PandaLabs Quarterly Report

April - June 2012

01 **Introduction**

02 **The Quarter at a glance**

- The Rise of Ransomware – Police Virus ‘Reloaded’
- Cyber-crime
- Mobile Phone Malware
- Mac
- Social Networks
- Cyber-war
- Flame

03 **Quarterly figures**

04 **Conclusion**

05 **About PandaLabs**

06 **Follow us on the web**

01| Introduction

Today, nobody doubts that we live in a society absolutely dependent on technology. Most of the information we have is in digital format. Long gone are the days when we kept photo albums to preserve our family's most precious memories. Now we store thousands of photographs, music, movies, work documents, bank statements, etc. in digital format. Our whole lives are intrinsically linked to digital resources and the Web.

But it doesn't stop here: computers figure everywhere in our lives, from TV sets to kitchen appliances. They are used to control traffic lights, public lighting systems, water and electricity supply systems… in power plants of all types, weapon control systems, etc.

This explains the revolution we are witnessing from the vantage point of our laboratory: thousands of new malware specimens are created every day. While the Internet has undoubtedly improved our lives, it has also provided cyber-criminals with new opportunities to steal and sell user data, profiting from it. And as their greed grows, their attacks have become increasingly virulent.

This report provides an insight into the new techniques and strategies used by cyber-criminals to maximize their profits. We provide information on the most recent cases of cyber-war, no longer a possibility but reality, with countries like the United States openly admitting to website hacking. Finally, we analyze the **Flame** malware, a cyber-espionage attack that has revived the fears sparked by the now-infamous Stuxnet virus.

02| The Quarter at a Glance

In our latest report, we described one of the most prevalent malware threats over the last few months, the so called 'Police Virus'. Over this quarter, the Police Virus has continued to evolve, from scareware to ransomware. As if pretending to come from the local police was not enough, the malware went on to use ransomware techniques, 'taking over' infected computers by encrypting some of their content and forcing users to pay a fine or lose access. Basically, attackers took this functionality from the PGPCoder Trojan, a malicious code designed to encrypt files and keep them locked unless the victim agreed to pay a ransom.

The Rise of Ransomware – Police Virus 'Reloaded'

The first versions of the new Police Virus only encrypted .doc files, and the encryption wasn't too hard to crack, so it was possible to decrypt the files without the key. Now, however, a more sophisticated encryption is being used, and the decryption key is required to unlock the files. And not only that, the files are encrypted with a different key for each infected computer, so, unless you are able to access the server that stores all keys, it is absolutely impossible to access the files. Additionally, the range of files being encrypted is also most sophisticated. Some variants use a blacklist of extensions to encrypt; others use a whitelist of critical system files not to encrypt.

The question is, how much further can this malware go? In the end, the purpose of scareware is simply to frighten the user into paying the money (or, as attackers call it, "the fine"). This Quarter, PandaLabs detected yet another variant of the Police Virus. This variant doesn't encrypt any files. Instead, it takes over the user's webcam. What for? Well, the malware has changed the screen it displayed so far to warn the user that 'illegal activity' had been traced to their computer…

FIG.01. *WARNING USED BY THE POLICE VIRUS UNTIL NOW.*

…And replaced it with one including images taken by their webcam:

FIG.02. *NEW WARNING USED BY THE POLICE VIRUS, SHOWING THE IMAGES CAPTURED BY THE COMPUTER'S WEBCAM.*

As you can see, the page includes a small window showing the images taken by the webcam in real time, together with the text: "Live recording". However, no images are actually being recorded or sent to law enforcement. The warning just displays the images currently captured by the webcam. Users, however, don't know this, and most of them will start to panic and be willing to pay the 'fine' to stop law enforcement from spying on them, as they are made to believe. As previously said, this new variant doesn't use encryption, probably because cyber-criminals think that the webcam trick is enough to scare potential victims.

