QUARTERLY REPORT PandaLabs

(JULY-SEPTEMBER 2010)

PANDA SECURITY

Index

Introduction

In the last edition of our **quarterly report**, published in July, we signed off by predicting that social networks would continue in the spotlight, as has been the case with the clickjacking attacks on the 'Like' button in Facebook.

We also mentioned that there would be news about the security of Android, and once again our predictions have come true, as you can read later.

The 'Mariposa' saga continues, and brings good news, as further arrests have been made in relation with the case, highlighting the progress that the authorities are making in dealing with cyber-crime.

In fact, the security world has seen a lot of activity this quarter. Perhaps one of the most significant stories picked up by the media in recent months has been the infections caused by the 'Here you have' worm.

In the last few weeks, we have witnessed a situation that we hadn't seen for some years, a typical email worm spreading using the subject 'Here you have', in the true tradition of *ILoveYou*. Although not reaching epidemic proportions, the worm has infected many major companies. As we have often explained, malware is now created for financial gain, and that's precisely why such worms had practically disappeared. So why has this new strain suddenly appeared? Well, as you will read below, it would seem to be an action targeting the USA by a group calling itself the "Brigades of Tariq ibn Ziyad."

We have also observed how little progress has been made in respect to security in SMBs over the last year, as they continue being infected, according to the data from the **Second International SMB Security Barometer**; and in 25% of cases they were infected by worms designed to spread via USB devices.

We have also published the **First Annual Social Media Risk Index for SMBs**. This reveals that some 77% of employees us e these networks while at work, and that 33% of SMBs have suffered infections originating from social media sites.

And more on malware: the data we have compiled indicates that the situation is worsening, and infections continue to spread across all countries.

Once again much has been happening, in addition to strategic movements in the sector –takeovers and capital injections– there has been considerable criminal activity. We hope you enjoy this Q3 report, packed with all the latest information.

More 'Like' button clickjacking

If we had to summarize this last quarter in just a few words, it would be: clickjacking, BlackHat SEO and 0-day, as most of the attacks in these few months have been based on at least one of these techniques.

Last quarter's report also talked about clickjacking; this technique was used by criminals to trick users into clicking the 'Like' button in Facebook. These attacks have continued throughout the last few months, using a variety of events, news items or celebrity names to draw users' attention, such as the case reported in our **blog** about Discovery Network's shark week.

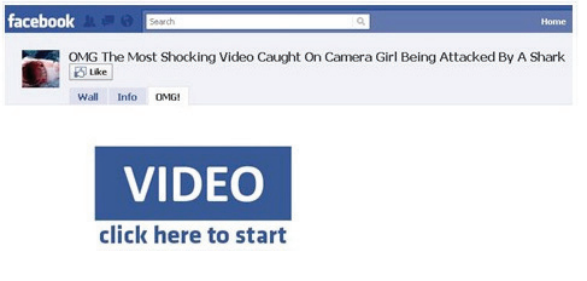

FIG.01

CLICKJACKING IN FACEBOOK

Other famous names have also been targeted using clickjacking, such as **McDonalds**.

FIG.02

CLICKJACKING IN FACEBOOK

Similarly with BlackHat SEO, cyber-criminals are finding out just how easy it is to spread malware using this technique. They have also gone as far as automating attacks.

Social networks and BlackHat SEO attacks continue to be the distribution methods of choice for hackers

We've seen cases targeting stories such as the wedding of **Chelsea Clinton**, where related searches in Google returned results that pointed to pages used to distribute malware, mainly fake antivirus programs (rogueware).

Yet we now need to take special care, as even the very youngest are being targeted by these attackers, to judge from a BH SEO attack using **Moshi Monsters**, a kind of mix of Tamagochi, Pokemon and NintenDogs and very popular among kids.

FIG.03

BLACK HAT SEO USING MOSHI MONSTERS

We have also noted how these actions are planned well in advance, as was demonstrated by the **attack** targeting Halloween and Thanksgiving uncovered in August.

The Mariposa saga continues...

Just when we had almost forgotten about Mariposa, this summer **several arrests** were made in Slovenia. People questioned whether this could really be related to **Mariposa**, as those behind Mariposa were Spanish and those arrested were Slovenian.

Last March, when the story was first announced, we talked about the Spaniards that had been apprehended, and that they had bought the bot. You may well remember that we said nothing about the seller of the bot. This wasn't because we didn't know who was behind it, but rather that the FBI had kindly asked us not to publish the information, as they were on the trail of Iserdo.

Who is Iserdo? It's the nickname of the Slovenian who developed the main Butterfly bot, and who was in contact with Netkairo. Similarly, he was the one who sold Netkairo the bot behind the Mariposa network.

According to Netkairo, he and Ostiator gave Iserdo "99%" of the idea to develop the bot. This is unlikely to be true; let's not forget that this 'revelation' was during a conversation in which Netkairo urged us to employ him in our laboratory.

A Slovenian newspaper claimed that the price paid for the bot could be as much as €40,000. It's not clear where this information came from, but it would seem wide of the mark. These are the prices for which the bot was sold:

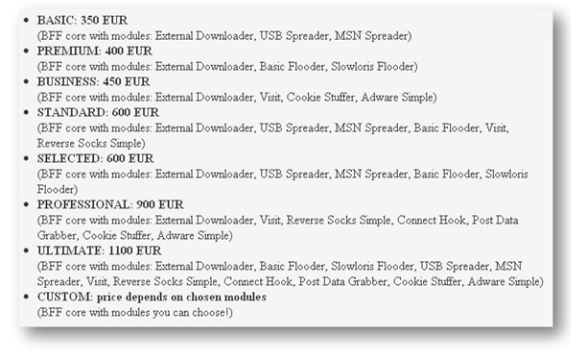

FIG.04

BOTS' PRICES

Netkairo bought the 'custom' model, and these are the prices for each model:

