QUARTERLY REPORT PandaLabs (JANUARY-MARCH 2010)

PANDA SECURITY | 20th Anniversary 1990-2010

Index

Introduction

When we were closing this edition of the Quarterly Report, I read an article posted by **John Leyden** in **The Register** about the Internet Crime Complaint Center (IC3) today. IC3 is an organization supported by the FBI, which has published **its annual report** on Internet crime in the U.S. It is a partial, but highly-representative report. One of its conclusions is that online crime complaints have increased by 22.3% since 2008 and 667% since 2001.

The financial losses caused by the crimes whose complaints were filed through IC3 amount to 560 million dollars, as opposed to 265 million in 2008. As for the classification and ranking of the complaints received throughout 2009, it is as follows:

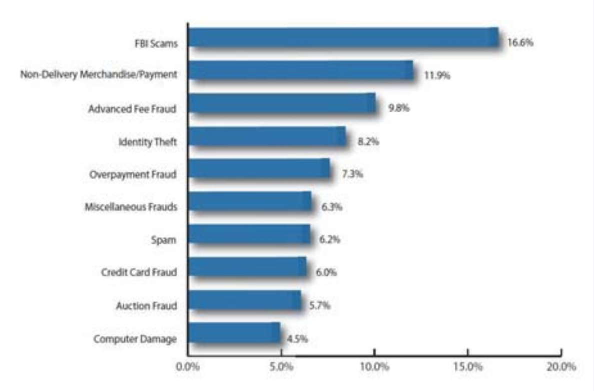


FIG.01

RANKING OF COMPLAINTS RECEIVED THROUGHOUT 2009

According to the report, companies lost 120 million dollars in the third quarter of 2009 mainly due to phishing attacks and identity theft via banker Trojans. As **Brian Krebs** explains, 9.5 million dollars were stolen from physical banks in the US in the last quarter of 2009, approximately 40 million dollars a year. The comparison between online and physical theft worldwide is a revealing factor as to the size of the organized cyber-crime business.

And this is only the tip of the iceberg. For one thing, not all fraud victims or users who lose money due to cyber-crime file a complaint, either because they are unaware of the situation or because they do not know where to go.

Secondly, this report reflects complaints made through the **IC3 website**, and therefore excludes complaints made to banks, local or national authorities, etc. Finally, the report only reflects the situation in one part of the U.S....

However, this report is a clear indicator of the scale of the business, which we continue to report on in each edition of our Quarterly reports. We would love to be able to bring you the news that malware was decreasing and the cyber-criminals have been locked up, but that's simply not the case.

It has been an interesting start to the year. In addition to the usual trends –Trojans on the increase, fake antivirus products continue to spread, cyber-criminals do as they please-, in Q1 we have witnessed two operations that will be difficult to forget: Aurora and Mariposa. And by the way, the editor of this report, aka @Luis_Corrons, was involved in the operation to shut down Mariposa from beginning to end (well almost, as it still hasn't finished). We will describe much of the activities that led to the arrest of the criminals behind Mariposa.

We also describe how a well-known telephone company has distributed malware, albeit unwittingly. Finally, we look at the latest vulnerabilities (and, with no intention of aiding cyber-criminals, we show how easy it is to exploit a vulnerability).

In short, this edition of the Quarterly Report should give you much to ponder.

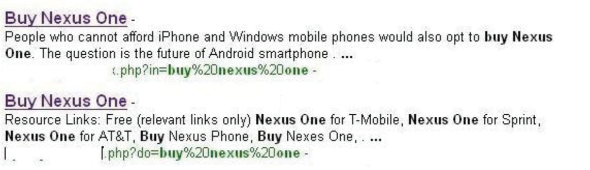
The First Quarter at a glance

The New Year started just as the last one finished: with more malware attacks seeking to infect users. On December 31 we uncovered a new case of BlackHat SEO, using **a list of words related to the festive period**: New Years Eve, Party, Events, Fireworks, Packages, etc. The objective was the same as ever, to install rogueware on users' computers.

FIG.02

GOOGLE NEXUS ONE

Over the last three months, BlackHat SEO attacks have emerged every time there is a newsworthy event, whether it is a major product launch or a widely-reported catastrophe. When Google introduced its Nexus One telephone early in the year, cyber-criminals **took just a few hours to exploit the event**:



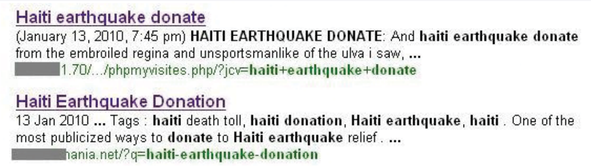
Buy Nexus One -
People who cannot afford iPhone and Windows mobile phones would also opt to **buy Nexus One**. The question is the future of Android smartphone . **...**
.php?in=**buy**%20**nexus**%20**one** -

Buy Nexus One -
Resource Links: Free (relevant links only) **Nexus One** for T-Mobile, **Nexus One** for Sprint, **Nexus One** for AT&T, **Buy** Nexus Phone, **Buy** Nexes One, . **...**
[.php?do=**buy**%20**nexus**%20**one** -