Cyber-crime

The 'golden age' of cyber-crime continues, as organizations around the world continue to suffer data breach and identity theft attacks. Here is a summary of the most important cases occurred during the second quarter of the year, to give you an idea of the current situation:

Wikipedia suffered an attack that forced the organization to release a statement warning its users that seeing ads on its website meant their computers had been infected. The attackers used a rogue Google Chrome add-on that inserted ads into the site. The foundation behind Wikipedia took the opportunity to remind users that Wikipedia is funded by donors and they don't run advertisements on their pages.

FIG.03. *ROGUE GOOGLE CHROME EXTENSION INJECTED ADS INTO WIKIPEDIA.*

We have mentioned on many occasions how cyber-criminals are becoming more sophisticated and are constantly improving their techniques. An example of this was the appearance of a new variant of the **SpyEye** banking Trojan, which hijacked the webcam of infected computers. What for? To monitor how victims reacted when they read the socially-engineered messages displayed by the malware on spoof banking websites, and see how effective their social engineering turned out to be.

Nissan Motor Company fell victim to a breach of employee information. The attackers compromised user IDs and passwords, which seems to indicate that the malware was designed for industrial espionage.

Khosrow Zarefarid, an Iranian security expert, discovered a critical flaw in Iran's banking system, providing affected institutions with the details. When the affected banks didn't respond, he hacked 3 million accounts across at least 22 banks. He then dropped these details – including card numbers and PINs– on his blog. Google took down Zarefarid's Blogger-hosted blog, whereas affected institutions warned customers to change their debit card PINs.

Hackers, perhaps from Eastern Europe, stole the personal details of over 900,000 of Utah's Medicaid beneficiaries from a server operated by Utah's Health Department.

These are just a few examples of the cyber-crime cases we have seen over the last three months. Not everything has been bad news, however. Little by little law enforcement agencies worldwide are getting better at catching cyber-criminals. UK cyber-crook Edward Pearson was jailed for 26 months after stealing the personal information of about 8 million people. Also in the UK, Lewys Martin, a Brit who distributed a Trojan horse that posed as a patch for the popular Call of Duty game, was jailed for 18 months for stealing user data and selling it on the black market.

Ryan Cleary - a 19-year-old from Essex, United Kingdom, who was arrested last year for participating in various LulzSec attacks-, was sent back to jail for breaching his bail conditions. Cleary, who isn't allowed to access the Internet, used it last Christmas to contact Hector Xavier Monsegur (a.k.a "Sabu"), the LulzSec hacker who the FBI used as a secret informant for months last year.

Higinio O. Ochoa III, from Galveston, Texas, was arrested by the FBI for allegedly hacking into the websites of several U.S. law enforcement agencies and releasing the personal information (names, addresses and phone numbers) of dozens of police officers. In this case, Ochoa's arrest was largely due to his own mistake, as he twitted a photo of his girlfriend's breasts with a sign attached to her belly that mentioned the hacker's online name ("w0rmer"). The picture was taken with an iPhone 4, which contains a GPS device that inserts GPS co-ordinates in all pictures taken. As a result, the police only had to use the GPS co-ordinates embedded in the photo to trace the exact street and house where the picture was taken. This served to identify the woman, who happened to be Ochoa's Australian girlfriend.

FIG.04. *PICTURED POSTED BY HIGINIO O. OCHOA III THAT LED TO HIS ARREST.*

In April, the FBI announced the arrest of John Anthony Borell III, another alleged member of Anonymous, in Ohio. On this occasion, the FBI found Twitter direct messages and tweets in which Borell admitted to taking down a number of websites.

Mobile Phone Malware

Android continues to be the fastest growing mobile platform, and also the most targeted by malware authors. This quarter we have seen many different types of Trojans designed to steal data from infected devices: from call and text message records to users' contact lists. Android is potentially exposed to far more security risks than its biggest competitor (iPhone and its iOS), as it allows users to get their apps from anywhere their want. However, using the official Android marketplace is no security guarantee either, as it has also been targeted by cyber-crooks luring users into installing Trojans disguised as legitimate apps. Something which, by the way, has also happened to Apple's App Store, but to a lesser extent than to Google's Play Store.