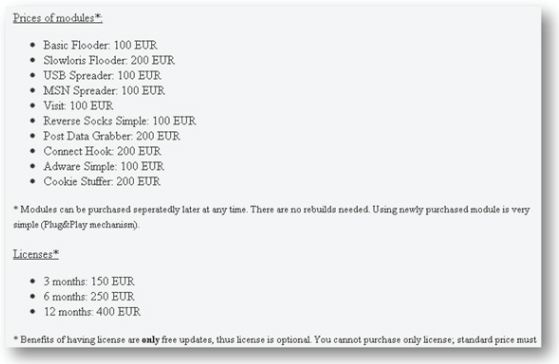

FIG.05

PRICES OF THE BOTS' MODELS

But there is still more to come. The Civil Guard are trying to make more arrests in relation with Mariposa and Iserdo has been selling the bot to different groups who are creating their own botnets (as we saw in the "**Vodafone incident**").

The Mariposa saga continues:
new arrests in Slovenia,
and the authorities are still investigating...

After the arrests in Slovenia, the police gave a press conference revealing more information about the case. They searched seven addresses and confiscated some 75 devices (computers, hard drives, memories, etc.). They confirmed that two suspects, aged 23 and 24, had been arrested. After 48 hours both were released, but the investigation continues. Police confirmed that one of those arrested is suspected of being the creator of the malware (known as ButterflyBot) with which the Mariposa botnet was created. They also indicated that they are investigating two crimes: the creation of tools facilitating digital crime and money laundering.

More information has been forthcoming from media sources, although yet to be confirmed by the Slovenian police: The 23-year-old arrested is thought to be Iserdo, otherwise known as Matjaz Skorjanc, of Maribor, Slovenia. A failed medical student, whose father has a small-business near Maribor selling and developing electronic devices. His alias, Iserdo, when spelled backwards means 'ransom' in Slovene (odresi).

The 24-year-old is Nusa Coh, also from Maribor, and whose alias on the IRC is L0La. It would seem that at least part of the money earned by Iserdo from the sale of the bot was paid to Nusa Coh, although she may not have known how Iserdo was getting the cash. She received transfers via Western Union from different people, such as Netkairo, the 'owner' of the Mariposa botnet.

(If you'd like to know more about why criminals use Western Union, you can read **the article** we published a few months ago.)

Another name cropped up during the investigation, that of the 24-year-old Dejan Janzekovic. Also from Maribor, he works as a systems administrator at Amis, a Slovenian telecom and ISP. He was wrongly identified by some media sources as Iserdo, but has not been arrested.

Janzekovic contacted the media who published his story. The police also searched his house though it would seem in this case that he has been just another victim. He was connected with the case as he had been a classmate of Nusa Coh (L0La) at high school. Janzekovic claimed that he had not been in contact with her for several years, and also that Iserdo had used his photo for identification on some occasions.

In the week that Iserdo and L0La were arrested, the Web page used to advertise and sell the bot was shut down. The following week, the page was up and running again, as you can see from these screenshots:

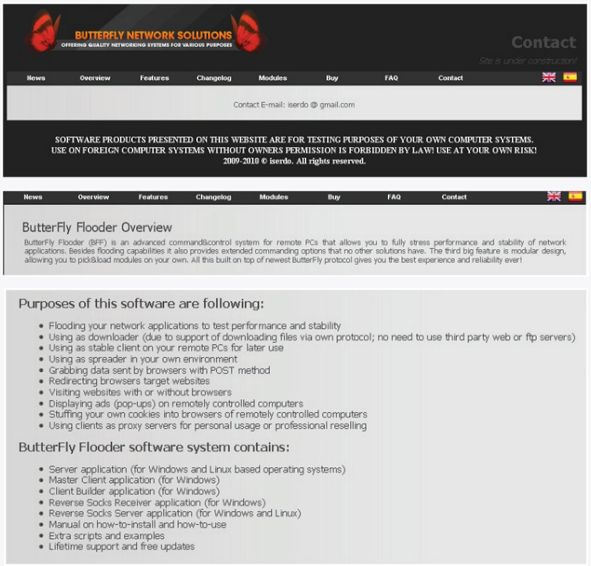

FIG.06

BUTTERFLY BOT

A few days later, the Slovenian CERT (SI-CERT) contacted the company hosting the page (West Hosting corp). It would seem that they were happy to collaborate, as the page has not been available since then.

New attacks on SCADA systems and "Here you have"

If there is one attack above all that stands out this quarter, it is the one on **SCADA** systems, in particular, because of the elaborate nature of the attack. It was carried out by exploiting a 0-day vulnerability in Windows, and installed a digitally-signed rootkit. It is still not clear who was responsible for the attack, but it's obviously not the work of amateurs.

At the end of this last quarter we witnessed a situation that we hadn't seen for some years, a typical email worm spreading using the subject 'Here you have', in the true tradition of *ILoveYou*. Although not reaching epidemic proportions, the worm infected many major companies. As we have often explained, malware is now created for financial gain, and that's precisely why such worms had practically disappeared. So why has this new strain suddenly appeared?

'Here you have', a new worm of the 'old-school' surprisingly emerged, infecting many large companies in the USA

The worm, dubbed 'Here you have', was the second variant of a worm that appeared in August, and one its main features is that the sender of the email message in which it spreads appears as "iraq_resistance", and would seem to be linked to the Brigades of Tariq bin Ziyad brigade terrorist group.

Three days after this variant appeared, someone claiming to be the author of the worm posted a video on Youtube, signed by 'IRAQ Resistance-Leader of Tarek Bin Ziad Group'. The poster used the alias "iqziad", and according to their YouTube profile is a 26-year-old in Spain.