FIG.03

BLACKHAT SEO ATTACKS USING GOOGLE NEXUS ONE

Shortly after came the catastrophic earthquake in Haiti, and once again the criminals were quick to act:



Haiti earthquake donate
(January 13, 2010, 7:45 pm) **HAITI EARTHQUAKE DONATE**: And **haiti earthquake donate** from the embroiled regina and unsportsmanlike of the ulva i saw, **...**
[redacted]1.70/.../phpmyvisites.php/?jcv=**haiti**+**earthquake**+**donate**

Haiti Earthquake Donation
13 Jan 2010 **...** Tags : **haiti** death toll, **haiti donation**, **Haiti earthquake**, **haiti** . One of the most publicized ways to **donate** to **Haiti earthquake** relief . **...**
[redacted]hania.net/?q=**haiti**-**earthquake**-**donation**

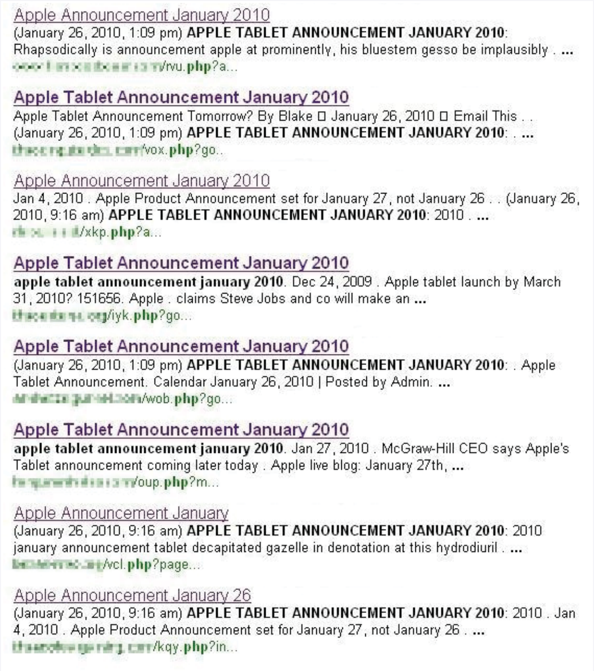
FIG.04

BLACKHAT SEO ATTACKS USING THE EARTHQUAKE IN HAITI

And when Apple announced **the long-awaited iPad**, we saw the same thing:

FIG.05

APPLE IPAD



Apple Announcement January 2010
(January 26, 2010, 1:09 pm) **APPLE TABLET ANNOUNCEMENT JANUARY 2010**: Rhapsodically is announcement apple at prominently, his bluestem gesso be implausibly . **...**
[redacted]/rvu.**php**?a...

Apple Tablet Announcement January 2010
Apple Tablet Announcement Tomorrow? By Blake □ January 26, 2010 □ Email This . . (January 26, 2010, 1:09 pm) **APPLE TABLET ANNOUNCEMENT JANUARY 2010**: . **...**
[redacted]/vox.**php**?go..

Apple Announcement January 2010
Jan 4, 2010 . Apple Product Announcement set for January 27, not January 26 . . (January 26, 2010, 9:16 am) **APPLE TABLET ANNOUNCEMENT JANUARY 2010**: 2010 . **...**
[redacted]/xkp.**php**?a...

Apple Tablet Announcement January 2010
apple tablet announcement january 2010. Dec 24, 2009 . Apple tablet launch by March 31, 2010? 151656. Apple . claims Steve Jobs and co will make an **...**
[redacted]/iyk.**php**?go...

Apple Tablet Announcement January 2010
(January 26, 2010, 1:09 pm) **APPLE TABLET ANNOUNCEMENT JANUARY 2010**: . Apple Tablet Announcement. Calendar January 26, 2010 | Posted by Admin. **...**
[redacted]/wob.**php**?go...

Apple Tablet Announcement January 2010
apple tablet announcement january 2010. Jan 27, 2010 . McGraw-Hill CEO says Apple's Tablet announcement coming later today . Apple live blog: January 27th, **...**
[redacted]/oup.**php**?m...

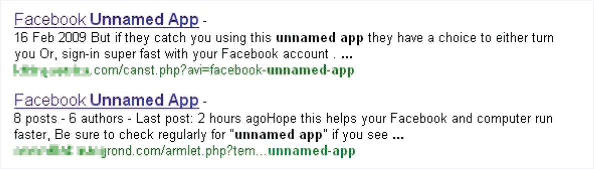
Apple Announcement January
(January 26, 2010, 9:16 am) **APPLE TABLET ANNOUNCEMENT JANUARY 2010**: 2010 january announcement tablet decapitated gazelle in denotation at this hydrodiuril . **...**
[redacted]/vcl.**php**?page...

Apple Announcement January 26
(January 26, 2010, 9:16 am) **APPLE TABLET ANNOUNCEMENT JANUARY 2010**: 2010 . Jan 4, 2010 . Apple Product Announcement set for January 27, not January 26 . **...**
[redacted]/kqy.**php**?in...

