PandaLabs Quarterly Report

January - March 2013

01 | Introduction

We have seen a thrilling start to 2013, a year in which it would seem that stories from the world of security will keep us glued to our seats. In this report we will first look at the figures returned by our cloud-based malware scanning systems, and see how cyber-crooks have created more than 6.5 million new strains of malware.

We will analyze some of the attacks witnessed in the first quarter of 2013, including the hacking of Twitter accounts of major organizations such as the BBC or Burger King. We will describe how one of the biggest attacks to date was perpetrated, targeting some of the world's leading technology companies: Twitter, Facebook, Apple and Microsoft.

We will also mention some of the victories of the security forces, including the arrest of a group of hackers accused of extortion using the infamous 'Police Virus'.

In the world of cyber-war and espionage, we will discuss the global situation, and the role of the Chinese government in some of the major events of the last three months, including attacks on media firms (The New York Times, The Washington Post or The Wall Street Journal), and companies like EADS (European Aeronautic Defense and Space Company) or ThyssenKrupp.

02| The Quarter at a Glance

On January 11, the European Commission inaugurated the European Cybercrime Center (EC3) in order to support member states in the fight against cyber-attacks. The truth is that cyber-criminals have often benefited from the difficulty in coordinating the police effort across different countries, and therefore such initiatives are always welcome.

Cyber-crime

In January, the FBI published details of an investigation that began in 2010 and thwarted a gang of cyber-criminals who had infected more than a million computers since 2005. This operation stands out not least because of the coordination between security forces in different countries. The FBI had the support of police in Moldavia, Romania, Holland, Germany, Finland, Switzerland and the UK.

There are also many different aspects to the fight against cyber-crime. And one which is often ignored is the need to alert companies to the importance of dedicating resources to protecting customer data. As a timely reminder of this, the UK division of Sony Computer Entertainment has been ordered to pay 250,000 pounds as a result of the theft of customer data in 2011. The sentence is the consequence of the lack of measures that the company had implemented to protect customer information.

POLICE VIRUS SCAM

One of the most infamous cases of the last year or so has been the ‘Police Virus’. In February this virus once again hit the headlines, but this time for a very different reason. Our friends in the Technological Investigation Division of the Spanish National Police, in collaboration with Europol and Interpol, dismantled the gang of cyber-criminals responsible for the virus. According to a statement from the Spanish Interior Ministry, ten individuals were arrested from the group’s financial cell, which generated a million euros a year from victims of malware. Six of those arrested were Russian citizens, two were Georgian and two Ukrainian. The head of the whole operation –a Russian resident- was also detained while on holiday in Dubai.

We noticed that the news mentioned the arrest of a ‘gang’ of cyber-criminals, yet the information we have at PandaLabs points to the existence of several gangs responsible for these attacks. We reached this conclusion after analyzing numerous variants of the malware over time, and observing significant differences between them.

On several occasions we have discussed the Police Virus on the PandaLabs blog, describing how it has evolved and how the techniques used have changed. Such changes are normal and do not necessarily imply that there are different groups behind the attacks, as cyber-criminals will often try new techniques to get as many victims as possible to pay up.

However, there are other factors that we have not previously mentioned. For example, certain techniques which had supposedly been improved have reemerged (including encryption of files on compromised computers), or how different variants show the screen with the fake police warning using completely different functions, clearly illustrating that they are different projects.

In any event, this is a relatively normal occurrence that can be seen in other contexts. Analyzing the situation from a purely commercial point of view, it is often the case that when someone has an idea that attracts a lot of attention -and makes a lot of money-, others are quick to jump on the bandwagon. In this case, it would seem that several different gangs are using the same techniques.

At PandaLabs we decided to investigate a little more and throw up some numbers to see if they are consistent with the evidence described above. As we have mentioned in the past, most infections are carried out using ‘exploit kits’, tools used by cyber-criminals to infect users’ computers simply when they visit a compromised website. Security holes are exploited, most of them in Java or Adobe (Flash, Reader), as these are applications with numerous flaws, and also many users have not installed updates, so infecting users is child’s play.