Tariq bin Ziyad (Arabic: طارق بن زياد), (died in 720) was a Berber commander who led the Muslim invasion of the Iberian Peninsula in the eighth century, conquering Visigoth Hispania, according to traditionally accepted history, based on the Arab chronicles of the 10th and 11th centuries.

The video claims the worm has been created and propagated principally to target the United States for two reasons: to commemorate the 9/11 attacks and to demand respect for Islam, with reference to the threat made by pastor Terry Jones to burn the Koran.

The video displays a map of Andalusia, Spain along with a photo and an emblem, presumably that of the group. The video transcript is (roughly) as follows:

> *"Hello, My nickname is Iraq Resistance. Listen to me about the reasons behind 9/September virus that affected NASA, Coca-Cola, Google, and most American ???. What I wanted to say is that the United States doesn't have the right to invade our people and steal the oil under the name of nuclear weapons. Have you seen any there? No evidence about any project. How easy you kill and destroy. Second, that the Christian, Terry Jones. What he tried to do the same day this worm spread is not even fair.*
>
> *I know that not all Christians are similar and some news papers wrote that I am a terrorist hacker because a computer virus and Mr. Terry Jones is not. And he is not terrorist because he affected all muslims behavior? I think, America, come on, be fair. Where is your freedom, which must end when you ???. As you say you modern educated people. I don't know that there is another one and really I don't like "smashing" and even there were no computers "smashed" as you know from the analysis report. I can "smash" all of those infected, but I wouldn't and don't use the word terrorist please. I hope all people understand that I'm not negative person. Thank you for publishing".*

Second International SMB Security Barometer

For the second consecutive year, we have published our annual **International SMB Security Barometer**. Almost 10,500 companies, with up to 1,000 computers, took part in the survey, across Europe, Latin America, the United States and Canada.

Compared with last year's figures, Spanish SMBs have improved notably in terms of implementing security measures, and now lead the way (92% of companies have a security system installed). However, they have also suffered more infections than their European and North American counterparts (59% compared to 49% and 34%, respectively). Only Latin America, with 65%, fared worse.

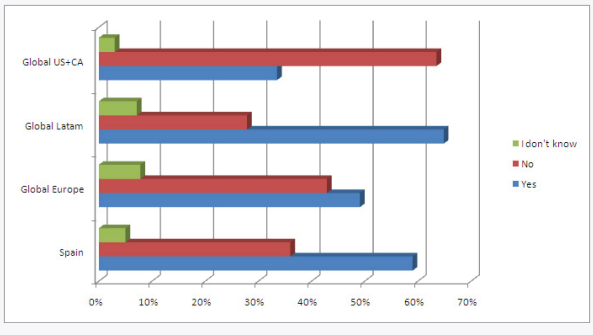

FIG.07

HAVE ANY OF YOUR COMPANY'S COMPUTERS BEEN INFECTED BY AN INTERNET THREAT?

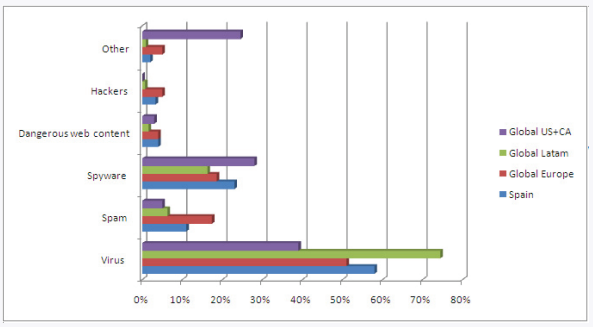

FIG.08

WHAT TYPES OF THREATS AFFECTED YOUR COMPANY?

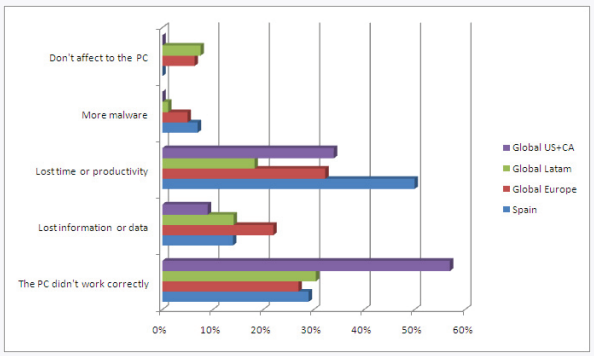

FIG.09

HOW DID THE INFECTION AFFECT YOU?

Awareness about the need for protection is very high across all geographic areas, although an average of 7% of users still believe it is unimportant. Between 11 and 13% of those surveyed said they had no security system installed.

Some 17% confirmed that they used free solutions to protect themselves. Even though companies are now more security aware and claim to be better protected, globally some 52% have suffered infections in the last year.

52% of SMBs have been infected in 2010, many through USB devices

Email continues to be the main entry point for malware along with the Internet. This year, however, there has been significant growth in the amount of infections caused through USB devices, with on average 27% of companies affected through this channel, while P2P, messaging and other similar applications are on the decline as a source of infection.

Wasted time and lost productivity, as well as interference with computers, are the main consequences of infections, followed by data leakage.

Overall, companies claim to have maintained a similar investment in security as last year, although when asked if they had anyone dedicated to security management, 58% in Spain said they did, as opposed to 67% in the rest of Europe, 68% in Latin America and 60% in USA and Canada. All these figures are fractionally up on last year.

The complete report is available at: **http://prensa.pandasecurity.com/wp-content/uploads/2010/07/2ndbarometro.pdf**.

More infections via USBs

The distribution of Internet threats via USB devices has become a growing trend. Infection of SMBs by malware that spreads in these gadgets and runs automatically is now a reality. Studies of the new threats created so far reveal that 25% of new worms are designed to spread via USB devices.