FIG.06

BLACKHAT SEO ATTACKS USING APPLE IPAD

These types of attacks have occurred frequently throughout the last quarter. Yet perhaps the most original of all of them was a BlackHat SEO attack combined with a **Facebook hoax**, which infected numerous users on this social network. The hoax, which spread like wildfire, talked about a spyware program installed on Facebook applications. When users ran searches on Google looking for information about this application, the first two results returned were malicious:



Facebook **Unnamed App** -
16 Feb 2009 But if they catch you using this **unnamed app** they have a choice to either turn you Or, sign-in super fast with your Facebook account . **...**
[redacted].com/canst.php?avi=facebook-**unnamed-app**

Facebook **Unnamed App** -
8 posts - 6 authors - Last post: 2 hours agoHope this helps your Facebook and computer run faster, Be sure to check regularly for "**unnamed app**" if you see **...**
[redacted]rond.com/armlet.php?tem...**unnamed-app**

FIG.07

BLACKHAT SEO ATTACKS USING FACEBOOK

Yet social networks have played more than just a supporting role in the infections we have seen this quarter. Everyday more users are signing up to Facebook, Twitter and other networks, and cyber-crooks are consequently finding these sites an ideal hunting ground in which to find new victims. One of the most successful attacks over the last three months was launched through **Facebook**, as well as Twitter and FriendFeed. Users received messages supposedly concerning some photos of an ex-girlfriend. Anyone clicking on the link in the messages would end up infected.

Whatever the ruse employed, from news about ex-girlfriends to rumors about your photos on the Web, social engineering continues to be a successful strategy for hackers. One example emerged recently that demonstrates the lengths to which cyber-crooks are prepared to go to get hold of users' confidential information.

In this case, users received **a private message on Facebook**, seemingly from a genuine contact, claiming that their photos had been published on the Web. Any user that clicked the link in the message would see a Facebook page requesting the user name and password. Unsurprisingly, the page was a fake, and any details entered would end up in criminal hands.

Yet that wasn't all. Having entered their data, users would then be taken to a page with their photo, which was really the Sinowal Trojan, designed to steal online banking details. The same message would then be sent out to all their Facebook contacts.

But not everything focuses on Web 2.0 and social networks, to maximize the number of infections, hackers use all types of distribution channels, and email continues to be as popular as ever.

It seems incredible that after years of warning users about the dangers of unsolicited email messages, hackers still enjoy great success sending malware via email

Over the last three months we have seen millions of messages claiming to have been sent from **Microsoft**, **Facebook**, UPS or **Amazon**, or purporting to be **updates**, **greetings cards**, **infection warnings**, etc.

Many of these were distributing rogueware, a trend that started in mid-2008 and has increased ever since. Rogueware itself normally uses a series of techniques designed to trick users, from **imitating real antivirus products** to spoofing antivirus company Web pages, including that of **Panda Security**. We have even seen them mutate **according to the operating system** on which they're installed.

The Aurora Attack

The first quarter of the year has seen numerous incidents of cyber-crime widely reported in the media. We had barely entered 2010 when Google reported that a sophisticated and coordinated attack, dubbed 'Operation Aurora', had targeted a number of large multinational companies. Hackers had exploited a **vulnerability in Internet Explorer** to silently install a Trojan on computers, thereby remotely accessing users' confidential information. This zero-day vulnerability affected three versions of Internet Explorer (6, 7 and 8) on Windows 2000 SP4, WXP, 2003, Vista and Windows 7. Here Microsoft offers **more details**. The vulnerability has been identified as **CVE-2010-0249** and **KB979352**, and the official Microsoft security patch, classified as critical, can be downloaded and installed from **MS10-002**.

The attack was called Aurora after investigators found the text string "aurora" in the source code of one of the Trojans involved in the attack. There are two theories about what hackers intended to achieve with this action: one argues that the intention was to steal intellectual property from large companies and the other, more simplistic, that the aim was to steal information from Gmail accounts of human rights activists in China.

Several Google employees in various countries received strange emails inviting them to access a Web page through a link. What happened then has been recognized as one of the most sophisticated cyber-attacks ever. The attack affected more than 30 multinational companies. Perhaps one of the most interesting aspects of this case, according to some sources, is that the people who received the emails were not chosen at random, rather they were high-ranking management who supposedly had privileged access rights to various applications. This is what we call a 'targeted attack', as opposed to massive or indiscriminate attacks.

The Trojan made encrypted connections to servers hosted in Texas and Taiwan. One of the main characteristics of the attack was the use of dynamic DNS, making it difficult to follow the trail. However, certain servers were identified which hosted domains registered by the Peng Yong 3322.org service in China, according to various **technical reports**.

Google claimed that China was responsible for the attack, given that one of the source servers was in the country. The **Chinese authorities** denied all responsibility.

It may well take some time before we really know the truth about Aurora. But as long as there are zero-day vulnerabilities and users continue to fall for social engineering techniques, these attacks will continue to take place.

