QUARTERLY REPORT PandaLabs

(APRIL-JUNE 2010)

PANDA SECURITY | 20th Anniversary 1990-2010

Index

Introduction

We are halfway through 2010 and it's time to take a look at what has been happening over the last few months. Once again, social networks –especially Facebook and Twitter– have been prominent in this second quarter.

Facebook has been in the news for all types of reasons, many of which were of its own making: from an error that allowed access to details of users' contacts, to changes in the privacy settings which caused data to be exposed without users' knowledge. However, data exposure doesn't only affect social networks. A security problem on AT&T's website revealed details of 114,000 iPad buyers who had contracted the 3G data service. A few days later, a service set up to process orders for the new iPhone4 was saturated, and consequently details of AT&T clients became accessible to other users.

Adobe has also been in the news, not just due to its conflict with Apple for not making its iPhone/iPod Touch/ iPads Flash-compatible, but also due to the amount of vulnerabilities detected, some of which were not patched and have actively been exploited by cyber-crooks.

I hope you enjoy reading the report as much as we did writing it.

BlackHat SEO Attacks

Q2 began on April 1, 'Fools' Day' in many countries. And unsurprisingly, cyber-criminals used the occasion to launch a new **BlackHat SEO** attack, "poisoning" the results of search engines to ensure malicious pages appeared among the first results when users searched for terms related with this date.


1. **April Fools**
Mar 31, 2010 ... This April 1st, the day the 2010 Census forms are officially due, the laughing you hear all around is the sound of an Obama **April Fools** Day ...
19 hours ago - Cached

2. **April Fools** Day Recipes
Mar 27, 2010 ... A fun menu for 6 with wacky **April Fool's** recipes By The Canadian Living Test . **April Fool's** Day recipe: Pineapple Fish Sticks. ...
- Cached

3. **April Fools** Jokes For Kids
Mar 31, 2010 ... What kind of pranks should you do for **April Fools** Day? What are good **april fools** day pranks for elementary school kids? ...
- 19 hours ago - Cached

4. **April Fools** Day Origin
Mar 31, 2010 ... The 1986 horror film **April Fool's** Day is themed around the day (akin to

FIG.01

MALICIOUS RESULTS RETURNED IN GOOGLE WHEN SEARCHING FOR "APRIL FOOLS"

Yet this was just the tip of the iceberg. These criminals, after all, are after our money, and to obtain this they first have to steal our information and they will use all possible means to achieve this.

> ***'Moral' and 'ethical' are words that are not in the vocabulary of cyber-criminals, and they will use any kind of news story, however tragic***

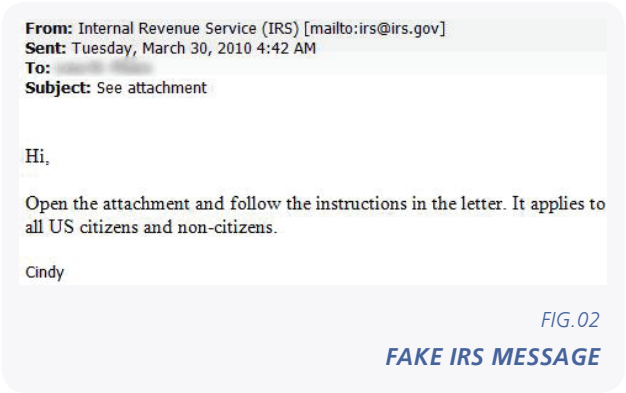
Such were the cases of **the death of Ronnie James Dio**, the **earthquake in Chile**, the **earthquake in China**, the **volcanic ash cloud** or the **crater that appeared in Guatemala**. Yet they don't stop there, any excuse can be used to infect our computers, the only criteria is that there is widespread interest in the topic: the last episode of LOST, the **elections in the UK**, a **false positive** in a well-known antivirus application, or, not least, **the World Cup in South Africa**.

Of course, cyber-criminals have more tricks up their sleeves than just BlackHat SEO attacks. As we have explained on other occasions, there are two very widely used infection techniques: exploits of security holes in software and social engineering (effectively, tricking users). We will deal with exploits a bit later, where we will look at how Adobe is once again in the spotlight, with zero-day vulnerabilities in several applications actively exploited by criminals.

Social engineering attacks

Social engineering attacks are ever present, using all types of techniques to trick users and steal their information. We have even witnessed fake prize-drawings, such as the one supposedly organized by Google claiming to offer up to **$1 million** to the winner. The best advice we can offer here is to use your common sense. If someone came up to you in the street and said you had won $1 million, would you believe them? Of course not. You should take the same approach on the Internet, and always be wary.