This information ties in with the data revealed in the **Second International SMB Security Barometer**, in which 48% of SMBs surveyed (from 2 to 1,000 PCs) admit to having been infected by some type of malware in the last year, and 27% confirm that the source of the infection was a removable memory device connected via USB to a computer.

So far, these types of infections have still not reached the levels of malicious email, but it is a growing trend. There are now so many devices on the market that can be connected via USB to a computer: digital cameras, cell phones, MP3 or MP4 players... And obviously this is very convenient for users. Yet all these devices have memory cards or internal memories and therefore it is very easy for your telephone, say, to be carrying a virus without your knowledge.

How they work

There is an increasing amount of malware, which like the dangerous Conficker worm, spreads via removable devices and drives such as memory sticks, MP3 players, digital cameras, etc. The basic technique used is as follows: Windows uses the Autorun.inf file on these drives or devices to know which action to take whenever they are connected to a computer.

This file, which is on the root directory of the device, offers the option to automatically run part of the content on the device when it connects to a computer This feature is being used by cyber-crooks to spread viruses, through the modification of Autorun.inf with commands so that malware stored on the USB drive, for example, is run automatically when the device connects to a computer. This will immediately infect the computer in question.

To prevent this, Panda Security has developed Panda USB Vaccine (available at **http://www.pandasecurity.com/spain/homeusers/downloads/usbvaccine/**), a free product which offers a double layer of preventive protection, disabling the AutoRun feature on computers as well as on USB drives and other devices.

Social Media Risk Index for SMBs

While on the subject of reports about the threats and risks faced by companies, this quarter we have also launched the **First Annual Social Media Risk Index for SMBs**. This first edition has analyzed the situation in the United States, talking to those responsible for security in 315 companies with up to 1,000 employees.

77% of SMB employees in the United States use social media during work time. 33% say that their companies have been infected by malware distributed through these communities

One of the most striking results is the frequency with which social networks are used during work time (77% of employees admit to doing so), and consequently, 33% of companies have been infected by malware through this channel.

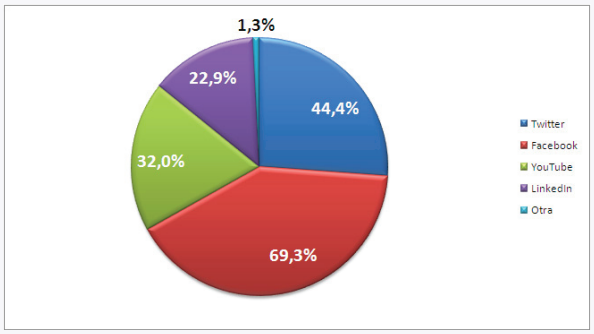

FIG.10

SOCIAL MEDIA MOST FREQUENTLY USED BY SMB EMPLOYEES IN THE USA

The benefits of social networks outweigh the concerns

According to the study, the main concerns for SMB's with respect to social networks include privacy issues and financial loss (74%), malware infections (69%), loss of productivity (60%) and issues related with corporate reputation (50%), followed by network performance problems (29%).

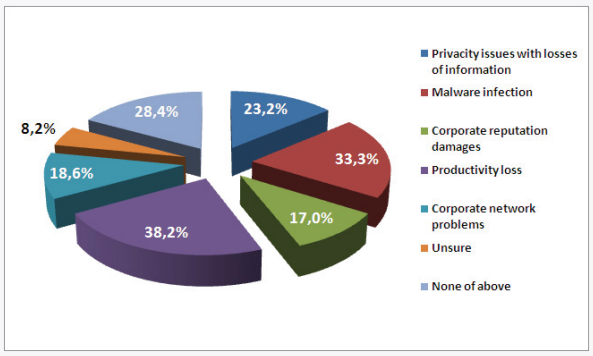

FIG.11

MAIN CONCERNS FOR SECURITY MANAGERS IN US SMBS BECAUSE OF THE USE OF SOCIAL MEDIA BY EMPLOYEES

Yet these concerns do not prevent SMBs from taking advantage of the benefits offered by social networks, with 78% of companies reporting that they use these tools to support research and competitive intelligence, improving customer services, implementing public relations and marketing initiatives and direct generation of revenue. Facebook is the most popular social media tool used by SMBs: 69% of companies have active accounts, followed by Twitter (44%), YouTube (32%) and LinkedIn (23%).

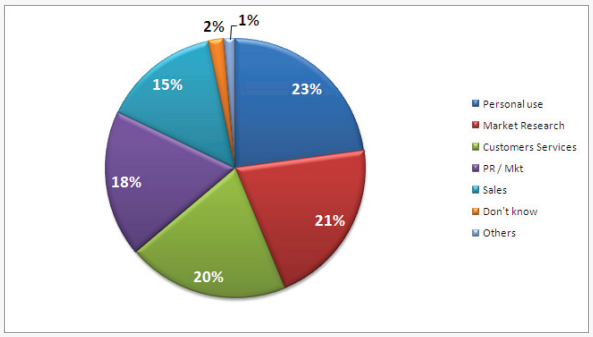

FIG.12

REASONS FOR USING SOCIAL MEDIA IN US SMBS

Facebook has become a major source of malware infections

Facebook likewise is mentioned as the main culprit in the case of malware infections (71.6%) and privacy violations (73.2%). YouTube is in second place in terms of infections (41.2%), while Twitter was responsible for a large number of privacy violations (51%). For those companies who reported financial loss through compromised employee privacy, Facebook was once again the social media from which most problems arose (62%), followed by Twitter (38%), YouTube (24%) and LinkedIn (11%).

Policies and training among SMBs

To minimize the risks associated with social media, 57% of companies currently have policies regulating their use, and 81% of these have personnel dedicated to implementing these policies. Moreover, 64% of the companies questioned claimed to deliver training programs to teach employees about the risks and benefits of social networks in the workplace. Most of those surveyed (62%) do not allow these sites to be accessed for personal use.