That’s why in 2012 we deployed an antivirus technology that blocks infections when a vulnerability of this type is detected (even if it’s unknown), and also sends data to the cloud about the file that attempted to infect the system.

From this data we have selected a couple of different families of Police Virus and counted the infections blocked from December 2012 through to mid-February 2013. We’re talking about Panda Cloud Antivirus users who, when using the Internet, were attacked through an exploit for which they were not updated (as mentioned above, most of these were Java or Adobe). The aim of the attack was to infect them with a virus from one of these two Police Virus families.

The alleged head of the gang was arrested in Dubai in December. If this really was the only person behind the Police Virus, as reported by some sources, infections should have ceased, or at least decreased significantly. Yet the reality is different:

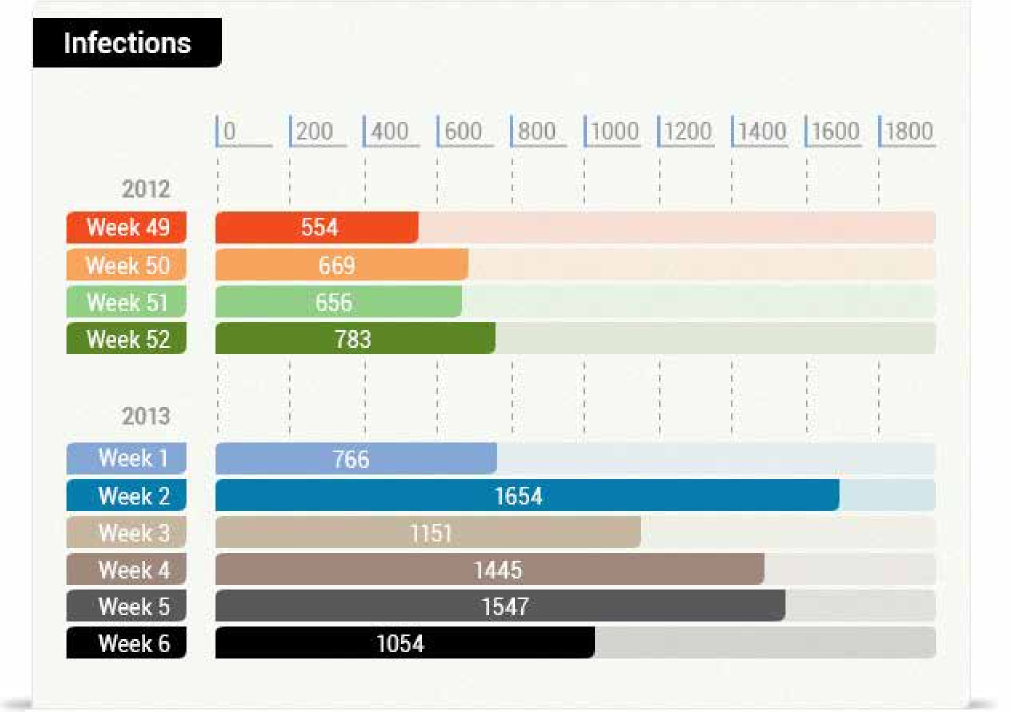


FIG.01. *INFECTIONS OF TWO VARIANTS OF THE POLICE VIRUS SINCE THE ARREST OF THE HEAD OF THE GANG.*

As you can see, the number of infection attempts has not decreased, it has doubled. This is clear empirical proof that the Police Virus is still going to be with us for a while, and we have to keep our guard up.

Twitter, Facebook, Apple and Microsoft victims of the same attack

On February 1, Twitter published an article on its blog ("Keeping our users secure") detailing how the social network had fallen victim to an attack resulting in unauthorized access to the details of some 250,000 Twitter users.