There are other more elaborate ruses, such as the one that emerged in April, coinciding with the internal revenue campaign in the USA. The message, aimed at stealing confidential user data, claimed to have been sent by the IRS:


From: Internal Revenue Service (IRS) [mailto:irs@irs.gov]
Sent: Tuesday, March 30, 2010 4:42 AM
To:
Subject: See attachment

Hi,

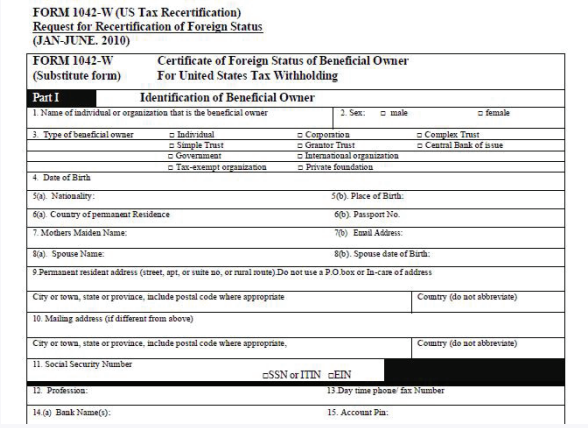
Open the attachment and follow the instructions in the letter. It applies to all US citizens and non-citizens.

Cindy

FIG.02

FAKE IRS MESSAGE

One of the documents was a spoof IRS form, requesting a series of confidential data. Recipients were asked to complete the form and send it to a fax number (in Canada). Evidently, anyone following the instructions would be laying themselves open to complete identity theft.



FORM 1042-W (US Tax Recertification)
Request for Recertification of Foreign Status
(JAN-JUNE. 2010)

FORM 1042-W (Substitute form)	Certificate of Foreign Status of Beneficial Owner For United States Tax Withholding		
Part I	**Identification of Beneficial Owner**		
1. Name of individual or organization that is the beneficial owner		2. Sex: ☐ male	☐ female
3. Type of beneficial owner	☐ Individual	☐ Corporation	☐ Complex Trust
	☐ Simple Trust	☐ Grantor Trust	☐ Central Bank of issue
	☐ Government	☐ International organization	
	☐ Tax-exempt organization	☐ Private foundation	
4. Date of Birth			
5(a). Nationality:		5(b). Place of Birth:	
6(a). Country of permanent Residence		6(b). Passport No.	
7. Mothers Maiden Name:		7(b). Email Address:	
8(a). Spouse Name:		8(b). Spouse date of Birth:	
9.Permanent resident address (street, apt, or suite no, or rural route).Do not use a P.O.box or In-care of address			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
10. Mailing address (if different from above)			
City or town, state or province, include postal code where appropriate,		Country (do not abbreviate)	
11. Social Security Number ☐SSN or ITIN ☐EIN			
12. Profession:		13.Day time phone/ fax Number	
14.(a) Bank Name(s):		15. Account Pin:	

FIG.03

FAKE IRS FORM

Social networks

If the most popular video site is a prime target for spoofing, Facebook is not far behind. In April we **published a list** of all the different pages that imitated the most popular social network in order to steal users' accounts.

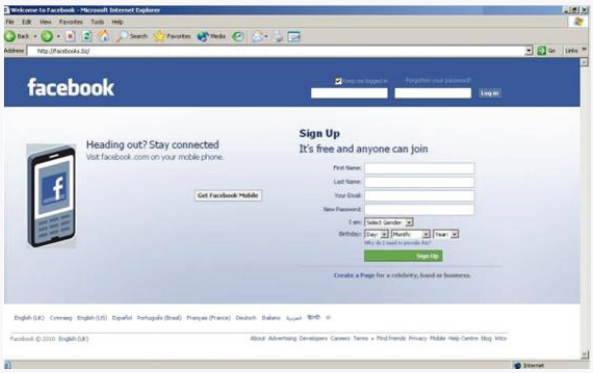


FIG.05

SPOOF FACEBOOK PAGE

Another frequent strategy is the imitation of popular websites, such as Youtube, where you are asked to install a codec in order to view the video. The downloaded file however turns out to be a new strain of malware. One such case was the malicious site called "Just a Tube":

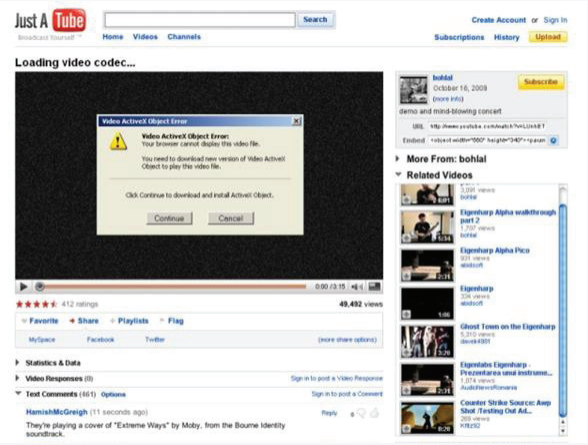


FIG.04

SPOOF YOUTUBE SITE CREATED TO INFECT USERS

It would seem that faking the most popular social networks is the order of the day when it comes to tricking users. In fact, one of the most successful attacks in Q2 has been a message purporting to be from Twitter support, offering a link to view unread messages.