In this scenario, it was very surprising to hear that giant aerospace company Boeing is preparing to launch an ultra-secure Android-based smartphone. But hold your horses… Before we all start ordering it, it is worth mentioning that this smartphone will be mainly deployed by government agencies or other companies in need of airtight mobile security, so it will be very expensive. We don't have much information about it yet, but apparently the device will include communications encryption.

Social Networks

One of the primary objectives cyber-crooks have when launching attacks on social media sites is to gain access to users' accounts so that they can impersonate them and access their personal details or information shared with other users. On Twitter, for example, accessing a user's account will allow them to send direct messages (DMs) to the victims' friends as we have seen on so many occasions during this quarter. A typical example would be as follows: You receive a DM from one of your contacts informing you that someone has just posted some embarrassing pictures of you. If you click the link, you'll be taken to the following page:

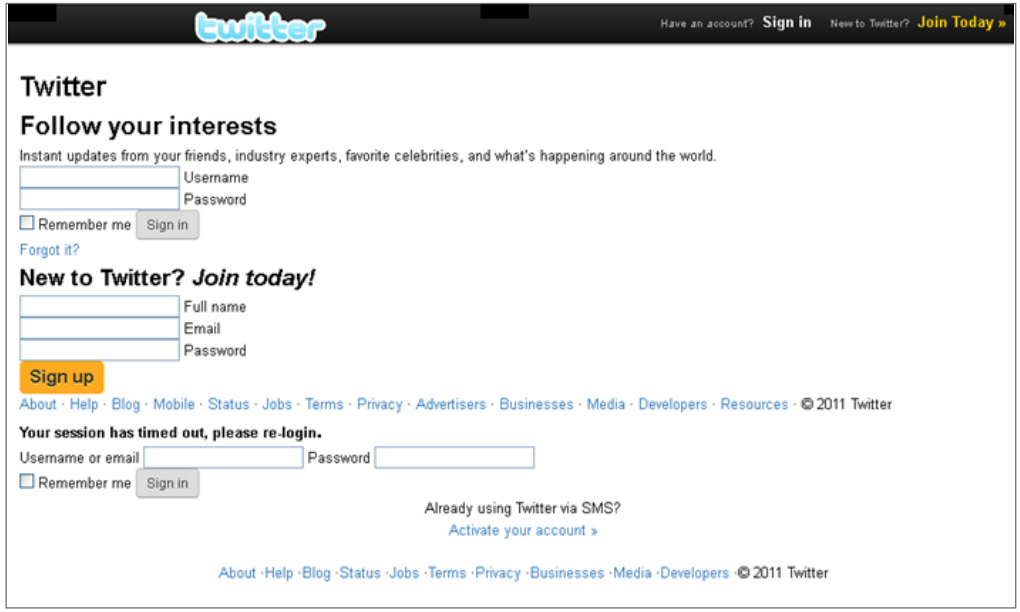

FIG.05. *PHISHING PAGE THAT STEALS TWITTER CREDENTIALS.*

This page informs you that your Twitter session has timed out and asks that you log in again. To make the phishing scam look as real as possible, all the links displayed on the page are actually Twitter links except for the "Sign in" and "Sign up" buttons, which will transmit the user data to the attackers. Once they have your Twitter login and password, they will begin sending the same misleading Twitter DM to all of your followers. This way, they will steal their Twitter login as well, and use their accounts to spread malware, send spam or turn those credentials into money by selling them to other cyber-crooks.

Social networking site **LinkedIn** had 6.5 million user passwords stolen and leaked online. Fortunately enough, however, these passwords were not stored in plain text files, but were encrypted. The bad news is that there was no other additional protection, so in case you haven't already done so, we advise that you change your LinkedIn password right now. And if you use that password for any other service as well, change it too, and always use different passwords for different programs and services.