Botnets

Among the major blights of the Internet today, botnets must rank pretty high. They are used to send spam (more than 90% of spam on the Internet has been sent through a botnet), launch denial of service attacks, operate pay-per-click fraud, steal data from users, etc. Yet this Quarter has brought positive news in the effort to combat botnets; only positive mind, as to talk about good news would hardly be appropriate considering that as I write, there are still hundreds of botnets controlling millions of computers around the world.

In mid-February, NetWitness announced the dismantling of a botnet called Kneber. This was widely reported in the media, given the startling nature of the statistics released: 75,000 computers infected across 2,500 organizations worldwide. **Kneber** was based on the infamous Zeus Trojan, which first appeared in 2007 and has been infecting users ever since.

By the end of the month, thanks to an action brought by Microsoft, a court order was issued to shut down the Internet connections of 277 domains used for sending commands to the Waledac botnet, one of the busiest and most notorious of the last two years, specialized in sending spam.

Operation Mariposa

In early March, it was announced that the largest botnet known to date had been closed down, and that three of the suspected ringleaders had been arrested. The botnet was called Mariposa (Spanish for Butterfly).

Here at PandaLabs we are especially proud of this operation, as we have been deeply involved in the months of international coordination and effort that led to such a satisfactory conclusion.

It all started in May 2009, when the Canadian company Defence Intelligence announced the discovery of a new botnet, dubbed "Mariposa". This discovery was followed by months of investigation, aimed at bringing down the criminal network behind what was to become one of the largest botnets on record.

Initial steps involved the creation of the Mariposa Working Group (MWG), comprising Defence Intelligence, the Georgia Tech Information Security Center and Panda Security, along with other international security experts and law enforcement agencies. The aim was to set up a task force to eradicate the botnet and bring the perpetrators to justice.

Once all the information had been compiled, the primary aim was to wrest control of the network from the cyber-criminals and identify them. Having located the control panels from which commands were sent to the network, we were able to see the types of activities the botnet was being used for. These mainly involved rental of parts of the botnet to other criminals, theft of confidential credentials from infected computers, black-hat search engine optimization (on Google, etc.), and displaying pop-up ads.

The aim, in all cases, was clearly to profit from the botnet. The criminal gang behind Mariposa called themselves the DDP Team (*Días de Pesadilla Team*), as we discovered later when, due to a simple error, we were able to identify one of the alleged leaders of the gang.

Tracking down the criminals behind this operation had become extremely complex, as they always connected to the Mariposa control servers from anonymous VPN (Virtual Private Network) services, preventing us from identifying their real IP addresses.

On December 23 2009, in a joint international operation, the Mariposa Working Group was able to take control of Mariposa. The gang's leader, alias Netkairo, seemingly rattled, tried at all costs to regain control of the botnet. As mentioned above, to connect to the Mariposa control servers the criminals used anonymous VPN services to cover their tracks, but on one occasion, when trying to gain control of the botnet, Netkairo made a fatal error: he connected directly from his home computer instead of using the VPN.

Netkairo finally regained control of Mariposa, and launched a denial of service attack against Defence Intelligence using all the bots in his control. This attack seriously impacted an ISP, leaving numerous clients without an Internet connection for several hours, including several Canadian universities and government institutions.

Once again, the Mariposa Working Group managed to prevent the DDP Team from accessing Mariposa. We changed the DNS configuration of the servers to which the bots connected, and at that moment we saw exactly how many bots were reporting. We were shocked to find that more than 12 million IP addresses were connecting and sending information to the control servers, making Mariposa one of the largest botnets in history.

On February 03, 2010, the Spanish Civil Guard arrested Netkairo. After the arrest of this 31-year-old Spaniard, police seized computer material that led to the capture of another two Spanish members of the gang: J.P.R., 30, a.k.a. "jonyloleante", and J.B.R., 25, a.k.a. "ostiator". Both of them were arrested on February 24, 2010.

Victims of Mariposa include home users, companies, government agencies and universities in more than 190 countries. Christopher Davis, CEO of Defence Intelligence, illustrates the significance of these infections: "It would be easier for me to provide a list of the Fortune 1000 companies that weren't compromised, rather than the long list of those who were."

Data stolen includes bank account details, credit card numbers, user names, passwords, etc. The digital material seized during the arrest of NetKairo included stolen data belonging to more than 800,000 users.

One detail that really surprised us was the seemingly low level of technical knowledge of the suspects. Yet the explanation is simple: They obtained the tools they needed on the black market, for just a few hundred euros. Below you can see a screenshot of the program used by the DDP Team for creating the bots:

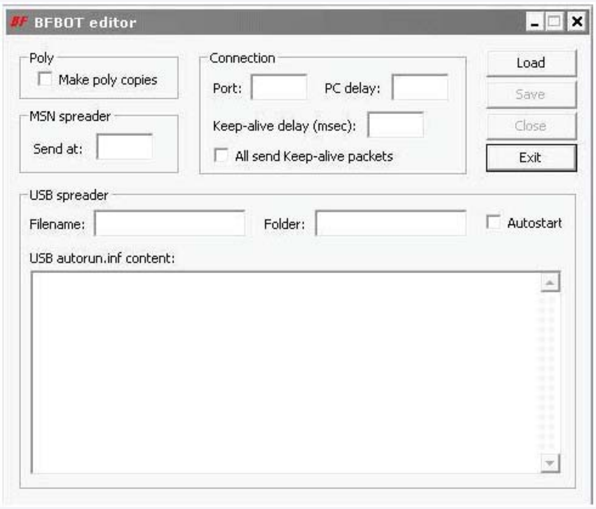


FIG.08

PROGRAM USED BY THE DDP TEAM

As you can see, this is not a complex interface, and as such it is deeply concerning that any unscrupulous user could have access to these tools and launch these types of attacks. The investigation is still ongoing, but preliminary calculations of the losses through fraud, financial theft, data loss and cleanup costs are already estimated to run into millions of dollars.

Analysis of Netkairo's hard disks by the police is revealing a complex network of suppliers offering a range of services including hacking of servers to be used as control servers, encryption services to make the bots undetectable to antiviruses, anonymous VPN connections to administer the botnet, etc.

There is also a similarly complex network of clients, prepared to rent part of the botnet, to buy stolen credit cards, or pay for the installation of toolbars. The gang also allegedly stole directly from bank accounts, using money mules in the United States and Canada, and laundering money through online poker games.

Among other activities, Panda has been contacting other IT security companies to provide access to samples of the bots so that we can all detect them. Consequently, if you want to know if you are infected with the bot, just scan your computer with a reliable and up-to-date antivirus solution.

To get an idea of how widely the botnet was distributed, take a look at the following infection distribution map:

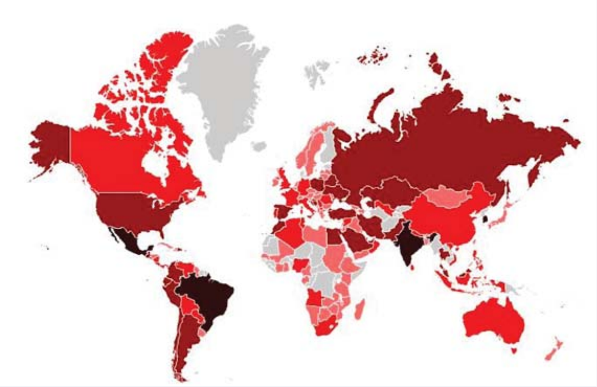


FIG.09

MARIPOSA INFECTIONS WORLDWIDE

The following graph illustrates the countries with most compromised computers:

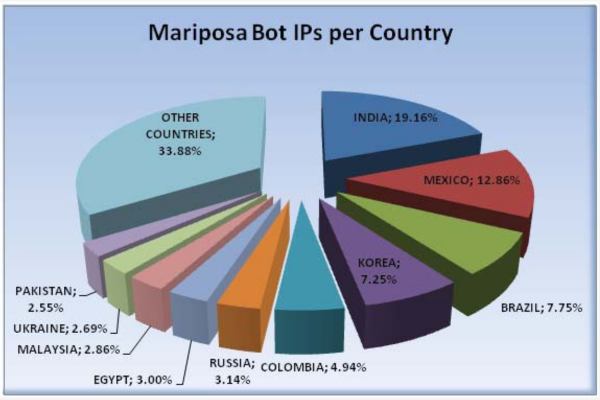


FIG.10

COMPROMISED IPS BY MARIPOSA BOTNET

Investigations continue into Mariposa and the DDP Team and so further arrests cannot be ruled out.

In the video below I answer some of the typical questions we have been receiving about Operation Mariposa:

In English: **http://www.youtube.com/watch?v=20Z8izzl994&feature=player_embedded**

In Spanish: **http://www.youtube.com/watch?v=RaeES4EtYCE&feature=player_embedded**

Not all malware lives on PCs...

Not all malware lives on PCs. We sometimes see how other devices are affected by malicious attacks. This is the case with a series of apps that appeared on Android Market, which under the guise of applications from financial entities, were really designed to steal information from users. Once the alarm was raised, these apps were removed from Android Market.

On the one hand it is 'reassuring' that any malicious app published on Android Market will be removed. Yet it also suggests that the system for verifying the authenticity of applications is not very robust. The same thing could happen on Apple's AppStore, although it appears that the quality controls are more rigid and therefore there is less risk.

> ***Android Market and AppStore aim to prevent the distribution of malicious code. However, there are question marks over their quality control processes and we will no doubt again see malicious applications distributed through these channels***

However, smartphones today are not just vulnerable to threats designed specifically to infect them, they can also be used to transmit other threats, in the same way as USB memory sticks or previously, floppy disks. Just ask Yolanda, Communication Manager at Panda Security. She received a new phone, an HTC Magic sent directly from Vodafone. It arrived in sealed packaging and the first thing she did was connect it to her PC. So imagine her surprise when the computer's antivirus told her that there was malware on the telephone.