The restrictions most commonly in place include: playing games (32%); publishing inappropriate content on social media (31%), installing unauthorized applications (25%). In addition, 25% say that they actively block employees from visiting the most popular sites, mostly using Web-based security services or applications (45%).

Also, 35% of companies infected have suffered financial losses, and more than a third lost more than $5,000.

You can see the full study at **http://prensa.pandasecurity.com/wp-content/uploads/2010/06/%C3%8Dndice-de-riesgo-de-las-Redes-Sociales-para-PYMES2.pdf**.

Malware on smart phones... Android in the line of fire

In previous articles we analyzed the situation of the smartphone market, indicating that it was more than likely that Android would become the most popular smartphone terminal. It would now seem that this is turning out to be the case, and although there are still not that many out in the street, we are already seeing the first applications with malicious intent and which can therefore be considered as malware.

The first threats

The first threats were spoof applications for accessing online banks, though these disappeared rapidly as they were promptly reported by users. These applications were quite simple, as they basically displayed a login form in which users were supposed to enter their user name and password. It was really an initial attempt at phishing targeting Android terminals.

Android is now targeted by hackers due to its increasing popularity

Yet this summer has seen the arrival of the first more complex applications that act maliciously on these cell phones.

The first to appear was Android/FakePlayer.A, a fake app for playing videos which really sends a text message to a premium-rate number. Any user infected with this Trojan will see their monthly telephone bills soar, given that the cost of these messages can be more than ten times the cost of a normal message.

FIG.13

ICON DISPLAYED BY THE FAKEPLAYER

The FakePlayer.A was really an initial Beta version of the Trojan, as analysis revealed it included test code and even the 'Hello World' class created by IDEs used for java programming, like Eclipse.

The 'B' variant of the Trojan, more refined and without junk code, was later distributed, although the basic app was the same and performed the same actions.

The spy market

The integration of GPS technology in smart phones allows the terminal to include geolocation information which can be leveraged according to the needs or preferences of the user. Yet this information can be exploited to spy on people, either with criminal intent or even by jealous or suspicious partners.

There are even commercially available spy apps that are on the border of what constitutes a legitimate application. Such legitimate uses may include finding the phone if lost or stolen, giving someone your location if you get lost, keeping track of young or vulnerable people. But if the terminal is tracked without the knowledge or consent of the owner, then we are talking about malware, specifically if it is dressed up as a game or the like, as is the case with TapSnake.

TapSnake is a game along the lines of the famous 'Snake', which also geopositions the terminal and sends the information to the servers of a company offering espionage services. This company also offers another app for Android which shows the location of users infected with TapSnake that have been registered with a certain email address.

Therefore to track this person, the spy has to get the victim to install the game and register it under a certain account.

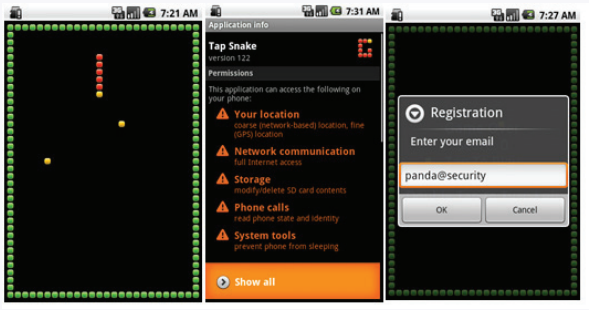

FIG.14

TAPSNAKE SCREENS

It is clear that malware on the Android platform is in the early stages, but the convenience with which apps are easily on Android Market means that users have little need to install those distributed in other ways.

We will therefore have to wait and see which distribution/security policy will be attacked most. A restricted Market/Store may push users into looking for other less secure sources of software, while a less restrictive Market/Store might seem more vulnerable initially, but may lead to greater control over the distribution of software.

Android as bait

Finally, in recent weeks legitimate Android apps have appeared compressed with self-extracting files that infect the computer on which the app is being installed. In other words, Android apps are being used as bait to infect computers with self-extracting files.

Vulnerabilities, exploits and 0-days

Throughout this third quarter there has been much talk of two major design errors in Microsoft Windows.

The story starts back on June 16 of this year, with the discovery of a new 0-day vulnerability, CVE-2010-2568[1], affecting all versions of Windows from Windows XP, and even betas of Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1. The vulnerability was classified by Microsoft as critical in all versions.

The problem arises because Windows incorrectly handles shortcut files (.lnk and .pif), allowing a malicious user to execute remote code when a specially-crafted shortcut icon is viewed. The vulnerability was first exploited in the wild using the malware *Rootkit/TmpHider*. Because of the way it is exploited, as with the Autorun malware family, USB devices are the principal distribution vectors for malware that leverages this vulnerability.

Microsoft quickly produced a workaround to mitigate the issue. This involved deleting the default value in the following Windows registry entries:

```
HKEY_CLASSES_ROOT\lnkfile\shellex\IconHandler
HKEY_CLASSES_ROOT\piffile\shellex\IconHandler
```

By removing this function from the operating system, the vulnerability was corrected, but the user would no longer be able to see shortcut icons for applications on the system.

Perhaps because the solution put forward by Microsoft was not deemed adequate, the Internet security community got to work, and created other solutions to the system without having to lose all Windows shortcut icons. Among them, researcher Didier Stevens, known for his PDF analysis tool developed in Python, created Ariad[2] to mitigate exploitation of the vulnerability.

Some two months later, on August 2, Microsoft finally fixed the security hole with the publication of MS10-046[3]. **PandaLabs** advises users to apply this update promptly.

On August 28, 26 days after Microsoft released its solution, a new critical vulnerability was published[4] which allowed the remote execution of code.

