PandaLabs Quarterly Report

January - March 2012

01 **Introduction**

02 **Q1 at a glance**

- Police Virus Scam
- Mobile Phone Malware
- Social Networks
- Cyber-crime
- Cyber-war
- Anonymous

03 **Quarterly figures**

04 **Conclusion**

05 **About PandaLabs**

06 **Follow us on the web**

01| Introduction

Welcome to 2012, a year which, at least in the computer security arena, promises to be as exciting as last year. In this report we look at the statistics gathered by our cloud-based malware scanning system. The malware situation has turned for worse, and the highlight of the first quarter is the new record set in the creation of Trojan samples (four of every five new malware strains were Trojans).

We analyze some of the attacks witnessed in the first quarter of the year, with a special focus on the widely-spread "Police Virus". Additionally, we report some new attacks exploiting the largest social network, Facebook, as well as the latest activities of the Anonymous hacking group. We also deal with the controversial police operation against Megaupload.

In the cyber-war scene, we will give you the lowdown on the politically-motivated cyber-attacks that took place in the Middle East in January.

We hope you enjoy our Q1 2012 report and find it useful to get ready for what the future holds.

02| Q1 at a Glance

An increase in 'ransonware' attacks has been detected over the past few months, effectively making this technique one of the most 'popular' attack methods ahead of fake antivirus software or rogueware.

Police Virus Scam

While we are used to seeing this kind of fake message in English, in this case the attacks were localized. We saw English, German, Spanish, Dutch and Italian messages (among others) depending on the targeted country. All of the attacks targeted some European nation, so it looks like they were related and the same cyber-criminal gang could be behind them. Let's take a closer look at one of the attacks. The file's icon was the popular logo used by LulzSec in their communications:

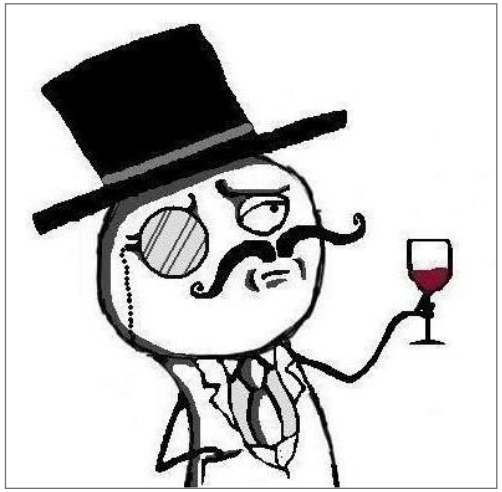


FIG.1. *ICON USED BY ONE OF THE "POLICE VIRUS" VARIANTS.*

Once their computer was infected, the user was confronted with the following full-screen window covering the entire desktop:

FIG.02. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN.*

The message informed the user that they had accessed illegal material (such as child pornography) or sent spam messages with terrorist motives, and their computer had been locked to prevent further abuse. To unlock their computer, they had to pay a €100 'fine'.

The worst thing for the user was that the Trojan actually blocked the computer, so it was not easy to remove it. To do it, the user had to restart the computer in safe mode and run a scan with an antivirus solutions that was able to detect it.

How come the message was displayed in the victim's own language and how did the Trojan purport to come from local authorities? Well, that's easy to explain: After infecting the computer, the malware connected to a certain URL and, based on the victim's IP address, retrieved the localized version of the message that appeared on the computer. Most messages pretended to come from European authorities (although we also saw examples targeting users in other countries, like Canada for example). Below are some examples of similar attacks launched in Q1 2012:

FIG.03. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN GERMAN.*

FIG.04. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN DUTCH.*

FIG.05. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN ITALIAN.*

FIG.03. *RSA SUFRIÓ UNA INTRUSIÓN EN MARZO.*

FIG.06. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN ENGLISH.*

FIG.07. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN SPANISH.*

Mobile Phone Malware

As Android market share continues to grow, so does the amount of malware targeting the platform. In January, Google had to remove several malicious apps from its Android Market (recently renamed to 'Google Play'). Basically, cyber-crooks repackaged popular games like Angry Birds or Cut The Rope with malicious code and uploaded them to Google Play. Users then downloaded and installed the apps unaware that they were also installing a Trojan that sent SMS messages to a premium rate number.