A couple of weeks later, Facebook also released an article on its blog, entitled "Protecting People On Facebook". According to sources from the social network, user data was not compromised in this attack.

The next victim was Apple. Just a few days after the Facebook announcement, spokesmen from Apple told Reuters that the company had also been targeted by the same attack.

And finally, of no less importance, Microsoft admitted that it too had been targeted.

An impressive list, isn't it? As far as we know, no other major company has claimed to have suffered the same attack. In any event, there are some positives we can take from the situation:

- Companies are not shy to admit they have been targeted.
- Many companies have good security teams that have been able to identify the attacks as they happened.

Of course, all these attacks exploited a previously unknown security hole in Java for which no patch was available. This is known as a zero-day vulnerability

Of course, all these attacks exploited a previously unknown security hole in Java for which no patch was available. This is known as a zero-day vulnerability.

Anyone who works in security knows that nothing is 100 percent secure. A number of preventative measures may work well most of the time. Yet there will always be weak points, a new vulnerability, human errors, etc. which may finally facilitate one of the thousands of attacks to which these companies are constantly subjected.

Here it is critical to be able to identify an attack when it is occurring. Twitter, Facebook, Apple and Microsoft were able to do this. All of them are gathering data about the attack. All are working with the police to find out who is behind this.

Perhaps those running a small or medium-sized business feel they don't have to worry as much about security as these giants, given that they don't make such a 'sexy' target. And that's true to an extent. They probably receive a very small number of targeted attacks (if any), they will however be bombarded with the type of attacks from cyber-criminals that infect millions of computers. And these criminals like nothing more than an easy target. In short, all those with unprotected computers, with out-of-date software and without a serious security policy are surefire targets.

JAVA

Most infections today occur through 'exploit kits', infecting users' computers through a vulnerability without their knowledge. More than 90 percent of these are through Java vulnerabilities in browsers. The recent attacks on Microsoft, Apple, Facebook and Twitter used Java. Most 'Police Virus' infections managed to reach victims' computers thanks to outdated versions of Java.

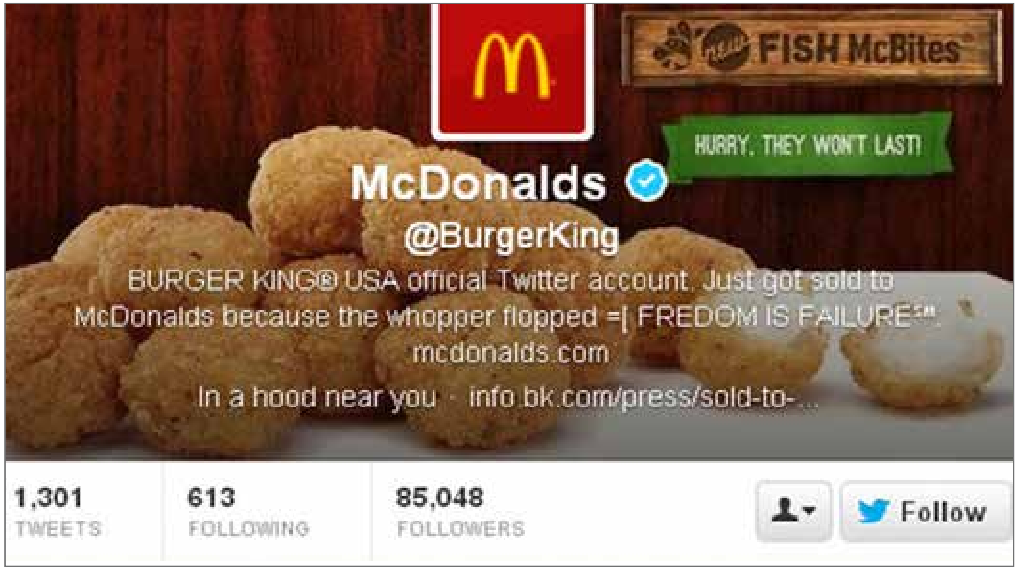
What is the best way of preventing these infections? Simple: Just remove Java from the browser. If for any reason you need Java on your browser to use an application, use it on another browser set up specifically for this task