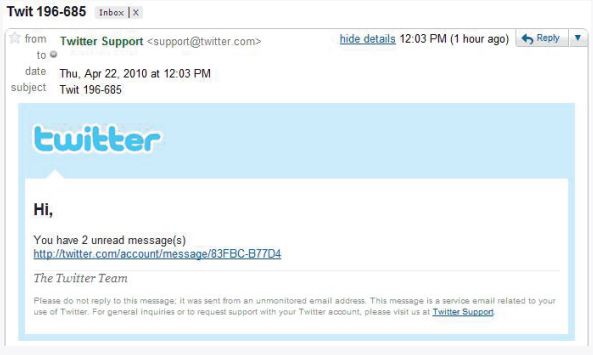


FIG.06

FAKE TWITTER MESSAGE

In the **first cases**, these links pointed to Web pages selling pharmaceuticals, such as Viagra. Recently however (Fig.07), we have come across other similar messages designed to install malware, in this case warning of an attempt to steal users' Twitter passwords.

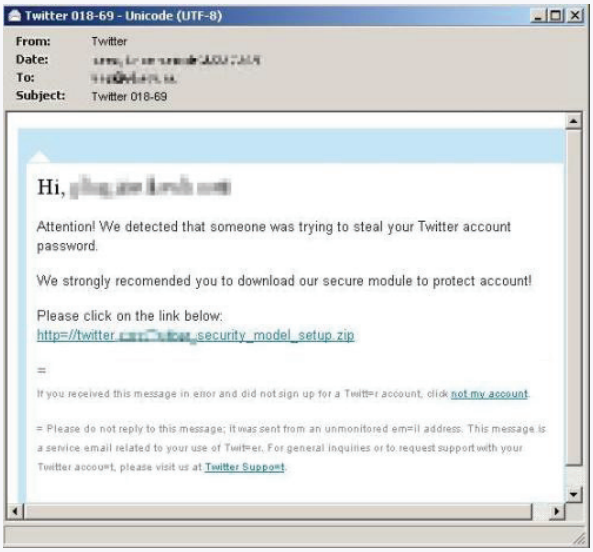


FIG.07

SPOOF TWITTER MESSAGE DESIGNED TO INFECT USERS WITH FAKE ANTIVIRUS PRODUCTS

One piece of advice we always offer, is simply to ignore any messages from banks or social networks claiming that there is a problem with your account and offering a link through which you can resolve the problem. This is a typical phishing ploy to steal account details. Other cases are designed to install malware, such as the fake Facebook message distributed at the end of April, claiming that the user's password had been changed and offering the new password in an attached document.

FIG.08

FAKE FACEBOOK MESSAGE

One message however, really did take us by surprise:

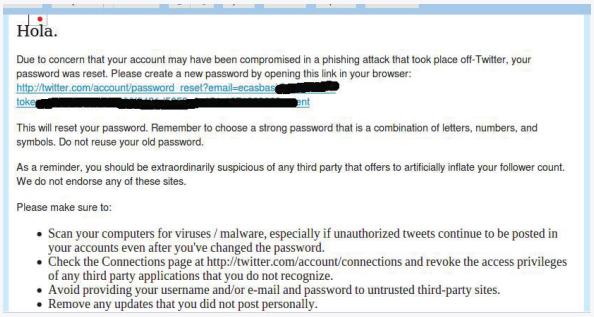


FIG.09

GENUINE MESSAGE FROM TWITTER

As you can see, this has all the attributes of a typical phishing message: supposedly sent from a trusted source, mentions a security problem, changes to your password and a link to continue the process. We have seen thousands of phishing messages with precisely this structure. So what's surprising? It's not phishing, it's a **real message**.

Returning to the issue of fake messages used to distribute malware, there can be few online services that haven't now been used by cyber-crooks: Twitter, Facebook, Amazon, UPS, iTunes, eBay, Outlook... And when it's not an online service, it could be a greetings card or resumé.

Social networks, when they are not being used as bait by criminals, are a fantastic channel for communication, but that also makes them a handy alternative to email for messages distributing spam and malware.

Cyber-criminals are using social networks as an alternative to email for sending spam and malware

The messages normally promise photos or videos, but users that click on the links will be in for an unpleasant surprise, as malware is downloaded onto their computers.

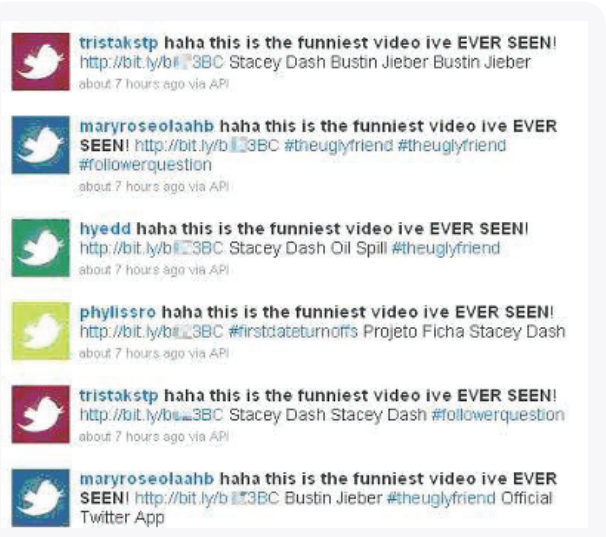


FIG.10

MALICIOUS MESSAGES SENT VIA TWITTER

What type of malware is used? Most of the attacks described here are used to distribute fake antivirus products to defraud users, or Trojans designed to steal confidential information.