Mac

Every time we discuss **Mac** threats, we present you with the cases that most caught our attention. Luckily enough, these infections are not massive, as despite the growth of Mac malware, the PC remains the biggest target for cyber-criminals. Unfortunately, many Mac users still believe they are immune to threats, even though little by little people, even at Apple, are beginning to realize that that is not the case. The Apple page that explains the reasons why Macs are better than PCs previously boasted that Mac systems 'don't get viruses' (a false statement, since macro viruses, for example, affect both platforms).

FIG.06. *APPLE'S WEBSITE SAID ITS OPERATING SYSTEM WAS VIRUS FREE.*

However, it seems that Apple is beginning to acknowledge the truth, as they have replaced the previous text with this one:

FIG.07. *APPLE REMOVES CLAIM OF VIRUS IMMUNITY.*

This change is probably related to the recent outbreak of the Flashback Trojan, a malware specimen responsible for the single most significant malware infection to ever hit the Mac community. This malware infected up to 600,000 Mac computers around the world, creating the largest botnet ever to target Apple computers. One of the Trojan's most unique features was that before infecting a computer, it checked to see if it had some kind of antivirus installed. If the computer was protected, Flashback didn't infect it; otherwise, it infected the Mac and triggered its payload.

This attack has once again demonstrated that, contrary to popular belief, Macs are in fact not immune to virus infection and malware, a myth largely exploited by cyber-criminals.

Cyber-war

In most cyber-war or cyber-espionage operations all you can do is speculate about who is behind the attack. It is extremely unlikely that a country openly admits to being responsible for carrying out this type of action. However, things might be changing. In a rare disclosure, U.S. Secretary of State Hillary Clinton admitted in May that U.S. intelligence agents had hacked into websites being used by Al Qaeda's affiliate in Yemen.

More specifically, the U.S. cyber experts hacked into Jihadist Web pages and substituted material that bragged about killing Americans with information about Muslim civilians killed in terrorist strikes.
Meanwhile, in South Korea, intelligence sources accused North Korea of running a special unit of elite hackers to steal military secrets and sabotage information systems of Seoul.

Flame

The Flame computer virus has been the highlight of the quarter without any doubts. Flame is a complex piece of malware used for information gathering and espionage in Middle East countries.

This malicious code is most likely created by a government or intelligence agency, and is clearly tied to the infamous Stuxnet malware (a Trojan reportedly designed and launched by the U.S. and Israeli governments in an attempt to sabotage Iran's nuclear program). Targeted attacks are generally carried out using Trojans, but in this case we are talking about a worm, which introduces a new factor: Worms can replicate themselves automatically, so virus authors could eventually lose control of who or whose computers their creations are infecting. That is really not advisable if you have a specific target to attack and want to stay under the radar in order to avoid detection. How did Flame resolve this? Well, the worm has a very curious and somewhat innovative feature: its ability to turn its spreading functionality on and off, something extremely handy when you want to go unnoticed.

One of the most striking features of Flame is that it can steal all kinds of data in multiple ways, even by turning on victims' microphones to record conversations.

As previously mentioned, this was undoubtedly a targeted attack aimed at specific individuals and organizations in the Middle East. And it seems that the cyber-espionage worm might have been active for many years without being detected by security companies, which has produced a number of conspiracy theories claiming that governments pressed antivirus vendors to not detect the worm. Obviously, this is completely false, and as soon as the worm has been discovered, it has been detected by all of them.

But, why did it take so long to detect Flame? Well, no antivirus solution has a 100-percent success rate at catching new, unknown threats. This is quite simple to understand: professional cyber-criminals make sure their malicious creations will go undetected before spreading them. They test them against all popular antivirus engines to make sure they cannot be detected by signature files or any other protection systems (behavioral and heuristic scanning, etc.). If you have the necessary resources at your disposal, you can set up a Quality Assurance process that eliminates the possibility of the malware being found, at least at the start. The threat will be eventually detected by antivirus solutions, but making it go unnoticed for as long as possible is the key to success.
For example, by infecting a small number of targeted computers instead of triggering a massive infection.