In fact, we learned that Google, tired of the malicious apps found on Google Play, has started analyzing apps before putting them in their catalog in order to detect anomalous behavior. According to their own sources, they have managed to reduce malicious app downloads by 40 percent.

Unfortunately, despite these efforts, criminals continued to target the Android mobile platform through apps not always accessible through Google Play. This was the case of Bmaster, a remote access Trojan (RAT) on the Android platform that tried to pass itself off as a legitimate application.

Social Networks

Facebook continues its reign as the number one social networking site but it also is a favorite target of cyber-crooks. In January, a worm was discovered that had stolen over 45,000 Facebook login credentials. Researchers fear that the criminals used these 'infected' accounts to send links to people's Facebook friends, spreading the computer worm further.

Meanwhile, what does Facebook do to protect users? Well, the good news is that at least they take the fight against cyber-crime seriously.

FIG.08. *FACEBOOK REVEALED THE NAMES OF THE SUSPECTS BEHIND THE KOOBFACE ATTACK.*

In January, Facebook finally revealed the full names and online names of the perpetrators behind the Koobface botnet that has affected the social site for a few years. The identities of those responsible for the attacks are: Stanislav Avdeyko (leDed), Alexander Koltysehv (Floppy), Anton Korotchenko (KrotReal), Roman P. Koturbach (PoMuc) and Svyatoslav E. Polichuck (PsViat and PsycoMan). Unfortunately, the men live comfortable lives in St. Petersburg (Russia), and have become rich from their various online schemes. All five have yet to be charged with a crime, nor has any law enforcement agency confirmed they are under investigation.

Despite the myriad malware and spam scams preying on Facebook, curiosity still gets users into trouble. This quarter we saw a new scam involving a supposed tape of Katy Perry and Russell Brand posted to the walls of hundreds of users. The malicious post looked as follows:

FIG.09. *MESSSAGE.*

If the user clicked the link, they were taken to a fake Facebook page where they were invited to download a plug-in to watch the video:

FIG.10. *MESSAGE.*

However, all the 'Likes', comments, etc. displayed on the page were false as the 'page' itself didn't exist, it was simply an image. If you clicked on "Install Plugin" and you were using Firefox or Chrome, the worm installed a browser plug-in and used it to post the scam to the victims' friends' pages. On Internet Explorer, as there was no plug-in that could carry out this task, the worm displayed an age verification page to access an application called 'X-Ray Scanner'.

FIG.11. *MENSAJE.*

As you can see, the page looked like a Facebook page to trick users into believing they were still on the social networking site. If the victim clicked any of the links they were taken to a page where they were asked to enter their cell phone number. However, after doing so, they started receiving unwanted premium rate text messages.

Cyber-crime

In a typical phishing attack, offenders usually steal consumers' identities to impersonate them and empty their bank accounts. However, the year started off with quite an unusual case. The first mayor cyber-crime of 2012 took place in South Africa, as hackers got away with about $6.7 million from South African Postbank. The robbery took place over three days, from Jan 1 to Jan 3. The hackers, who had planned the attack for months, used stolen login details from a Postbank teller to transfer the stolen money into multiple bank accounts that were opened across the country.

MEGAUPLOAD CASE

In January, the FBI shut down the popular Megaupload file-sharing website, charging the founders for "copyright infringement" (you can read the FBI press release here, with more information about the case). If convicted, those involved face up to 50 years in prison on all charges.

Hacker group Anonymous reacted swiftly to the news, launching DDoS attacks on several Web pages, including the sites of the U.S. Department of Justice, RIAA (Recording Industry Association of America) and Universal Music Group.

Going back to the press release, the FBI stated that:

This case is part of efforts being undertaken by the Department of Justice Task Force on Intellectual Property (IP Task Force) to stop the theft of intellectual property.

Well, as we all know, in the 'real world' cyber-criminals are siphoning millions of dollars into their pockets every year by attacking hundreds of thousands of computers. However, it seems that authorities consider copyright infringement to be far more serious. As always, this is a question of priorities, and it seems that in this case the highest priority of law enforcement agencies is not exactly to protect the individual.

FIG.12. *IMAGE DISPLAYED ON ACCESSING MEGAUPLOAD'S SITE AFTER THE FBI'S INTERVENTION .*

Going back to real cyber-crime, we have some good news to share with you. Interpol has announced they are planning to open a "Global Cybercrime Center" in Singapore in 2014 to improve global cooperation among law enforcement.