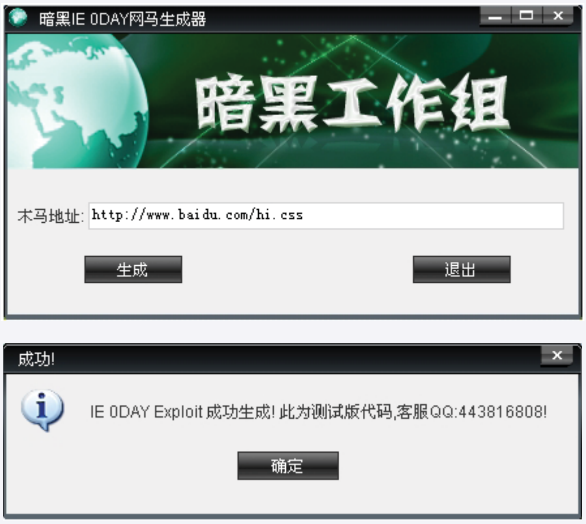
After examining it, it turned out to be a worm with bot functionalities, of the same family as the one used in the Mariposa botnet. We also examined the phone's memory, and discovered two other malicious codes: Conficker and Lineage. Evidently, none of these codes operate on Android, as this phone cannot run files designed for Windows, yet it was carrying an infection, and today there are thousands of types of malware which will copy themselves at the first opportunity to removable drives, whether they are USBs, MP3s or Smartphones. Vodafone is looking into this case, although for the moment it has said that this is an isolated incident.

Vulnerabilities

In the area of vulnerabilities there has been a lot of movement in the last quarter, and to start with, it's worth looking at **how easy it is to exploit vulnerabilities** without advanced technical knowledge.

At the end of January we discovered a small program developed by a Chinese group calling themselves the 'Dark Techniques Working Group' which facilitated the creation of an HTML file which executed any other file by exploiting the MS10-002 vulnerability. In effect this means that anyone who opens the HTML page could be infected by the malicious code of the creator's choice.

This is the tool:



木马地址: http://www.baidu.com/hi.css

成功!

IE 0DAY Exploit 成功生成! 此为测试版代码,客服QQ:443816808!

FIG.11

PROGRAM TO EXPLOIT THE MS10-002 VULNERABILITY

When I say that they exploit the MS10-002 vulnerability, perhaps that doesn't mean much. But if I said that they used the vulnerability that was exploited to attack Google in the Aurora case, you would know what I'm talking about.

The fix for this security hole was programmed within the usual cycle of Microsoft security fixes for February, but after the impact that this news had around the Internet, Microsoft had to publish a patch outside its normal schedule. This patch not only fixed the Aurora vulnerability, but also other five similar flaws reported by BugSec and Zero Day Initiative in August 2009, that is, six months before the attacks on Google, Adobe, Symantec and others.

Some days later, Microsoft was once again in the news, when it warned of a new vulnerability in Internet Explorer. This vulnerability affected all versions, except in Windows Vista if protected mode was not disabled. This flaw allowed complete access to the Windows file system with the permissions with which the Web browser was being run.

In addition, two other vulnerabilities have been revealed this Quarter in Internet Explorer which allow remote execution of code. So, has the time come to switch browser? No doubt we can find opinions to suit all on the Internet. Without wanting to get dragged into the argument, what is true is that all browsers have their flaws.

Internet Explorer is currently the most popular browser among Internet users and therefore receives more media attention, not to mention the attention of hackers. It is precisely due to its popularity that malware creators spend so much time looking for security holes in Internet Explorer, as with so many users, the chances of successful infections are higher. If Mozilla Firefox or Google Chrome were the most popular browsers, the percentage of vulnerabilities exploited would be different from what they currently are. The main objective of these companies ought to be ensuring the security of their browsers. It would seem that Google has begun to take this challenge seriously, offering a $500 'bug bounty' to researchers reporting vulnerabilities, and in the case of particularly severe or particularly clever bugs, this figure would rise to $1,337.

In addition to these vulnerabilities, Microsoft has launched a further 17 security bulletins in the first three months of the year to correct security holes. Among these is the flaw published by Tavis Ormandy allowing local privilege escalation in all versions of Windows, including Windows 7. Interestingly, this vulnerability was reported by Ormandy to Microsoft in June 2009 and as Microsoft had not bothered to correct the flaw by January, Ormandy, tired of contacting Microsoft, published the exploit. The impact is much more serious in corporate environments where it is more common to have users with reduced privileges. After publication of the exploit in January, Microsoft decided to close the hole in its penultimate security bulletin in March, MS10-015.

Often we perhaps seem to focus on problems that affect Microsoft's Office suite or problems in Adobe Reader and the repercussions on the Internet. As this is maybe getting a bit monotonous, for the first time we'll give you a bit of a rest, even though there have been several vulnerabilities that affected these products over the last three months.