1 **http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568**.
2 **http://blog.didierstevens.com/2010/07/18/mitigating-lnk-exploitation-with-ariad/**.
3 **http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx**.
4 **http://www.microsoft.com/technet/security/advisory/2269637.mspx**.

The vulnerability is caused because of the order in which Windows searches for a library to load when the path has not been specified.

Library search order:

1. Directory from which the application has been loaded.
2. System directory (%system%).
3. 16-bit system directory.
4. Windows directory.
5. Current Working Directory (CWD).
6. Directories contained in the PATH environment variable.

This mistake can occur using the LoadLibrary[5] function. As is clear from the following example, the programmer does not specify the complete path of *mylibrary.dll*.

```
HMODULE handle = LoadLibrary("mylibrary.dll");
```

In this case, the malicious library will be loaded by the program if it is found before the original program library.

Displaying the full path of the library avoids this possible threat.

```
HMODULE handle = LoadLibrary("c:\\windows\\system32
\\mylibrary.dll");
```

One real-world example is Apple's iTunes application, which is vulnerable to this attack. If a malicious user were to share a folder with various multimedia files in a path accessible to other users and if one of these users tried to play one of the files on this shared resource, when iTunes needs to load a library dynamically it starts searching the same directory as the file it wants to run. In this case, if the malicious user has copied a library in this location similar to the one iTunes needs to load, the system could be completely compromised when the code of the malicious library is run instead of that of the requested library.

Unlike other vulnerabilities published by Microsoft in its security bulletins, where an update is provided for vulnerable environments, in this case the developer of the application is responsible for publishing the solution, e.g. by updating the vulnerable software.

In its security bulletin, Microsoft has created a new registry entry with the name *CWDIllegalInDllSearch*, which allows users to control the DLL search path algorithm. Information about this new function introduced by Microsoft can be found at **http://support.microsoft.com/kb/2264107**.

To continue with Apple, on August 29 the researcher Rubén Santamarta published a new 0-day attack allowing execution of arbitrary code on Quicktime Player 7.x and 6.x. The vulnerability can be exploited thanks to an oversight of the programmer by not deleting the parameter __Marshaled_pUnk of the "QTPlugin.ocx" plug-in which had been used in previous versions of the plug-in.

Rubén Santamarta's research has not only identified a new 0-day vulnerability, but has also created an exploit able to evade ASLR[6] and DEP[7] protection, successfully demonstrating the exploitation of this vulnerability in different versions of Microsoft's operating system, including Windows 7.

All information about this discovery has been detailed by the author on the following page: **http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1**.

We will close the present report with the latest 0-day vulnerability discovered in Adobe Acrobat and Adobe Reader. Although this might seem just one of the usual stories that we read about this product, the peculiarity of this vulnerability is the way in which attackers have exploited it.

5 **http://msdn.microsoft.com/en-us/library/ms684175(VS.85).aspx**.
6 **http://en.wikipedia.org/wiki/Address_space_layout_randomization**.
7 **http://en.wikipedia.org/wiki/Data_Execution_Prevention**.

The vulnerability is a buffer overflow in *CoolType.dll*. This library calls the *strcat*[8] system function, which is insecure as it does not have the capacity to specify the size of the buffer to be added to the target buffer. If the buffer to be added is bigger than the space remaining where it is to be copied, an overflow is provoked. It's like trying to fill a 1 litre bottle with 1.5 litres.

Microsoft, on its Windows API page, is suggesting that the function should not be used (the link above explains the function of strcat).

```
LPTSTR StrCat(
  __inout  LPTSTR psz1,
  __in     LPCTSTR psz2
);

Note: Do not use. See Remarks for alternative functions.
```

VUPEN, a specialist in exploit creation for this application, details in the article "Criminals Are Getting Smarter: Analysis of the Adobe Acrobat/Reader 0-day Exploit"[9] how an attacker can avoid the ASLR and DEP protection in Windows using a method never seen before.

Without going into too much technical detail, when a stack overflow is triggered, there is normally an attempt to overwrite the return address or the exception handler to change the program execution flow and allow the malicious user to execute injected code. However, in this case it is not viable, because the combination and configuration of the Microsoft protection that verifies possible buffer overflows (option /GS[10] of the Visual Studio compiler) and the exception handler prevent the vulnerability from being properly exploited.

Nevertheless, the attacker goes further and discovers a way of exploiting the vulnerability satisfactorily without having to overwrite the return address or the SE handler in order to control the execution flow. However, our malicious user still has to resolve the obstacle of the ASLR and DEP protection. Getting past ASLR was "simple", using the *icucnv36.dll* library which is not compatible with this protection system and creating an exploit using ROP[11]. However, this library does not import VirtualAlloc, VirtualProtect, HeapCreate, WriteMemory functions, or even LoadLibrary, which are needed to overcome DEP. So the user came up with CreateFileA, CreateFileMappingA, MapViewOfFile and memcpy functions which were imported by the library to execute malicious code on the compromised machine. For a more detailed analysis of how the vulnerability was exploited, refer to the article mentioned above.

This exploit demonstrates the high level of technical knowledge possessed by malware creators determined to infect as many computers as possible by evading the latest protection delivered by Microsoft in Windows. ASRL and DEP are powerful protection components against this type of vulnerability provided both are enabled and all program modules are compatible with ASLR. On this occasion, the *icucnv36.dll* library has been the Achilles' heel and the cause of a successful exploit of the vulnerability.

8 **http://msdn.microsoft.com/en-us/library/bb759925(VS.85).aspx**.
9 **http://www.vupen.com/blog/**.
10 **http://msdn.microsoft.com/en-us/library/8dbf701c(VS.80).aspx**.
11 **http://en.wikipedia.org/wiki/Return-oriented_programming**.

Global distribution of malware

We were recently asked on Twitter what could be done to eradicate malware... Not an easy question if we avoid facile, 'I want peace in the World' –type answers.