CYBER-ATTACKS

The number and variety of attacks in this quarter have been significant to say the least. In addition to those described in the report, many organizations and business have been considerably affected. **Evernote** was the victim of an intrusion that prompted the firm to release a statement calling on more than 50 million users to change their passwords. According to a statement from the **U.S. Federal Reserve** its website was also attacked, although it did not say whether any data was stolen. The incident coincided however with the publication, by Anonymous, of the personal information of 4,000 U.S. bank executives, suggesting that the attack on the Fed may have been carried out by this group. The NASA was also the victim of an intrusion. Internal information including email addresses, real names and passwords was published on the popular website Pastebin.

Social Networks

During this quarter various Twitter accounts have been hacked, including those of celebrities and also those of companies. One of the most notable cases was that of Burger King, with attackers seemingly managing to work out the account password and take control of the account. They changed the background image to that of McDonalds and claimed that the company had been taken over by its main rival.



McDonalds

@BurgerKing

BURGER KING® USA official Twitter account. Just got sold to McDonalds because the whopper flopped =[FREDOM IS FAILURE℠.

mcdonalds.com

In a hood near you · info.bk.com/press/sold-to-...

1,301	613	85,048
TWEETS	FOLLOWING	FOLLOWERS

FIG.02. *IMAGE OF BURGER KING'S TWITTER ACCOUNT AFTER BEING HACKED.*

The Twitter account of Jeep was also the victim of a similar attack, in this case stating that the company had been bought out by Cadillac. Other attacks on Twitter accounts have had a more political slant. A group of cyber-crooks calling themselves the "Syrian Electronic Army" managed to hack accounts belonging o several organizations. From what we can determine, phishing attacks were launched to get the passwords and then the accounts were hijacked. Their victims included Human Rights Watch, the French news channel France 24 and the BBC weather service..