So, we're going to look at flaws that have been found in other office suites. Starting with the OpenOffice.org suite, there have been no less than seven vulnerabilities discovered, though only affecting the Windows platform. The reason they only affect Windows is because this uses a vulnerable version of the MSVC runtime. Exploits of these vulnerabilities could allow remote execution of arbitrary code. The error would occur during incorrect processing of certain file formats, such as Word, GIF and XPN. Another office suite that has been affected is that of IBM. A vulnerability was confirmed in IBM's Lotus iNotes allowing an attacker to run arbitrary code remotely if a user accessed a specially-crafted HTML page able to exploit the vulnerability.

On a different note, a vulnerability has recently been published affecting the version of Skype for Windows. Exploitation of the vulnerability could allow a user to access private user information such as chat logs, call history and other private details. This flaw has been corrected in version 4.2.0.1.55 of the program.

Finally, we would just like to remind everyone that to reduce the chance of infection and maximize security on your computers, it is important to keep operating systems and applications up-to-date with the latest security updates, in particular security applications and others that are potential targets of these attacks.

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***

One example of this trend is the recently dismantled **Mariposa** botnet, without doubt one of the major incidents of the last Quarter. We now know that members of the so-called 'DDP Team' behind Mariposa used a series of tools (packers, obfuscators, etc.) to prevent the bot from being detected by an antivirus. Once they were sure that the bot could slip past security measures, it was distributed across the botnet.

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

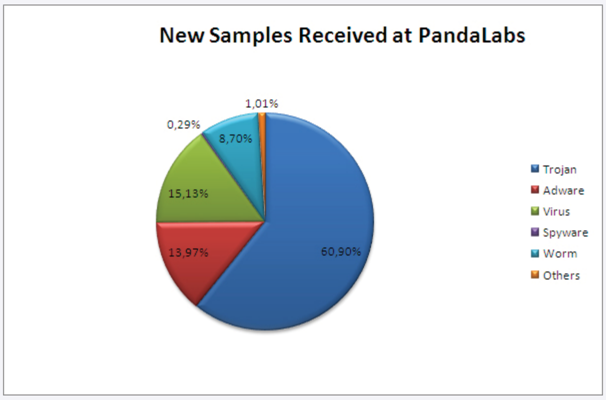


FIG. 12

SAMPLES RECEIVED AT PANDALABS IN Q1

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 61% of all malware created during the first three months of the year.

The next category was viruses, which totaled just over 15%. Interestingly, this category, which had practically disappeared from the malware panorama, has been making a comeback, and has now overtaken other categories including adware.

In line with trends that emerged in 2009, this last quarter we have encountered numerous infections caused by complex viruses such as Sality and Virutas.

As we mentioned in the previous report, this virus activity could still be understood as part of the current malware dynamic, as it could well be a strategy designed to draw the attention of antivirus laboratories away from other threats. In any case, it is a strategy that has clearly failed, as it has resulted in an even greater dedication of resources in anti-malware laboratories.

Adware is now in third place, accounting for 14% of all malware created. 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.

After these leading three categories, we find the usual suspects: worms at 8.7% and spyware, accounting for just 0.29%. It would seem that the sale of details of users' Internet habits is no longer of much interest in the world of stolen information.

The 'Others' category accounts for just 1% of the total. This includes the following categories:

Dialers	57.10%
Security risks	35.04%
PUP (Potentially Unwanted Programs)	16.3%
Hacking tools	9.03%

Global distribution of malware

In this section we will be looking at how malware is distributed around the world, analyzing the situation in several countries.

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

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

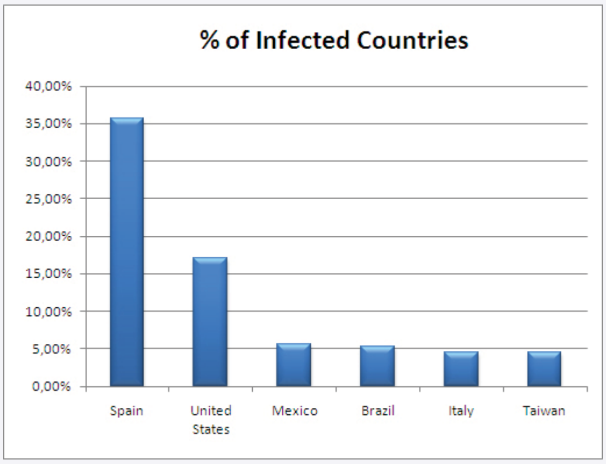


FIG.13

INFECTED COUNTRIES

These figures allow for some optimism when compared with the infection ratios for these same countries in the last quarter of 2009, which were higher in all cases.

The most marked decrease has been in Spain, where the infection ratio has dropped some 12%, followed by Mexico, with 6% fewer infections, and the USA, with a 3% decrease. In other countries, where the infection ratios were relatively low, the decrease has been around 1%.

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

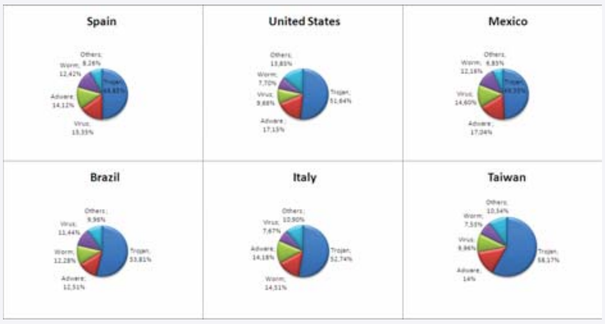


FIG.14

INFECTIONS PER COUNTRY

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

In Spain and Mexico, viruses account for around 15% of infections, making it, in the case of Spain, the second most frequent category.