03| Quarterly figures

During the second quarter of the year we have collected over 6 million malware strains at the laboratory, a similar figure to the first quarter. The type of malware was also similar: four out of every five new malware specimens created were Trojans (78.92 percent). Here are the details:

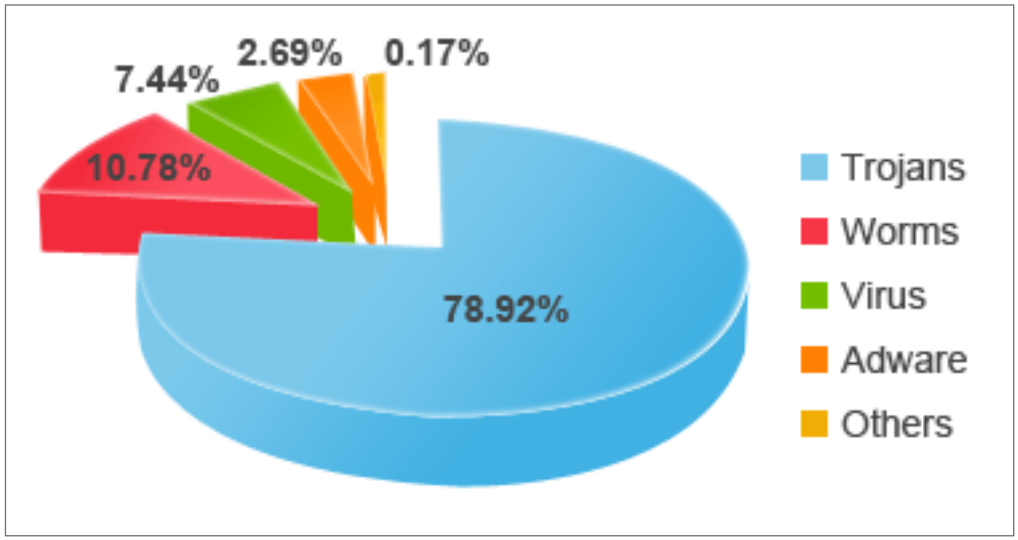

FIG.08. *NEW MALWARE CREATED IN Q2 2012, BY TYPE.*

When it comes to the number of infections caused by each malware category, Trojans occupied the first spot in the ranking according to our Collective Intelligence data: three out of every four infections were caused by Trojans. The graph below shows last quarter's distribution of malware infections:

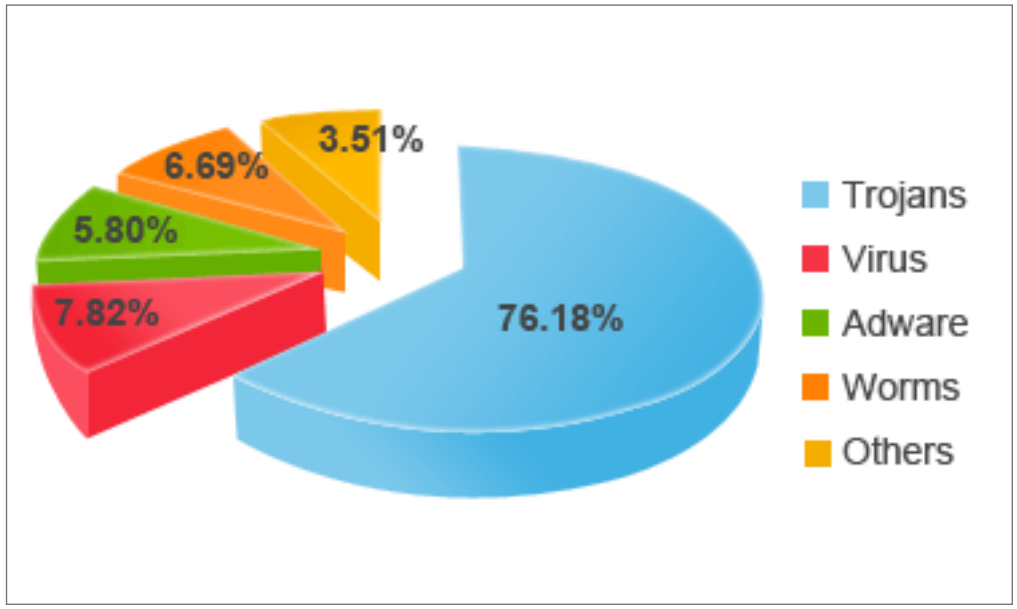

FIG.09. *MALWARE INFECTIONS BY TYPE IN Q2 2012.*

While, as expected, Trojans accounted 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 the quarter. The figures corroborate what is well known: massive worm epidemics have become a thing of the past and have been replaced by an increasing avalanche of Trojans, more specifically, banking Trojans and the infamous 'Police Virus".

Let's now look at the geographic distribution of infections. Which countries were most infected? Which countries were best protected? The average number of infected PCs across the globe stood at 31.63 percent, down almost four percentage points compared to Q1. South Korea led our ranking of most affected countries for the first time ever (57.30 percent of infected PCs), followed by China (51.94 percent). These were the only countries whose infection rates exceeded 50 percent. Next came Taiwan (42.88 percent). In the case of China, it is interesting to note that some of the country's most developed regions have much lower infection rates than the rest of the country; that's the case of Hong Kong for example, whose infection rate stands at a mere 23.36 percent. The graph below shows the ten countries with the most malware infections in Q2 2012:

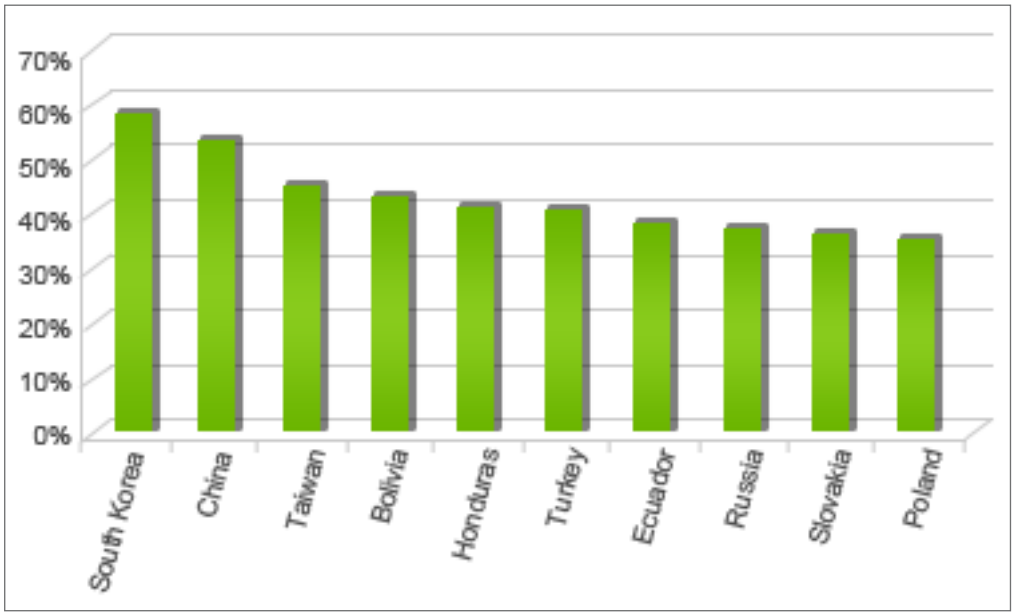

FIG.10. *MOST MALWARE INFECTED COUNTRIES.*

Even though the list shows countries from all over the world, the top positions are occupied by Asian countries. In contrast to the above numbers, none of the least infected countries had infection rates in excess of 25 percent. The list was dominated by European countries (with the sole exception of Uruguay), and topped by Switzerland (18.40 percent) and Sweden (19.07 percent). These were the only countries whose infection rates stood below 20 percent.