The sums of money generated in the nefarious business activities of cyber-mafias are such that the amount of malware created to infect new victims is inevitably increasing every day.

And the rate of infection remains high, largely due to the many different channels used to try to infect users by surprise: just as they begin to recognize threats that arrive via email, suddenly they start coming through social networks or fake Web pages...

Yet although it may seem somewhat generic and global, there is a valid answer to the question: cyber-crime will at least slow down when there is greater international collaboration and more criminals are put behind bars, and when the sentences handed down are sufficiently stiff to deter people from committing these crimes and to ensure that their actions don't pay.

Until governments and authorities start dedicating the attention and effort required, fomenting international collaboration and toughening sentences for the hackers apprehended, the situation will continue to worsen.

This is supported by the malware figures over the last quarter.

Looking at the distribution of types of threats received by **PandaLabs** in the last three months, it is clear that the percentage is more or less the same as before, although Trojans increased four points with respect to the previous quarter. In the end it is logical: Trojans are designed, by and large, for financial gain, and they offer the best ROI to their creators.

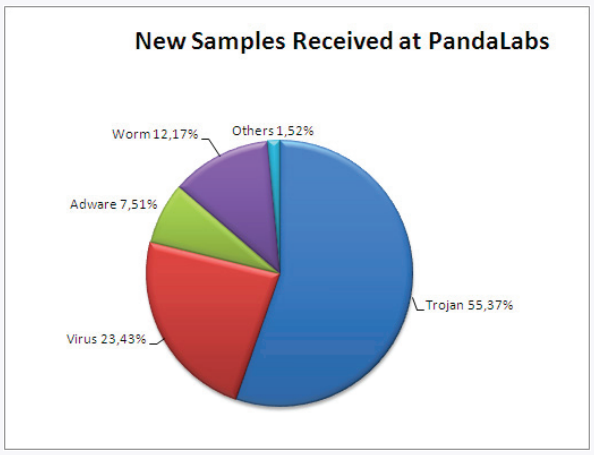

FIG. 15

SAMPLES RECEIVED AT PANDALABS

Consequently, global infection ratios can be correlated to the new malware created, as the number of users and companies infected by Trojans continues to grow. In fact there was a five point increase in this figure with respect to the previous quarter.

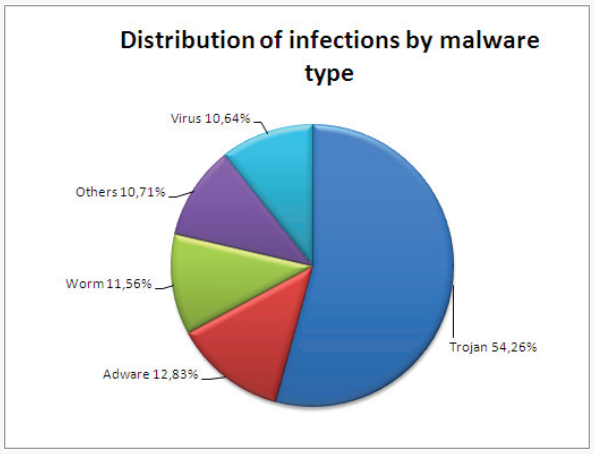

FIG. 16

DISTRIBUTION OF INFECTIONS BY TYPE

This data, compiled through our Panda ActiveScan (**www.activescan.com**) free online antivirus, not only includes active malware, i.e. code which is running when the scan is performed, but also latent malware, lying dormant on the computer and waiting to be run either unwittingly by the user or remotely.

And here is the infection ranking by country:

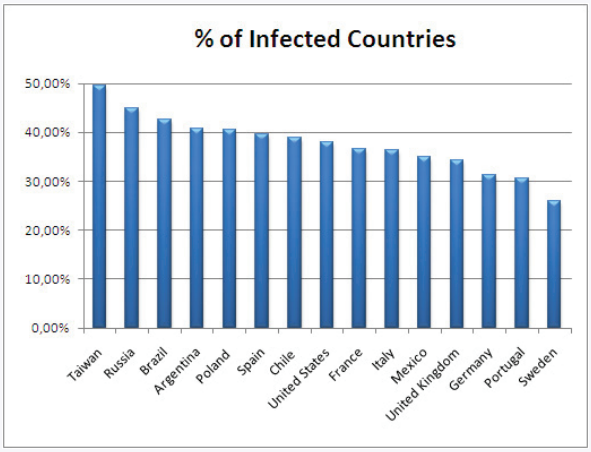

FIG. 17

INFECTED COUNTRIES

It is worth noting that Brazil has risen from 6th place in the previous quarter to 3rd place; and also Chile, which was not in the last ranking, but is now in 7th.

If you're wondering about the type of malware infecting users across these countries, here you have more details, although few surprises: Trojans are responsible for most infections, as is to be expected for the reasons detailed above.

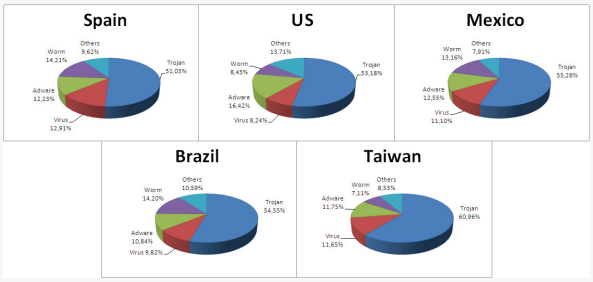

FIG. 18

INFECTIONS BY COUNTRIES

Now we'll look at how Trojans have affected each country individually.