In February, the online Microsoft Store in India was compromised by a group of Chinese hackers. The team of hackers defaced the site and stole data from thousands of Microsoft customers.

FIG.13. *MICROSOFT INDIA WEB STORE HACKED.*

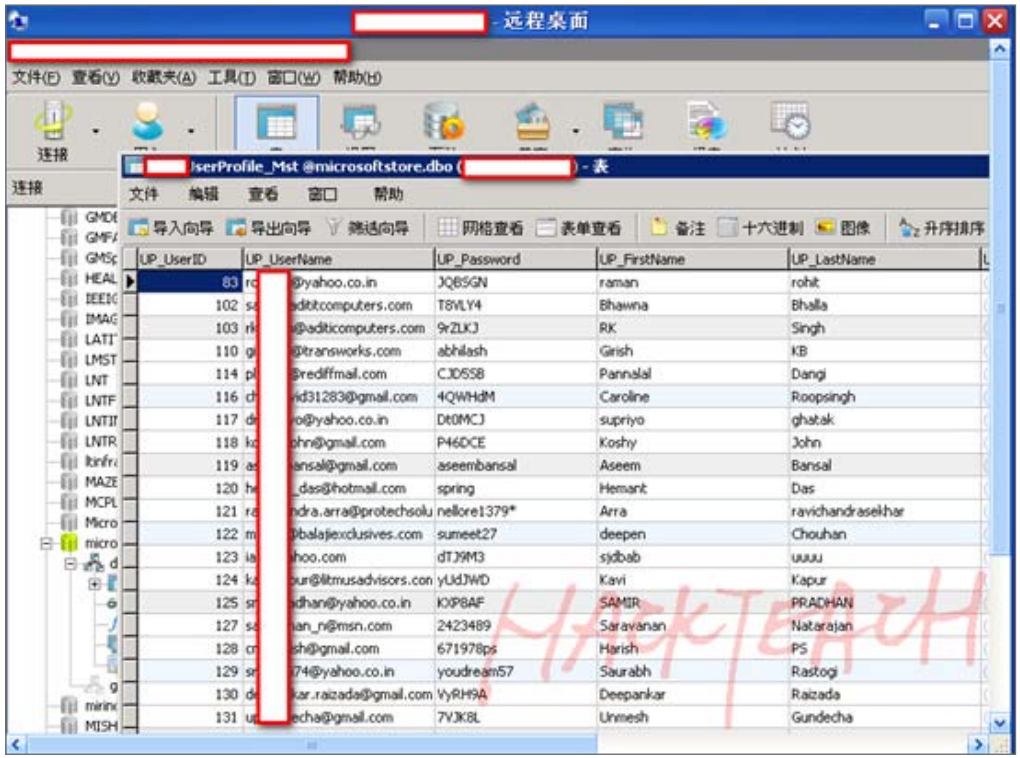
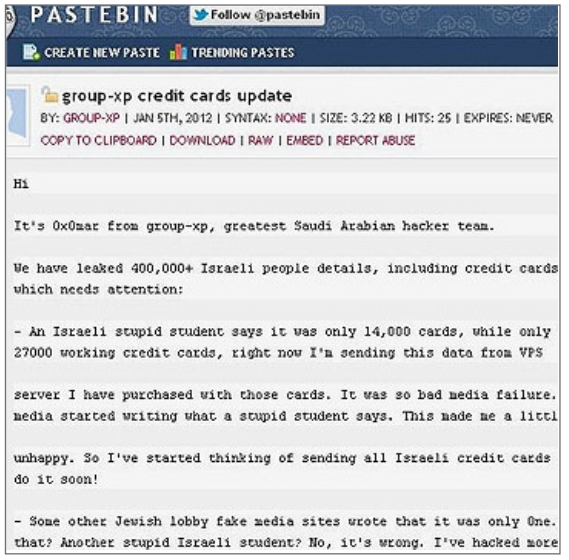


FIG.14. *SCREENSHOT SHOWN BY CYBER-CRIMINALS TO PROVE THEY HAD STOLEN DATA FROM MICROSOFT'S CUSTOMERS.*

Also in February, it was reported that attackers stole information from millions of users of YouPorn, one of the world's most popular porn video websites. This data was posted on Pastebin, a popular dumping ground for cyber-attackers, potentially compromising the security of thousands of users who reuse passwords on multiple sites.