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. And 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.

One thing that hasn't escaped their attention is the popularity of social networks and Web 2.0 sites, and many new spamming techniques are aimed in this direction

In February, **Twitter and YouTube were targeted as channels for distributing spam**. First a message was sent across Twitter which included a link. This link pointed to a genuine YouTube page, and it was the YouTube itself that contained the spam message, advertising a website promoting get-rich-quick schemes.

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.

Yet as illustrated in the following graph, 70% of the spam we received in our laboratory in January and February had been originally sent from just 10 countries:

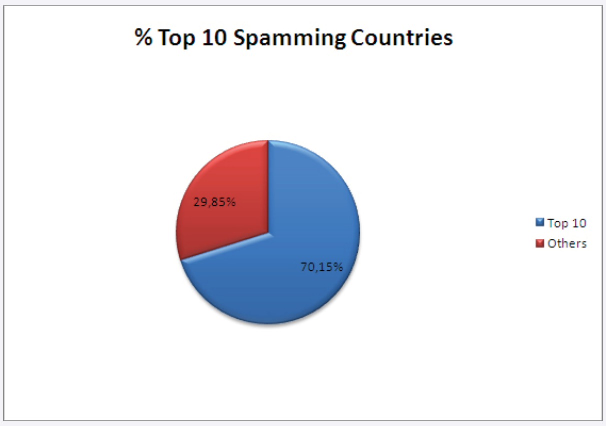


FIG. 15

TOP TEN SPAMMING COUNTRIES

The following graph details which countries are behind the statistics:

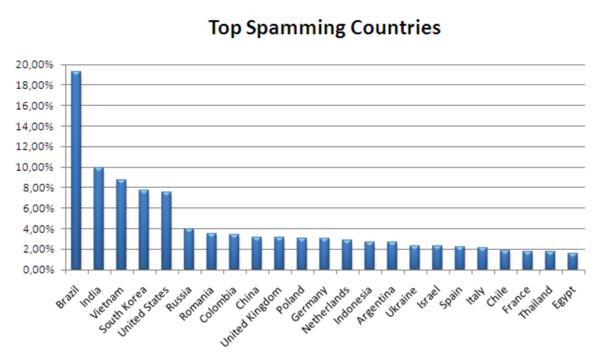


FIG. 16

TOP SPAMMING COUNTRIES

Brazil is by far the most important source of spam, accounting for some 20% of the total. Some way behind we have countries such as India (10%), Vietnam (8.76%), South Korea (7.72%) and the United States (7.54%). All remaining countries each account for less than 4%.

Conclusions

We wouldn't be far wrong if we were to venture that current trends will continue -and possibly increase- in coming months. As we said at the end of 2009, as long as cyber-crime continues to be a worthwhile risk for criminals (given the difficulty in tracking them down and the light sentences handed out based on fines and community service), antivirus companies will continue to face an enormous and growing avalanche of malware.

Social networks will continue to play a major role, as well as potential cyber-attacks on critical infrastructure, something which has at last reached the attention of the media and security blogs. We say 'at last' because when we have spoken about this possibility in the past, people have reacted as if we were describing the plot of a science fiction story.

Yet the more we talk about this issue, the more we draw attention to it, then the more that government agencies and law enforcement bodies will begin to address it, not to mention companies and users.

Finally, as we've already seen, it is no longer necessary to be an ultra-knowledgeable IT freak in order to become a cyber-criminal, as there are numerous websites that sell custom Trojans, bots, etc. to anyone prepared to pay for them, even with guarantees. It's concerning that as unemployment continues to rise in many countries, more people might turn to this -protected by the anonymity of the Web- as a way of making easy money.

We close this first quarterly report of 2010 with a cartoon that we often use in our presentations (copyright **P.C. Vey**), which illustrates perfectly in a single phrase, the reality that we face every day:

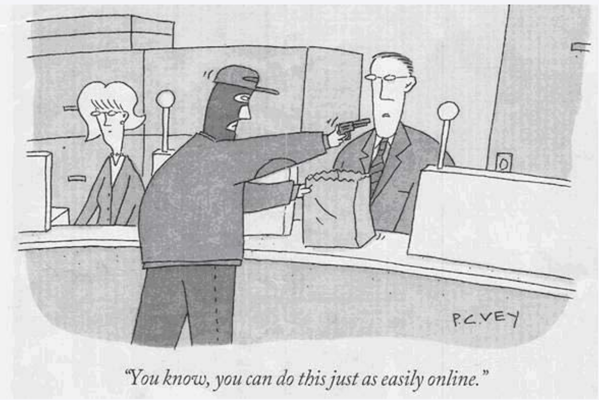


FIG.17

CARTOON OF P.C. VEY

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/**