Facebook clickjacking

Facebook is the biggest social network, and in spite of the controversy caused by the (lack of) privacy of information, it doesn't stop growing. One of the easiest actions it enables is to say that you "like" something. When we are logged in this social network, just by clicking the corresponding icon you express that you like a friend's picture, a comment, an application...and you can also say that you like something without being in Facebook page. Many websites have added this feature, in such a way that you can say that you like something just with a click as long as you're logged in Facebook.

The best way to understand this is with an example; there is an online role game about vampires called **Blood Wars**, which has nothing to do with Facebook. However, the option to say that you like it in Facebook has been added recently to the main site of the game:

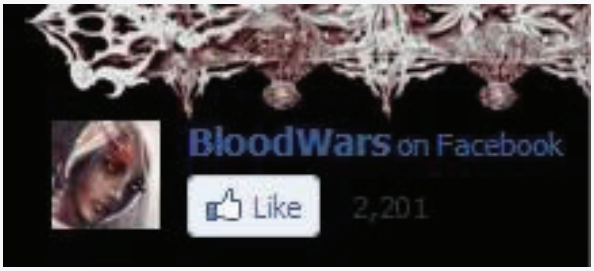


FIG.11

"LIKE" OPTION IN BLOOD WARS

When clicking this link, your Facebook page is automatically updated, indicating that you like Blood Wars:

FIG.12

UPDATED FACEBOOK PAGE

That's good, it's easy for Facebook users, it's great for the companies as people may talk about them or their products easily... Then, where is the problem? Well, we're talking about websites, and with some simple javascript code, we can "corrupt" the original use that was given to this functionality.

Imagine that we add to the PandaLabs blog an icon so that you can say that you like PandaLabs. You'll think that your Facebook account will be updated with the information that you like Pandalabs. But, what if we've changed the code to "to know that he is dummy"? In Facebook, you'll see the following text: **"Luis likes to know that he is dummy"**. Well, this is not so serious, it's just a joke. We could make it more interesting, We could add a link promising that if you click on it, you'll participate in the draw of an iPad, but instead THE TEXT I WANT will be displayed in Facebook.

But let's put ourselves in a cybercrook's place, who is looking for money. They may want to earn money by making you visit for example a website which contains advertisements. Or even worse, which distributes malware and we get infected by rogueware, Trojans, etc. For the moment we've not seen any case of malware distribution, but it's just a matter of time.

In the last weeks we've seen many cases which use baits like "101 Hottest Women in the World", "Farmville" or "Sex & the City 2", promising us to access the content about the topic of the site, to watch a video, etc. and the only thing that happens is that it is being distributed by appearing in Facebook and making all the friends that follow the link fall into the trap.

A good advice: be distrustful, don't trust anything and disable javascript in your browsers.

New phishing techniques (Tabnabbing)

There's a saying in the IT world which cyber-criminals probably bear in mind when planning their attacks. It goes like this: *"The most destructive virus sits between the keyboard and the chair"*.

Why design complex algorithms and spend hours detecting programming errors, when users are the most vulnerable point of any computer? This is what many criminal mafias believe, and they have consequently found numerous original ways of getting users to fall into their traps.

This is a new phishing concept which was first documented in May 2010. We don't know if it's really been used or whether it's simply a proof of concept, but it provides an insight into the way in which our behavior is analyzed.

Tabnabbing consists of exploiting the tab browsing system to make users believe they are in a familiar Web page such as Gmail, Hotmail, Facebook... and stealing their passwords.

Many people tend to keep numerous tabs open in their browsers, and they often lose track of how many are open, or even open the same Web page more than once.

FIG. 13

VIEW OF A BROWSER WITH SEVERAL TABS OPEN

In order to return to a Web page, they use the *favicon* or website icon, in addition to the title, and don't usually pay attention to the address displayed in the browser bar.

This behavior could be exploited to get users to access a fake Web page and compromise their passwords.

The *modus operandi* is quite simple.

1. Get users to access the fake Web page. There are multiple possibilities; from traditional spam, to messages via social networks, forums, etc.

2. Use JavaScript to detect when the fake Web page is no longer being viewed (users have accessed a different tab, program or browser). A few seconds later (to make sure users have forgotten about this tab), and also using JavaScript the *favicon*, title and content of the Web page can be modified so it resembles a known service page. We will use Gmail as an example.

3. Having browsed through different Web pages and opened numerous tabs, if users want to access their Gmail email, for example, they check whether the corresponding tab is open. In this case, it is the fake Gmail Web page. Users cannot remember when they accessed the Web page and on seeing the login form assume they opened it a long time ago and the session has expired.

4. On entering their credentials, the fake page stores the data and redirects users to the original page.

Users aren't aware their credentials have been compromised and these can now be used by criminals.

We don't want to alarm you, but you should keep your guard up every day and be wary of any strange things you believe are caused by your forgetfulness. Only this together with the implementation of adequate security policies will allow you to use your computer without fear of becoming a victim of social engineering tricks.

Many specialists claim the user name and password login system is obsolete and it is browsers themselves that have to migrate to more secure systems such as the "Account Manager" proposed by Mozilla Labs a few months ago.