In March, it was revealed that Michael Jackson's entire back catalogue had been stolen from Sony Music, including some previously unreleased material. This follows last year's attacks on Sony that exposed personal data from more than 100 million accounts at Sony Online Entertainment and the PlayStation Network (PSN).

FIG.15. *MICHAEL JACKSON'S ENTIRE MUSIC CATALOGUE STOLEN IN SONY MUSIC HACK.*



16. *SCREENSHOT FROM 0X0MAR'S ONLINE CLAIM OF AN ISRAELI HACK ATTACK.*

It seems that the cyber-criminals who hacked into Sony Music's systems thought it would be easy to access the company's information. Unfortunately, they were right, although in this case they were arrested and are due to stand trial in January 2013.

Cyber-war

This first quarter of 2012 has seen some remarkable events in the cyber-war arena. On January 2, thousands of credit card numbers belonging to Israeli citizens were stolen. A Saudi hacker, calling himself 0x0mar, took credit for the hack attack, although further investigation revealed the hacker's real identity: 19-year-old computer science student Omar Habib, born in the United Arab Emirates, but currently living in Mexico. Later on, 0x0mar denied the allegations.

Soon after, a war began to brew between the hackers of Israel and Saudi Arabia: Arab hackers paralyzed the websites of the Tel Aviv Stock Exchange, El Al Airlines and several Israeli banks, whereas Israeli hackers brought down the websites of both the Saudi Stock Exchange (Tadawul) and the Abu Dhabi Securities Exchange (ADX) in retaliation, claiming to act on behalf of the Israeli Defense Forces and vowing to strike Arab countries' websites related to their economies unless attacks on Israeli sites were halted.

To make matters worse, Tariq al-Suwaidan, one of Kuwait's most famous TV preachers, called for a cyber-war against Israel. He used his Twitter account to call on all Muslim hackers to unite against Israel in a "cyber-jihad against Zionist enemy, which will be rewarded by God".

Also in the Middle East, thousands of emails received and sent by Syrian president Bashar al-Assad were stolen by Saudi hackers.

In the Far East, it was reported that Japan's Defense Ministry had commissioned Fujitsu to develop a cyber-weapon virus capable of tracing and disabling computers being used in cyber-attacks against the country. The information is a bit confusing, and it looks like a bad idea anyway as, even if created with the best of intentions, there may be adverse effects that turn the weapon against its creators or the entire world. In any event, users of Panda Security's solutions can set their mind at ease, as we will detect every virus created, either by public or private writers.

Let's look now at two of the countries that usually take the spotlight in this section: China and the United States. In January, it was revealed that Chinese hackers had deployed a Trojan targeting smart card readers used by the U.S. Department of Homeland Security. These cards are a standard means of granting users access to intranets, networks and physical locations. Had the hackers actually managed to crack the smart cards, they could easily access lots of confidential information.

Also in China, we learned that a group of hackers managed to penetrate the corporate network of Nortel, using passwords stolen from seven top Nortel executives, including the CEO. Apparently, they had been spying on the company from as far back as 2000.

Anonymous

Both Anonymous and LulzSec have been very busy over the last few months.

In January, in the wake of controversial legislation such as SOPA and ACTA, the hacking group posted the following Twitter message: "If you hated #SOPA, you'll burst into flames about #ACTA http://is.gd/Bo68r4 Negotiated in secret. iPod searches at border crossings.". Soon after, they launched an unprecedented string of attacks on government and business sites around the world.

In February, they recorded and released a sensitive conference call between the FBI and Scotland Yard. Amid growing speculation about how the hackers had been able to obtain the recording, Anonymous published an email purportedly sent by an FBI agent to international law enforcement agencies, with a phone number and password for accessing the call.

All,

A conference call is planned for next Tuesday (January 17, 2012) to discuss the on-going investigations related to Anonymous, Lulzsec, Antisec, and other associated splinter groups. The conference call was moved to Tuesday due to a US holiday on Monday.

Date: Tuesday, January 17, 2012
Time: 4:00 PM GMT=20
BridgeTN: 202-393-2430
Access Code: 6513211#

Please contact me if you have any questions.