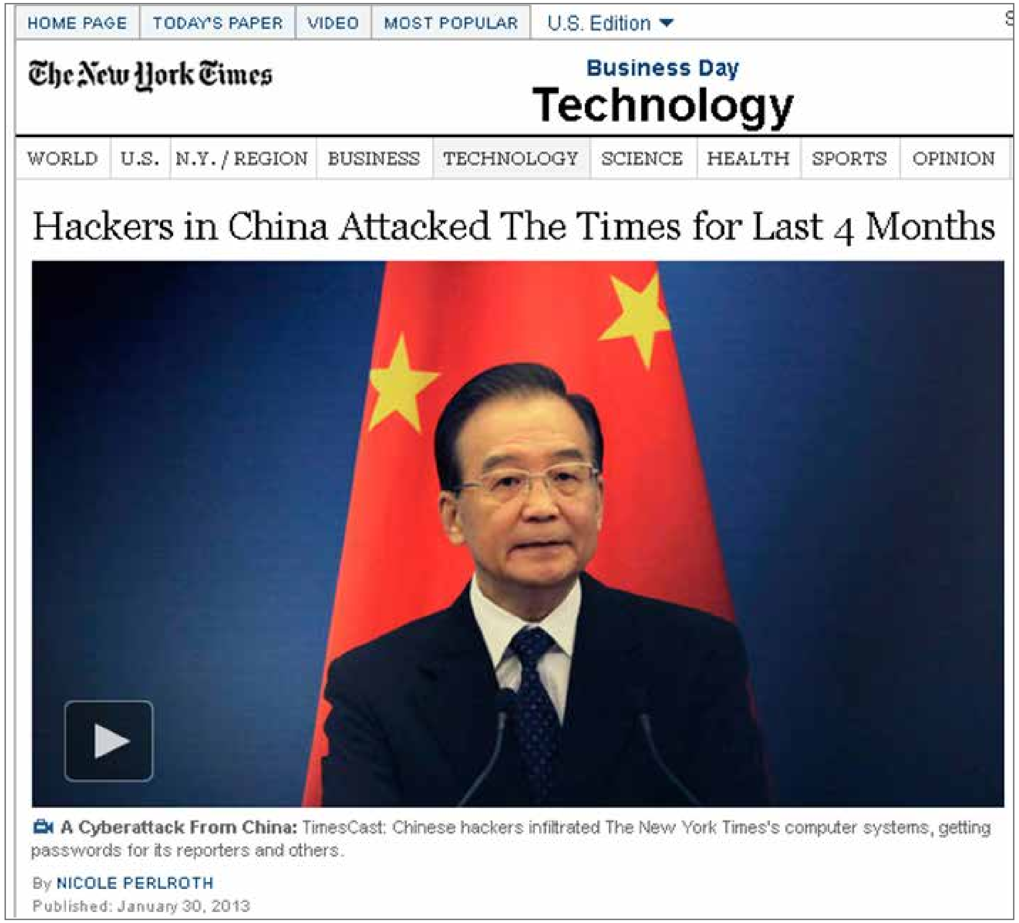
Mobile Phone Malware

Practically all news regarding malware attacks on mobile platforms involves the Android operating system, which has the largest share of this market. In addition to the usual attacks, this quarter we have seen new techniques that deserve mention. A strain of Android malware -hidden inside Google Play- not only infected cell phones but could also infect computers via smartphones or tablets.

The technique is very simple: Once it runs on the phone, it connects to the Internet to download files which it stores in the root directory of the device storage card, so then when it connects to a computer via USB, it automatically runs one of the files, a Windows Trojan.

Cyber-war

China often gets a mention in this section, but in Q1, the Asian giant has earned all the headlines. On January 30, the **New York Times** ran a front-page article explaining how they had been victims of an attack that had allowed their computers to be accessed and spied on for months. Coincidentally, the attack came just after the paper released an article describing how Chinese PM, Wen Jiabao, and his family had amassed a billion-dollar fortune.



Hackers in China Attacked The Times for Last 4 Months

A Cyberattack From China: TimesCast: Chinese hackers infiltrated The New York Times's computer systems, getting passwords for its reporters and others.

By NICOLE PERLROTH

Published: January 30, 2013

FIG.03. *NEW YORK TIMES STORY ON THE ATTACK FROM CHINA.*

A day later, The **Wall Street Journal** declared that it had also been the victim of a similar attack by Chinese hackers. The Chinese government protested against these ‘unjustified attacks’ and Hong Lei –Chinese Foreign Minister– claimed it was “… unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence”.

Interestingly, in both incidents the attackers were able to access all types of data (customer details, etc.), yet only focused on information about journalists and employees, trying to find any reference to investigative journalism regarding China, and in particular, looking for the papers’ sources.

The day after the Wall Street Journal’s revelations, another US media giant, The Washington Post, announced they had suffered a similar attack in 2011, also originating in China.

Some weeks later, Mandiant published a damning 76-page report (APT1: Exposing One of China’s Cyber Espionage Units, http://intelreport.mandiant.com/) explaining how Unit 61398 of the Chinese army has specialized in cyber-espionage. The report reveals more than 3,000 pieces of evidence showing how this unit has been running since at least 2006, stealing information from no less than 141 organizations worldwide.

We may not truly appreciate the importance of the Mandiant report and the impact it may have in the mid to long term. Proving who is behind any attack is highly complex, even in normal cyber-crime cases. When it comes to cyber-espionage things are further complicated by the simple fact that whoever is behind the operation is highly qualified and adept at covering their tracks. For some years now, people have turned their gaze to China whenever this type of incident occurs, yet without any real evidence that the Chinese government is behind such attacks. Now, for the first time, it has been proven that the Chinese army is actively involved in espionage on a global scale, infiltrating companies across many sectors and stealing information.