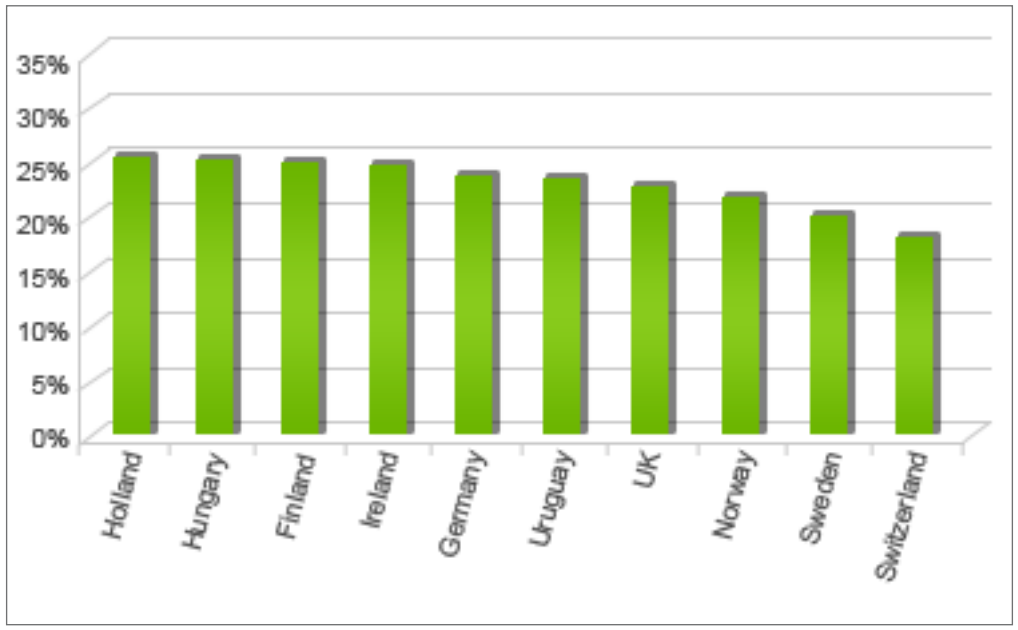

FIG.11. *LEAST MALWARE INFECTED COUNTRIES.*

Interestingly, the ranking of least malware infected countries is mostly dominated by technologically advanced countries. But, is there a correlation between the two aspects? Let's find out by analyzing the data from the countries belonging to the OECD (Organization for Economic Co-operation and Development). Here is the result:

DATA FROM THE COUNTRIES BELONGING TO THE OECD

South Korea	**57.30%**
Turkey	**39.29%**
Slovakia	**36.09%**
Poland	**35.74%**
Spain	**33.35%**
Czech Republic	**32.31%**
Chile	**31.94%**
USA	**30.03%**
Mexico	**30.00%**
Italy	**29.82%**
Australia	**29.56%**
Slovenia	**28.86%**
Denmark	**28.42%**
France	**28.40%**
Portugal	**27.56%**
Japan	**26.99%**
Belgium	**26.23%**
Austria	**26.18%**
Canada	**24.89%**
Holland	**24.74%**
Hungary	**24.54%**
Finland	**24.02%**
Ireland	**23.64%**
Germany	**22.61%**
UK	**21.01%**
Norway	**20.50%**
Sweden	**19.07%**
Switzerland	**18.40%**

Indeed, there seems to be a connection between technological development and malware infection rates. Even though there may be other factors that influence these results, you can see that only the first seven countries have percentages above the worldwide average, whereas the others, from the United States to Switzerland, stay below that barrier.

04| Conclusion

Everything seems to indicate that the number of threats that users will have to face will continue to grow, so now more than ever protection is essential: having a good security program, keeping antivirus solutions up to date, and using common sense are the best ways to avoid falling victim to the powerful social engineering ploys used by cyber-criminals.

We start the summer season with the London 2012 Olympic Games, so we are very likely to see cyber-attacks that use the sporting event as bait to trick and infect users. As previously advised, use your common sense to avoid these types of attacks.

As we enter the second half of the year, we'll continue to inform you about the latest news surrounding the computer security world, and fight the battle against malware and virus writers.

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