Regards,

Tim
Federal Bureau of Investigation

FIG.17. *FBI MESSAGE INTERCEPTED BY ANONYMOUS.*

In February, Anonymous published the source code of PCAnywhere and Norton, stolen in 2006. The theft was committed by a group of cyber-criminals who aimed to blackmail Symantec. However, once it became clear the American security firm was not going to give in to the blackmail, they decided to pass the data to Anonymous to make it public.

In March, several alleged members of LulzSec were arrested in the course of a police operation launched in 2011. It was immediately discovered that Sabu, the alleged leader of LulzSec, had been secretly arrested by the FBI and had been working for the government to arrest other members of the hacker collective.

Luis Corrons, technical director of PandaLabs, lauded the arrests on the laboratory's blog and Anonymous reacted swiftly by breaking into the external server that hosted the blog and defacing it. Anonymous make a big deal about freedom of speech, calling themselves 'the Voice of Free Speech' and 'aggressive proponents for the Freedom of Speech'. However, in reality, the self-appointed defenders of free speech shut down people's websites when they don't like what they read. Uhmm… It is ironic, isn't it? It seems that Anonymous are only interested in defending freedom of speech when it serves their own interests. Actually, a British journalist asked them about this apparent contradiction on Tweeter but his question, unsurprisingly, went unanswered.