Smartphones: target for hackers?

We have previously mentioned in reports that the emergence of malware for any platform depends on its profitability. Consequently, malware is normally created to target the market-leading platforms, those with a high number of users, in order to justify the time invested by cyber-crooks in R+D worthwhile.

It seemed at one point as though Symbian was likely to dominate the smartphone market, and as such it was the first platform targeted by malware.

As new platforms such as iPhone and Android appeared, Symbian's popularity evaporated, as did the malware designed to target it

Additionally, from version 9 of Symbian, security policies became stricter, which made malware creation and 'homebrew' development more difficult. Symbian is therefore no longer cyber-crooks' main target.

It seems like Android and iPhone will now be in hackers' sights, but we don't know which platform they will target most, as it depends on their profitability. There are several arguments for both: Apple or Google, "techie" or general public, control in the Market/Store...

Although Symbian still tops markets such as Asia and Africa smartphone markets, the global data paints a different picture:

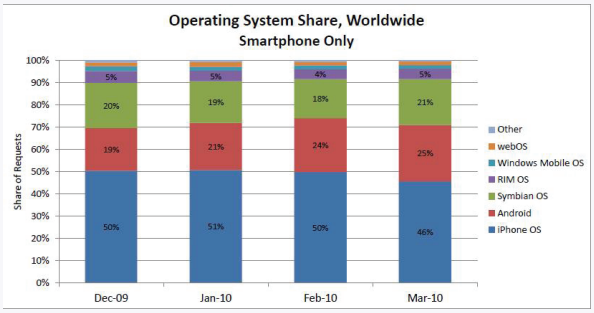


FIG. 14

DISTRIBUTION OF OS FOR MOBILES

SOURCE: adMob

As you can see, iPhone dominates the global market, thanks to its strength in the principal markets. It is also interesting to take a look at the United States. As one of the most important markets, its trends could be extrapolated to the rest of the countries in the near future:

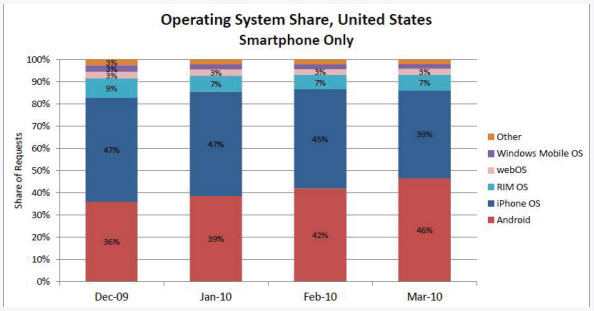


FIG.15

DISTRIBUTION OF OS FOR MOBILES IN THE US
SOURCE: adMob

According to adMob's data, the traffic generated by Android smartphones in the US exceeded that of iPhone smartphones. Bearing in mind the distribution of Android smartphones is not evenly spread around the globe (they are still not available in many countries), and the fact that smartphones based on Linux or on other open platforms are highly successful in Asian countries, Android could well become the mainstream smartphone platform.

However, only time will tell which platforms cyber-crooks decide to target. Even so, you should always keep your guard up in order to remain One Step Ahead.

Vulnerabilities

At the beginning of April we saw an update to correct a vulnerability in Firefox during the *Pwn2Own* competition at the **CanSecWest** security conference in Vancouver.

In the same month, Apache released a notice revealing that its infrastructure had been compromised through the exploitation of an unknown vulnerability in its error and incident management software, JIRA. The report explained that the attackers had exploited an XSS vulnerability to compromise several user sessions, including various accounts with administrator privileges.

It would seem that a malicious link was hidden in the URL shortening services frequently used on social networks to avoid exceeding the maximum limit when creating messages on services such as Twitter or Facebook. What does the following URL hide? **http://tinyurl.com/yd5dm77**.

And neither are social networks free from security holes. A TechCrunch **article** explains how it was possible for any Facebook user to view conversations of their friends with other people in real time. Once again, these security holes are a timely reminder of how important it is to be careful about the information you share on these types of networks. A few hours later, the organization released the following communiqué:

"For a limited period of time, a bug permitted some users' chat messages and pending friend requests to be made visible to their friends by manipulating the "preview my profile" feature of Facebook privacy settings. When we received reports of the problem, our engineers promptly diagnosed it and temporarily disabled the chat function. We also pushed out a fix to take care of the visible friend requests which is now complete. Chat will be turned back on across the site shortly. We worked quickly to resolve this matter, ensuring that once the bug was reported to us, a solution was quickly found and implemented."

Although Facebook claims that the bug was present for a limited period of time, there are still questions to ask. For how long was it being exploited? For how long was users' privacy compromised? Is it still vulnerable?

Let's move on now to the world of databases, in fact to one of the biggest of them all, Oracle, who started out this quarter correcting 47 vulnerabilities, of which just 19 were exploited only if the attacker had authenticated. That means 28 vulnerabilities could be exploited by users without prior authentication. Applications and services affected by these 28 vulnerabilities include *Oracle Fusion Middleware*, *Oracle Collaboration Suite*, *Oracle E-Bussines Suite*, *Oracle PeopleSoft Enterprise*, *JID Edwards EnterpriseOne* and *Oracle Industry Suite*.