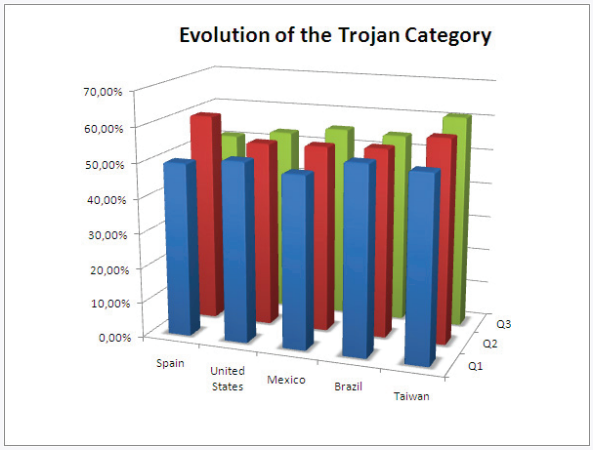

FIG. 19

EVOLUTION OF TROJANS

The situation varies, in some countries there has been an increase and in other countries not, although the differences are small, and we're not talking about a change in the trend. It is clear that the methods used by hackers to spread Trojans are still effective.

In global terms, we can say that for every ten potential victims that receive a Trojan, five are infected. It would be useful to know how many of this 50 percent finally fall victim to financial fraud or theft, but to get this data we would need a better data flow from the law enforcement agencies in each country that receive the complaints.

Spam info

The truth is, the situation regarding spam has not improved either. As we always insist, cyber-crooks are constantly looking for as many ways as possible for spam to reach its target, and as security solutions become able to detect them, the techniques used change.

Often we wonder how victims continue to fall for these ruses, as the criminals don't waste too much time with the design or text of these messages. They do however put effort into improving the methods of distribution, and are even sending spam in mp3 files.

Other the last three months, 95% of email in circulation was spam. Much of this originates from botnets (numerous computers hijacked by hackers), and many users whose systems are being employed to send spam don't even realize they are doing it, and consequently committing a crime. In this period, the Top 10 countries were responsible for 55% of all spam in circulation.

FIG.20

TOP 10 SPAMMING COUNTRIES

Which countries are they? You can see below:

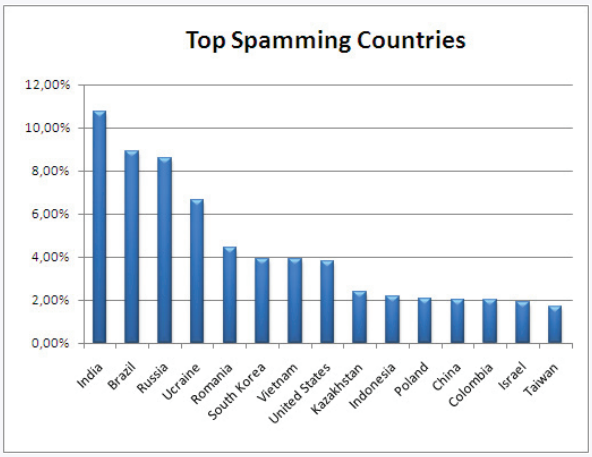

FIG.21

TOP SPAMMING COUNTRIES

There are no real surprises compared with the last quarter. Perhaps what is most interesting is that the United Kingdom has disappeared (for the moment at least) from the ranking. They must be doing something that has helped keep them out of the top ten.

Conclusions

The truth is, we would genuinely like to be able to sign off one of these annual or quarterly reports with a positive message; we would like to say the situation has improved. However after some deliberation, the editorial team have decided that this is still not the case.

The reasons are quite clear: there continues to be more malware than before, cyber-criminals continue to infect users, new techniques are emerging to take users by surprise, smart phones are under attack... so really, nothing out of the ordinary.

However, in various countries there have been some successes, particularly the bringing down of the Mariposa botnet initially, as well as the sales model of the original kit, Butterfly. The collaboration to this end which began last year, continues to prosper, and we believe there will be yet more arrests. This has been a great example of teamwork and international collaboration.

And we continue to work along these lines, dealing with different cases across various countries and with different law enforcement agencies. We hope to be able to tell you of more cases in forthcoming editions, as this will mean the results have been successful.

As we head towards the end of the year, everyone, cyber-criminals included, will be looking to maximize profits before celebrating the New Year (that's if they celebrate it). So what are we likely to see? More malware, new distribution methods, more BlackHat SEO attacks, more viruses for new platforms...

Keep an eye on Mac, which is increasingly becoming a target for malware. And it's not just the computers, but also iPads, iPhones, etc... It will be on our radar for future reports. We have always insisted that Mac would become much more of a target for cyber criminals when Apple's global market share became more significant, and that is now the case. The real risk is that the Mac community will be taken by surprise. Therefore our advice is that it is better to get protection just in case... it's better to be safe than sorry.

We'll also be keeping close track of mobile devices (we have already seen how Android is becoming a more popular target in the world of malware...).

We also won't be surprised if between now and the end of the year there are more old-style worms like "Here you have"... But we will be ready to minimize the impact.

So, as the next edition of this report will be in 2011 (at the beginning of the year we will publish our annual summary), let me be the first to wish you all a Happy Christmas (I know, it's a bit early, many of you don't celebrate Christmas , etc...) ;-).

Thank you for following us. I hope you have enjoyed the report!

About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory, and is the nerve center of the company with respect to the processing of malware.

- **PandaLabs** works around the clock to produce the vaccines and other countermeasures needed to protect Panda Security's clients around the world from all types of malicious code.
- **PandaLabs** undertakes detailed analysis of all types of malware, in order to improve the protection offered to Panda Security clients, and to provide information to the general public.
- With its constant monitoring, **PandaLabs** closely follows trends and evolution in the fields of malware and IT security. Its aim is to warn of imminent threats and dangers as well as to develop strategies for future protection.
- For more information on the latest threats, refer to the **PandaLabs** blog at: **http://pandalabs.pandasecurity.com/**.