A week after the Mandiant report was published, several other stories of cyber-espionage emerged that also pointed towards China: EADS (European Aeronautic, Defence and Space Company), manufacturer of the Eurofighter and owner of Airbus, was attacked by hackers according to Der Spiegel (http://www.spiegel.de/international/world/digital-spying-burdens-german-relations-with-beijing-a-885444.html). The article also mentions another similar attack on the German company ThyssenKrupp.

03| Malware Figures in Q1 2013

During the first three months of 2013 our laboratory collected over six and a half million malware samples. Trojans are still the most common culprit, accounting for some three out of four cases. The figures in general are similar to those we saw during 2012:

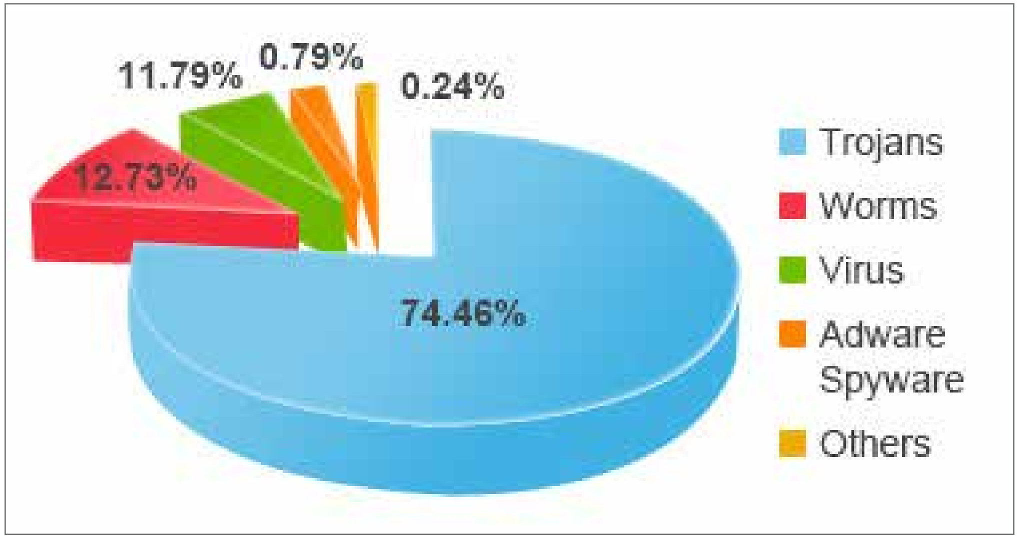


FIG.4. *NEW MALWARE STRAINS IN Q1 2013, BY TYPE.*

Let's take a look at the number of infections caused by each malware category around the world. As mentioned in earlier reports, one of the features 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:

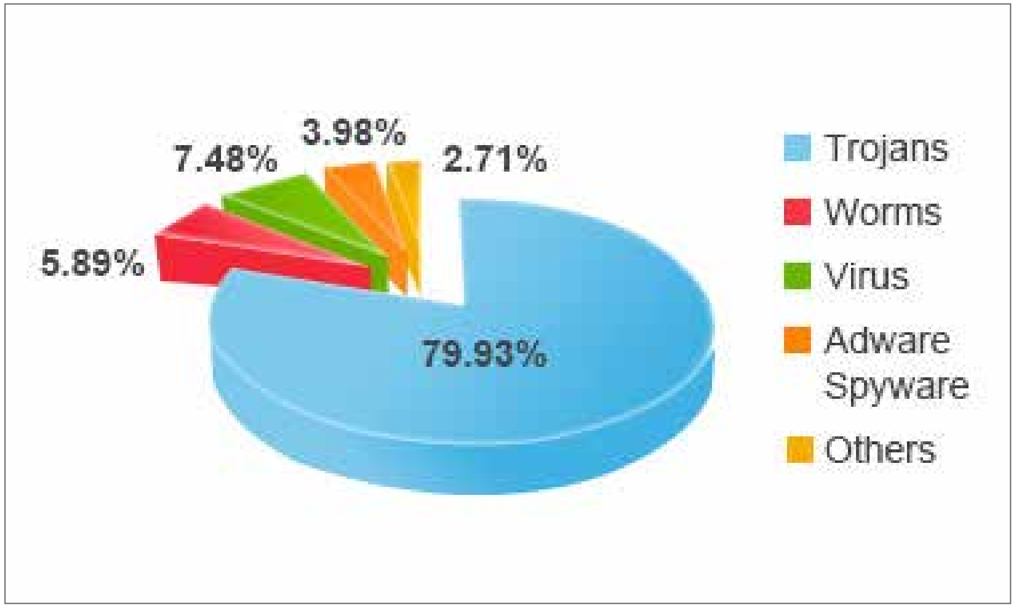


FIG.5. *MALWARE INFECTIONS BY TYPE IN Q1 2013.*

Trojan infections have reached record levels, accounting for almost 80 percent of all infections. How could this be possible if they cannot self-replicate? The answer is in the last part of the question: "**self-replicate**". Today most Trojan infections are through compromised websites, often exploiting some kind of vulnerability in Java or Adobe. This means that in just a few minutes (in the case of a popular Web page) there may be thousands of infections with the same Trojan. Similarly, they could be different Trojans, as attackers can change the Trojan in accordance with numerous parameters, such as the victim's location, the operating system, etc.

Analyzing infections by region, in Q1 2013 the average infection ratio was 31.13 percent (percentage of infected computers worldwide). As is often the case, China tops the global infection ranking, being the only country with an infection ratio of over 50 percent. China is followed by Ecuador (41.01 percent) and Turkey (40.38 percent).

The graph below shows the ten countries with the most malware infections in the first quarter:

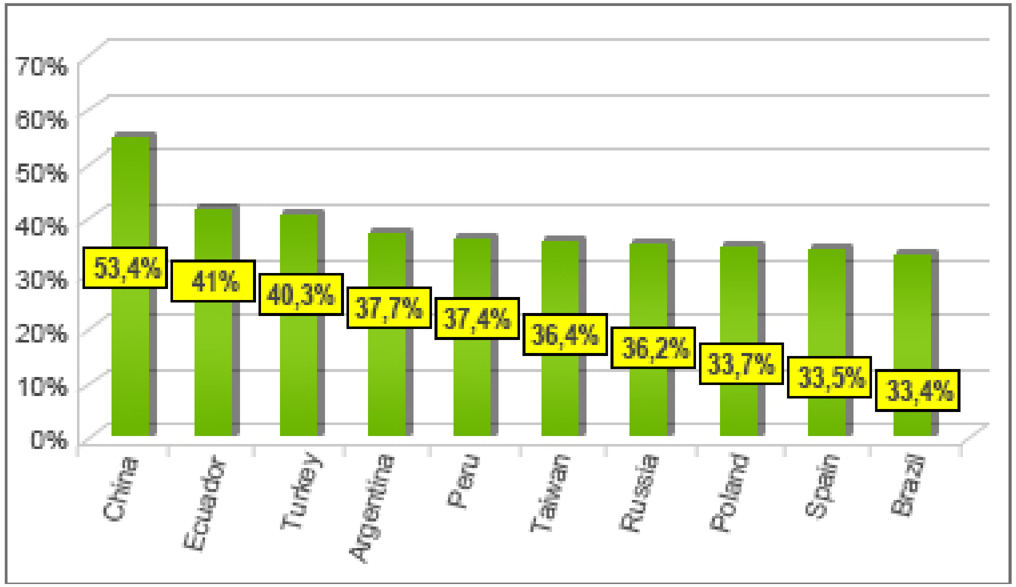


FIG.6. *MOST MALWARE INFECTED COUNTRIES.*

All these countries obviously have an infection rate over the global average. There are four other countries that also exceed this figure: Chile (33.37 percent), Colombia (32.01 percent), Italy (31.97 percent) and Venezuela (31.45 percent).