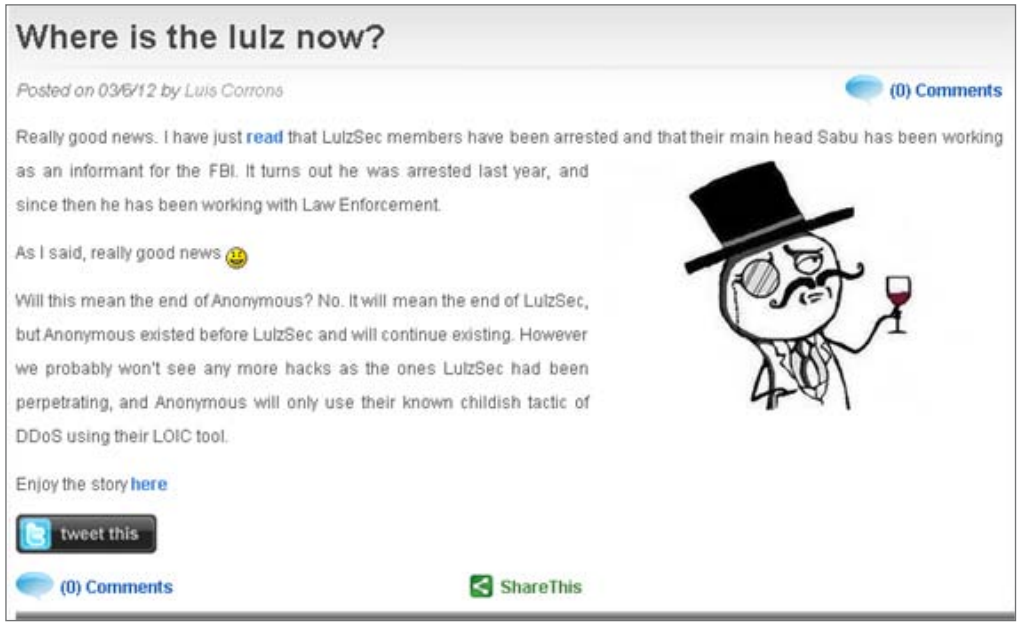


FIG.18. *PANDALABS BLOG POST PRAISING THE LATEST LULZSEC ARRESTS.*

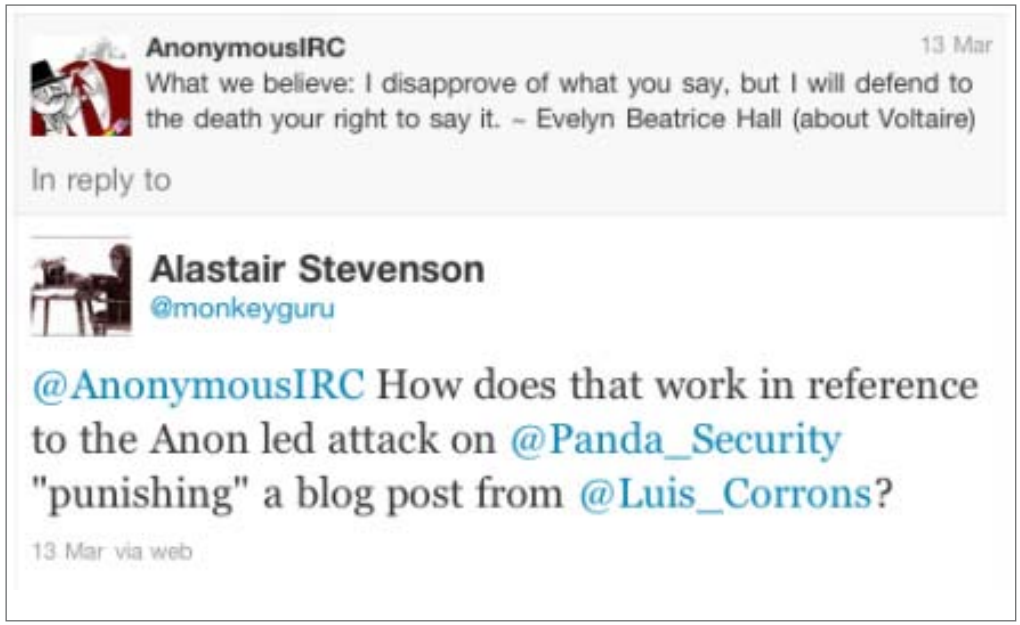


FIG.19. *UNANSWERED QUESTION TO ANONYMOUS FROM A BRITISH JOURNALIST.*

One day later, they launched an attack on the main website of the Vatican, rendering it inaccessible. And five days later they attacked the Vatican again, this time breaking into the Vatican Radio database and posting user names and passwords.

03| Quarterly figures

In the first three months of 2012 our laboratory identified over six million unique malware samples, which is in line with the overwhelming number of malware strains detected over the last few years. Most of the infections were caused by Trojans (80 percent of all new malware samples), setting a new record high. This is a continuation of the trend established over the last few months.

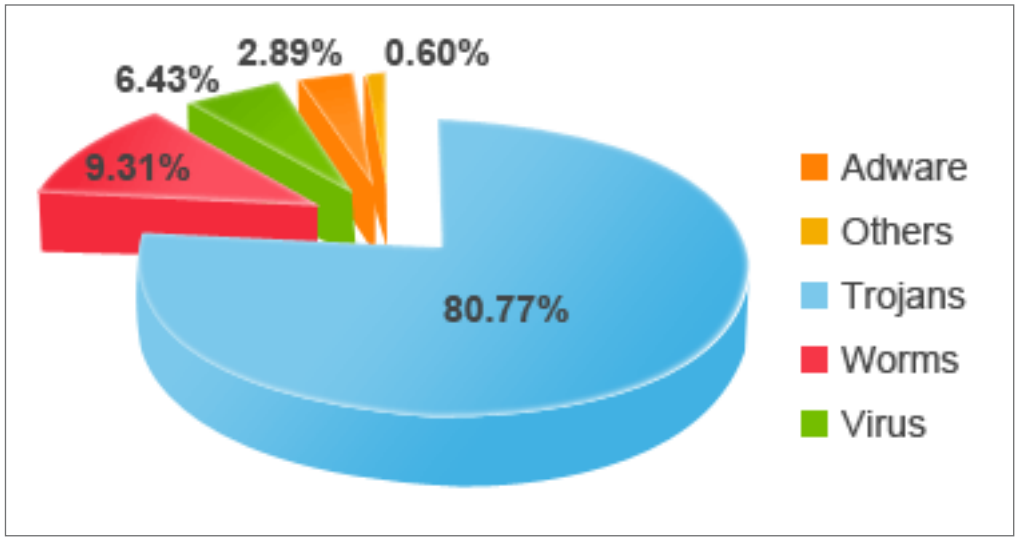


FIG.20. *NEW MALWARE STRAINS IN Q1 2012, BY TYPE.*

One of the culprits of this surge in the number of Trojans in circulation is the so-called "Police Virus", covered extensively in the "Q1 at a Glance" section.