Similarly, Microsoft continues to publish its monthly security bulletins every second Tuesday of the month. Among those corrected were the five vulnerabilities announced in **MS10-020**, which allowed remote execution of code through a malformed SMB reply, and affected all versions of Microsoft Windows.

A vulnerability corrected in **MS10-026** allowed execution of code when a user opened an AVI file containing an MP3 audio track designed to exploit the vulnerability. The problem centered on Microsoft's MP3 codec. This problem, however, did not affect Windows 7. Interestingly, in this cycle of security fixes, Microsoft was forced to republish bulletin **MS10-025**, as it did not adequately remedy the vulnerability affecting the *Windows Media Unicast Service* on Windows 2000 with Service Pack 4.

The **MS10-040** bulletin corrected a remote code execution vulnerability allowing an attacker to run code remotely on IIS 6 and IIS7, installed on Windows Server 2003, Windows Vista and Windows Server 2008. The vulnerability occurs when the Internet Information Services Web server does not correctly allocate memory when analyzing authentication information received from the client. These commands are run with WPI rights, which is configured by default with network service account privileges. However, if there are IIS servers whose application groups are configured with a WPI using an account with administrator privileges, these can be seriously affected.

Microsoft still have an unpatched vulnerability, discovered by the well-known Google researcher, Tavis Ormandy. On June 9, he published a vulnerability that affected Windows Help. This vulnerability allows execution of commands on Windows XP and Windows 2003. Microsoft **says** that the Google researcher has not given them sufficient time to correct the vulnerability and thereby protect clients. It also claims that the solution proposed by Google is incomplete and easily circumvented.

"Without giving us time to resolve the issue for our potentially affected customers, makes broad attacks more likely and puts customers at risk."

"While this was a good find by the Google researcher, it turns out that the analysis is incomplete and the actual workaround Google suggested is easily circumvented."

Nevertheless, Microsoft has published a **workaround** to mitigate the threat to vulnerable systems, although it has not prevented the first functional attacks being launched by cyber-crooks.

Adobe has also been kept busy this quarter. Not only have Reader and Acrobat had their share of vulnerabilities, but also versions CS3 and CS4 of Adobe Photoshop, which are vulnerable through the incorrect processing of TIFF images. This vulnerability allows remote execution of code on Windows and Mac.

Finally, we would also like to mention the latest **critical vulnerability** reported in Adobe Reader and Adobe Acrobat which are currently being exploited on the Internet. The problem lies in version 10.0.45.2 of Adobe Flash Player, as well as in previous versions, along with the autoplay.dll included in Adobe Reader and Acrobat 9.x. This vulnerability allows code to be run on compromised systems.

As a workaround, Adobe advises deleting or renaming the *autoplay.dll* library on Windows, *libauthplay.so.0.0.0* on Linux and Solaris and *AuthPlayLib.bundle* on Mac. Adobe says that certain errors and error messages may occur when trying to view a PDF with SWF content.

Adobe intends to resolve this incident on June 29. Nevertheless, thanks to TruPrevent, users with Panda Security solutions installed are protected against this zero-day attack.

Our colleague Sean-Paul Correll has prepared a video demonstrating how the new version of **Panda Cloud Antivirus** with TruPrevent technologies has protected our clients against this zero-day attack, even before it appeared and before the developer produced a real solution to the vulnerability. The workaround proposed by Adobe affects the product functionality, while Panda Cloud Antivirus does not diminish the product's feature and just blocks malicious PDF.

Nobody now doubts that there is more malware in circulation than ever. When just a few years ago we started to speak of an exponential growth in threats, users seemed not so sure. Today, this is not only a proven fact, but cyber-crime is actually continuing to grow. And it is not just new strains of malware that are increasing. There are numerous variants to existing versions, designed to foil the security measures put in place by antivirus companies.

This should not surprise us given that cyber-criminals now offer services enabling even users with limited IT knowledge to create malware with a wide range of functions, including evading detection by security products.

There are tools that allow users without advanced IT knowledge to create malware

Such was the case with the Internet portal selling **undetectable bots**, which was uncovered in May, specialized above all in targeting social networks. This would seem to be the perfect combination: undetectable malware and social networks.

The malware we have received at the laboratory during the second quarter of this year can be broken down as follows:

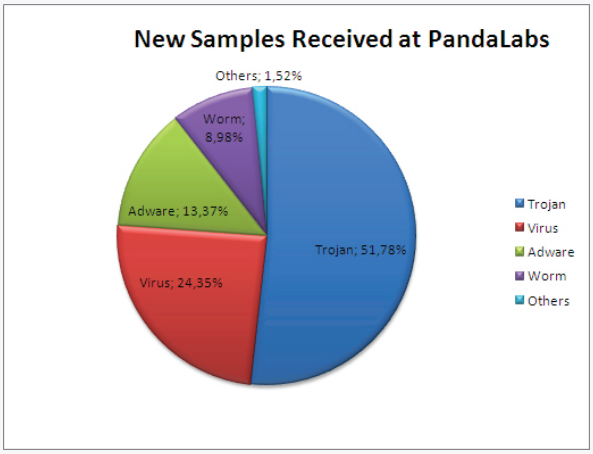


FIG.16

NEW MALWARE RECEIVED AT PANDALABS

Trojans continue to rank as the weapon of choice of cyber-criminals, given that most of their revenue comes through identity theft or stolen bank and credit card details. As such, Trojans accounted for 52% of all malware created during Q2. The next category was viruses, which totaled just over 24.35%. Comparing this figure with the previous quarter (15.13%), it is clear that viruses continue to gain ground.