Below you can see the countries with the least infections:

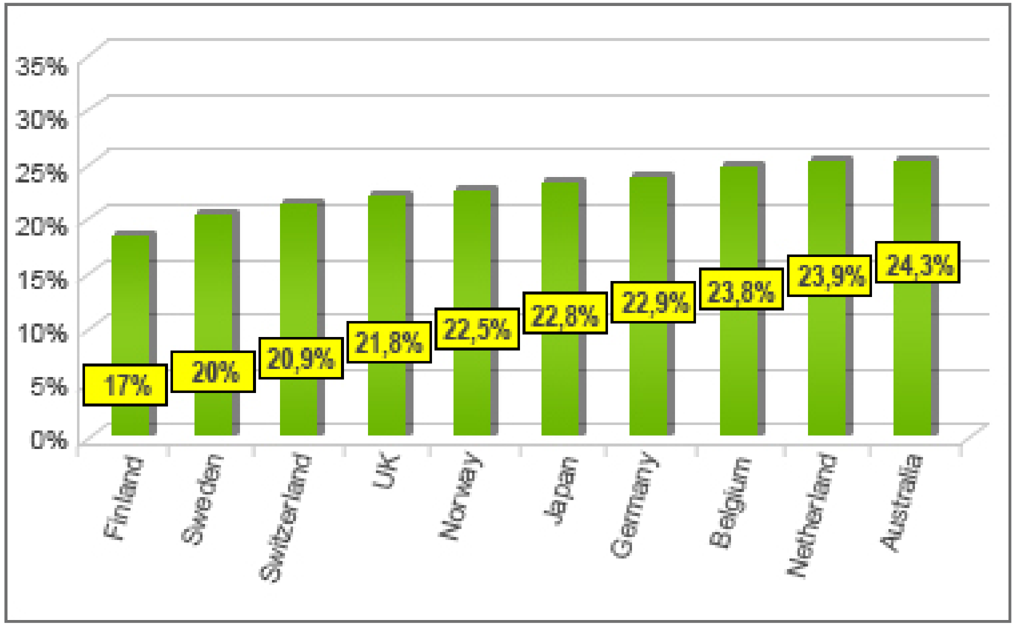


FIG.7. *PAÍSES CON MENOR ÍNDICE DE INFECCIÓN.*

Europe continues to have the lowest infection rates. In Finland, which tops this ranking, just 17 percent of computers were infected followed by Sweden (20.01 percent) and Switzerland (20.99 percent). Other countries outside this Top 10 but with infection rates below the average are: Canada (24.89 percent), Denmark (25.72 percent), Portugal (26.91 percent), Costa Rica (27.22 percent), France (27.43 percent), USA (27.79 percent), Mexico (29.91 percent) and Hungary (30.69 percent).

04| Conclusion

As we've seen, throughout these three months there have been numerous incidents whose repercussions will be discussed for some time, and 2013 has only just begun. The fight against cyber-crime is on the right tracks, and though there is still a long way to go, we can see how international co-operation among security agencies is beginning to pay off and how criminals around the world are being brought to justice.

The area of cyber-war and espionage is becoming more and more interesting. Many countries are looking suspiciously at China regarding its suspected involvement in attacks on large organizations and public institutions around the world, and this could lead to real world consequences. There are those who argue for international agreements, a type of Geneva Convention, to attempt to establish limits to these activities. We will be tracking events over the coming months, as the Internet as we know it could start to change considerably.

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