Let's take a look at the number of infections caused by each malware category all over the world. One of the characteristics of Trojans is that they cannot replicate automatically, so they are less capable of triggering massive infections than viruses or worms, which can infect a large number of PCs by themselves. The graph below shows the distribution of malware infections for this quarter:

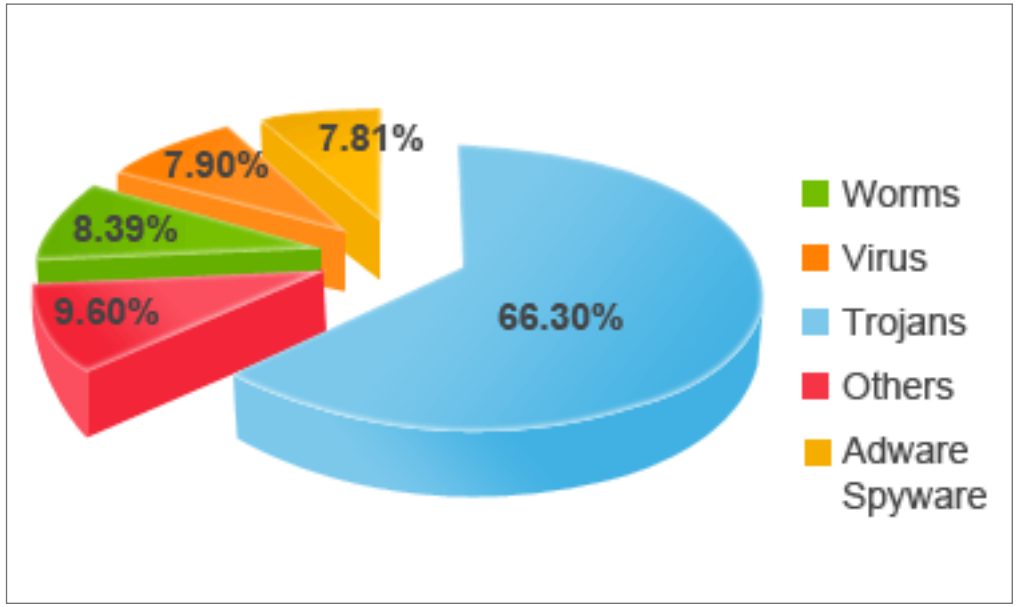


FIG.21. *MALWARE INFECTIONS BY TYPE IN Q1 2012.*

While, as expected, Trojans account for most infections, it is worth noting the relatively small number of PCs infected by worms, which is lower than the number of new worms created over these three months. This demonstrates that massive worm epidemics have become a thing of the past, and have been replaced by a silent Trojan invasion.

Let's now look at the geographic distribution of infections. Which countries are most infected? Which countries are best protected? The average number of infected PCs across the globe stands at 35.51 percent, which is over three points lower than in 2011. China continues to be the most affected country (54.10 percent of infected PCs), and remains the only country with an infection ratio over 50 percent. China is followed by Thailand (47.15 percent) and Turkey (42.75 percent). The graph below shows the ten countries with the most infections in Q1 2012:

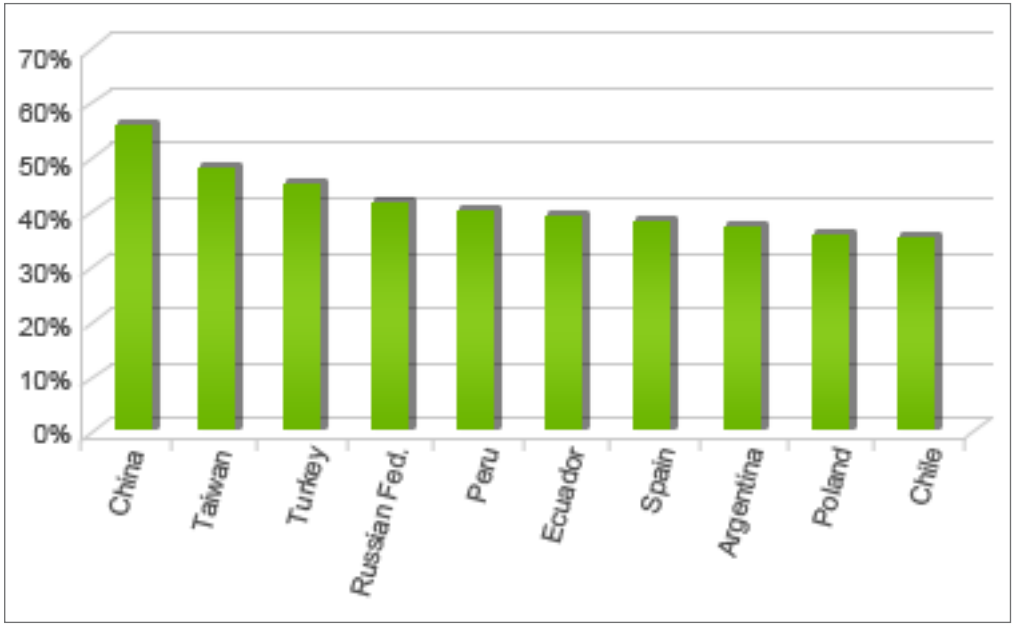


FIG.22. *MOST MALWARE INFECTED COUNTRIES.*

As the table shows, there are high-infection countries in almost every continent. The list of the least malware infected nations is topped by European countries, with the exception of Japan. Sweden came in lowest with less than 20 percent of infected computers (setting a new record).

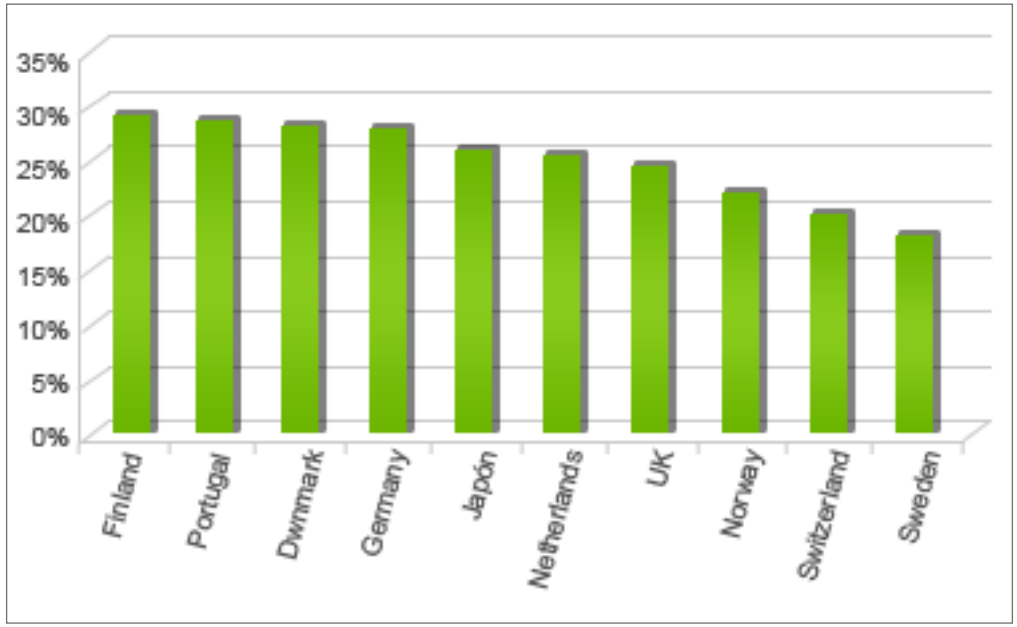


FIG.23.*LEAST MALWARE INFECTED COUNTRIES.*

04| Conclusion

We are just at the beginning of 2012, and it promises to be a very exciting year in the fight against cyber-criminals trying to steal user information and make money.

Anonymous will continue to hit the headlines with their hacking stunts and the arrests of alleged members of the organization, and we'll follow the group's activities very closely after the arrest of several key members of its splinter group LulzSec.

As for cyber-war, reality never ceases to amaze us, so who knows what we'll see. One thing is certain: We'll be back in three months' time with more IT security news.

05| About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

- **PandaLabs** creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.

- **PandaLabs** is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.

Likewise, PandaLabs maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security. Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.

- For further information about the last threats discovered, consult the PandaLabs blog at: **http://pandalabs.pandasecurity.com/**

Follow us on the Web

facebook
https://www.facebook.com/PandaUSA

twitter
https://twitter.com/#!/Panda_Security

google+
http://www.gplus.to/pandasecurity

youtube
http://www.youtube.com/pandasecurity1

PANDA SECURITY