This might seem to indicate that traditional malware has made a comeback, but that is not the case. Bear in mind that this just reflects the number of virus samples received, and although this figure has increased, it does not mean that the number of different viruses that have appeared over this period has increased. This is better demonstrated perhaps, by the number of infections, where it is clear that the number of computers infected by, say, Trojans, is several times higher than the number infected by viruses. We will see this in more detail later.

The figures for adware continue much in the same vein as for the previous quarter, in third place with 13.37%. This category includes malicious programs such as rogueware or fake antivirus products, which have continued to grow since they first appeared two years ago. As with Trojans, the reason for the existence of rogueware is purely financial. Following this with 9%, come some more usual suspects, worms.

It would seem that the sale of details of users' Internet habits is no longer of much interest in the world of stolen information. From the first quarter of 2010, spyware seemed to be taking a nosedive, accounting for just 0.29% of the total. And this quarter the decline has continued, with the measly figure of just 0.16%. Consequently, this category has now been relegated to the 'Others' section.

The 'Others' category includes all those types of threats which, even combined, account for a minimal percentage (1.52%) of the total. This includes the following categories:

Dialer	30.53%
PUP (Potentially Unwanted Program)	28.45%
Hacking tool	17.36%
Security risk	13.08%
Spyware	10.58%

Global distribution of malware

In the previous section we described the distribution of the main malware categories on the basis of the samples received at PandaLabs.

In this section we will be looking at how malware is distributed around the world, analyzing the situation in several countries. First of all, let's see the following graphic which illustrates the worldwide distribution of malware infections by type:

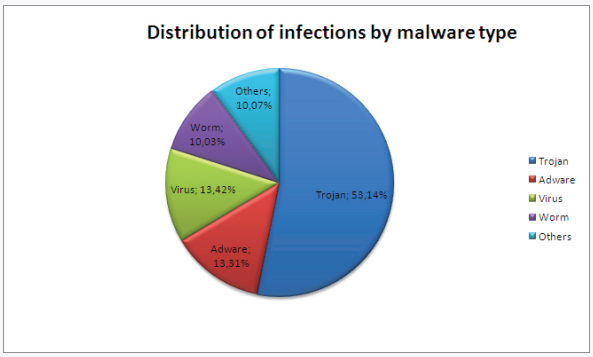


FIG.17

DISTRIBUTION OF MALWARE INFECTIONS BY TYPE

Predictably, Trojans lead the way, as they are the tool most frequently used by criminals to steal information. More than half of the computers infected were the victims of Trojans. Viruses and worms however account for less than half of the number of infections as Trojans, despite being designed specifically to spread to other systems.

The following graph reflects data obtained through scans performed using the **ActiveScan 2.0** online tool. This service allows users to run free online scans of their computers, and check whether they are infected or not.

This data 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.

Below you can see the countries with the highest percentages of infections:

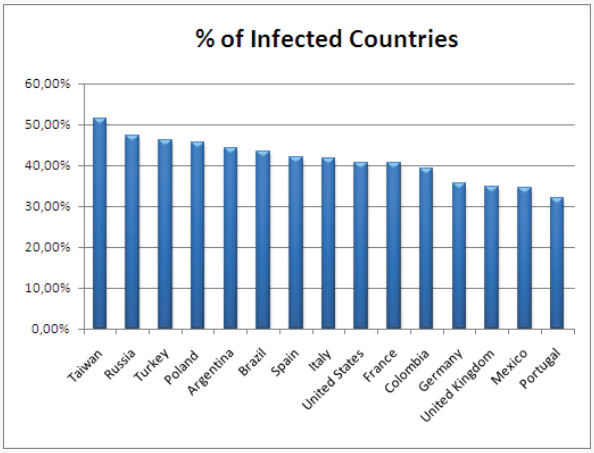


FIG.18

COUNTRIES WITH MOST INFECTIONS OVER THE LAST QUARTER

With respect to the most prolific threat, in many countries Trojans are way ahead of any other category:

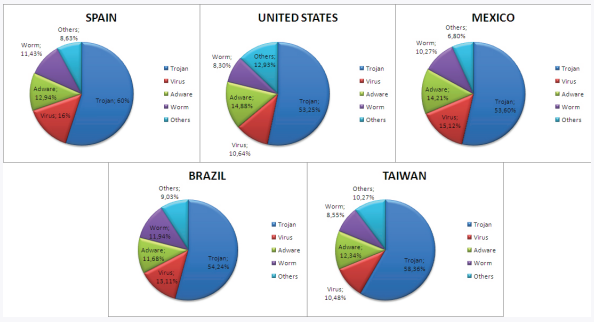


FIG.19

INFECTIONS BY COUNTRY

The percentage of Trojans in all countries is over the 50% mark, highlighting the preference among cyber-criminals for this type of malware, primarily used for stealing information.

