways. Since there is a great deal of competition in this industry, the rule of supply and demand ensures that prices are competitive, and operators even offer bulk discounts to higher-volume buyers. They will offer free 'trial' access to stolen bank or credit card details, as well as money back guarantees and free exchanges.

Many sellers use underground forums to keep out of sight.

However, since it is a black market, there are clearly many areas that differ from traditional business. Since anonymity is of the utmost importance, many sellers use underground forums to keep out of sight. Their offices are effectively the Internet, though they even go as far as advertising their 'office hours.' Some are more brazen about their activities, and have accounts on Facebook and Twitter which they use as shop windows. To ensure anonymity, contact is always made across instant messaging applications or free, generic email accounts.

Once contact is made, the transaction can be executed directly or through a website set up by the seller, using a username and password, which as with any online store, allows buyers to browse and fill their "shopping cart." Payment is always made up-front using services such as Western Union, Liberty Reserve and WebMoney.

FIG13

CYBER-CRIME BUSINESS MODEL

Conclusion

The security world is more exciting than ever. As new protection technologies emerge, cyber-criminals find ways to avoid them. Many Western nations are finding out about cyber-attacks the hard way, by becoming a victim, and have started to enforce strict protection measures. The Libyan conflict has worsened over the past few days and as the civil war enfolds, cyber-activism has disappeared from the spotlight. Despite this, tension is building up in other dictatorial regimes in the area, and we will have to follow the events in the region very closely.

In the next quarter we will have some data about sales of Android-based tablets like Motorola XOOM or Samsung Galaxy Tab II, an aspect that can have a major impact on the future of malware attacks on Android devices. If tablets end up replacing PCs, Android will become the new Windows. From a malware perspective as well...

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/**