If we compare this with the previous quarter, all countries have seen an increase in all categories, except worms, which have decreased slightly. However, the increase in Trojans is most significant. For example, in the case of Spain the figure went from under 50% last quarter to over 60% in Q2.

The following graph shows how this category has evolved in the first two quarters of 2010:

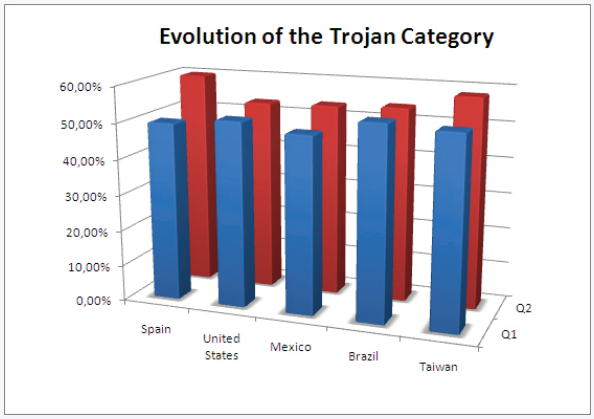


FIG.20

EVOLUTION OF TROJANS IN Q1 AND Q2

Spam info

Every day, users' inboxes are saturated with avalanches of spam. It comes in many forms, plain text, HTML, images, PDFs, even MP3.

Even so, as users we are becoming accustomed to it, and as such most of us are getting better at identifying spam at a glance. Also, if we consider the improved anti-spam filters offered by email services, it would seem that the net is closing around spammers.

However, cyber-crooks are always coming up with new ideas for sneaking past anti-spam filters and for tricking users. Even so, traditional spam messages are still very much in use, and the global figure for spam currently runs into thousands of millions of messages circulated every day.

Most spam is now generated through botnets. Compromised computers that make up these botnets are distributed around the world but, where are the greatest concentrations of spam?

As illustrated in the following graph, over half the spam we received in our laboratory in March, April and May had been originally sent from just 10 countries:

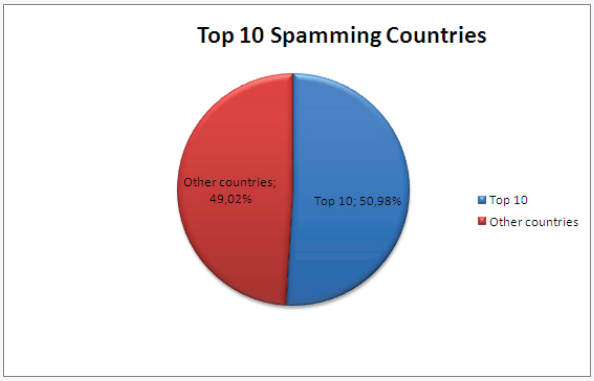


FIG.21

TOP 10 SENDERS OF SPAM

The following graph details which countries are behind the statistics:

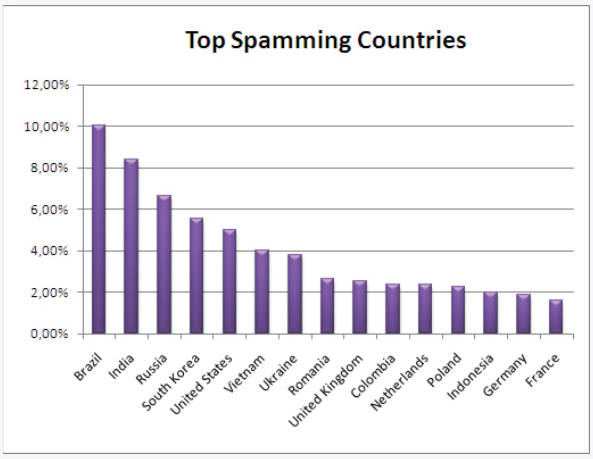


FIG.22

TOP COUNTRIES SENDING SPAM

Brazil continues to be the country responsible for most spam, accounting for more than 10% of the total; in the previous quarter, almost 20% of spam was sent from the country. India ranks in second place, with just over 8%, followed by Russia (6.64%), South Korea (5.54%), USA (5%) and Vietnam (4.02%). All remaining countries each account for less than 4%.

Conclusions

It's clear there has been much activity over the last quarter, and in this report we have only looked at the most significant events. And if we could make a wish, it would be for Adobe to get moving and give security the importance it deserves, otherwise it will continue to be responsible, albeit indirectly, for many infections.

Over the next few months, social networks will continue to be the center of attention, as cyber-criminals keep looking for new ways to reach users. Users must demand clear options to protect their privacy, and if a new option to share information is added, it should not be enabled by default. This is an error Facebook has made all too often.

In the second half of the year we will see tablet PCs based on Android and Windows 7, along with new security challenges.

Stay up-to-date on **our blog**, where we offer the latest news about malware and security.

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, refer to the **PandaLabs** blog at: **http://pandalabs.pandasecurity.com/**.