QUARTERLY REPORT PANDALABS

APRIL-JUNE 2013

01| Introduction

In this report we will be analyzing the statistics returned by our cloud-based malware scanning systems, which illustrate how cyber-criminal activity continues to increase, with more and more malware being created and saturating antivirus laboratories.

We will analyze some of the attacks witnessed in the second quarter of 2013, including the hacking of Twitter accounts by the 'Syrian Electronic Army'. We will also look at one of the latest malware attacks on the Android platform, and analyze the figures showing a worrying increase in malware targeting Google's popular operating system.

We discuss some of the major stories concerning cyber-war and cyber-espionage, and see what truth there is in one of the major stories of the year, regarding the claim that the NSA has been spying indiscriminately on users of the world's most popular platforms, including Facebook and Skype.

02| The Quarter at a Glance

This quarter started with good news, when it emerged that Russian and Ukrainian police had arrested the cyber-gang leader responsible for the Caberp botnet, along with 20 other individuals who were part of the malware development team. This was a joint action between these two police forces. The gang leader (28) is a Russian citizen living in the Ukraine.

CYBER-CRIME

Cyber-criminals often try to exploit newsworthy events or notable dates to try to spread malware to new victims. This was apparent during the second quarter of 2013 when they used the terrorist attack on the **Boston marathon**. Similarly, the news of a fatal accident at a Texas fertilizer plant was used as a ruse to spread malware.

> The news of the attack on the **Boston marathon** was used by cyber-crooks as a subject for spam messages

Another type of attack took advantage of International Workers' Day -May1- to compromise the US Department of Labor website and spread malware.

When talking about how cyber-criminals infect computers to steal data and profit from it, perhaps the first thing that comes to mind is theft of online banking credentials in order to steal from bank accounts. However, there are other, more imaginative types of theft that take place in virtual worlds.

For example, in **World of Warcraft**, the world's most popular MMORPG, cyber-criminals have stolen millions of 'gold' pieces from players' accounts. Investigations determined that this gold had been used to buy items in the game's auction house. It finally became clear that the attackers had exploited an error in the web and smartphone app to enter the auction house.

> An error in the Smartphone app for the **World of Warcraft** Armory was used by cyber-crooks to steal millions of pieces of gold

The British Federation of Small Businesses issued a report revealing that 41% of small businesses had suffered attacks from cyber-criminals during 2012, with a cost of 785 million pounds.

In the second quarter of 2013, the US government was responsible for a major blow to the financial structure used by cyber-criminal gangs around the world when it shut down **Liberty Reserve**, the favourite bank of cyber-crooks. This company enabled anonymous cash transactions, and investigations led to some of the owners being arrested. It's not yet clear what will happen to the money of the bank's legitimate clients who were not involved in any illicit activities.

> After several years of investigation, **Liberty Reserve** was shut down by the US government and the owners arrested

The **LivingSocial** website was the victim of a cyber attack that could affect as many as 50 million clients. Compromised information includes names, email addresses, dates of birth and passwords.

One of the most common ways for attackers to compromise computers is through security holes. Some major software development companies, such as **Google**, use reward programs to encourage researchers to discover new security problems, with rewards varying according to the severity of the problem discovered. Along these lines, **Microsoft** launched a new program in June offering rewards of up to $100,000 for people who discover new ways of by-passing security measures implemented in the new Windows 8.1. It has also offered an additional $50,000 if the discovery is accompanied by suggestions on how to defend against the attack.

In Spain, the government is considering legal reforms to allow security forces to use Trojans, with judicial control, to spy on suspects in certain investigations. As yet the bill has not gone through Parliament and could undergo changes. Since the proposal was announced many concerns have been raised over the potential for breaches of privacy. There is little legislation regarding this issue worldwide, Germany being one exception, where it is acceptable to use Trojans in investigations related to terrorism.

SOCIAL NETWORKS

In the second quarter of 2013 we saw the consequences of a hacked Twitter account. The 'Syrian Electronic Army' which was responsible for several attacks earlier in the year, hacked the Twitter account of the Associated Press. Once it had taken control of the account, it published a fake breaking news story: 'Two Explosions in the White House and Barack Obama is injured.' Immediately, numerous followers of the account helped the story to spread like wildfire, resulting in the Dow Jones index dropping 145 points.

It was discovered that the attackers had sent a malicious email to AP staff claiming to be an item from a major American newspaper. Recipients were encouraged to click a link in the mail. Anyone who followed the link would be taken to a fake Twitter sign-in page, and asked to enter their login credentials. This was how the 'Syrian Electronic Army' managed to take control of the AP Twitter account.

This same group has continued to launch attacks, with victims including CBS, who had three Twitter accounts hacked, including the '**60 Minutes**' account, and the satirical news site, the Onion.

> The Twitter account of the CBS '**60 Minutes**' program was hacked by the 'Syrian Electronic Army' group

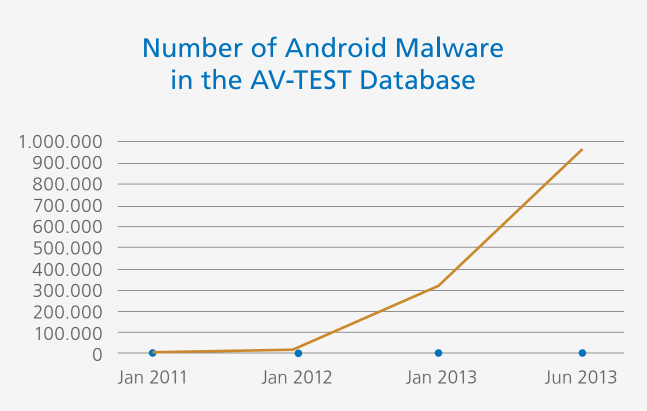
We are always reminding users of the importance of being cautious about the information they share on social networks. In some cases, even though all possible precautions are taken, a simple mistake can ruin your efforts. Facebook recently announced that an error had led to the phone numbers and email accounts of million users being revealed.

MOBILE PHONE MALWARE

In April, a new type of attack on **Android** operating systems was discovered. In this attack, malware was being spread through non-malicious apps. Many free apps include some kind of advertising as a way of financing the app, instead of charging for it. In this case, cyber-criminals apparently offered apps that were not in themselves malicious, but they controlled the advertising displayed.

Once they had enough users of these applications, they began to display ads with fake app update notifications, which if installed on the device, used a Trojan to send SMS messages to premium-rate numbers. There were 32 apps in all, and the total number of downloads through Google Play reached nine million.

While the amount of malware for Android is still low compared to Windows, it is definitely on the increase. According to **data published by AV-Test** in June 2013, there were already over 900,000 different strains of malware for this platform:



CYBER-WAR

With so many new developments in the world of cyber-espionage and cyber-warfare it would be impossible for us to relate all the stories that have come to our attention without dedicating an entire report to the issue. Here therefore, we cover just some of the most notable stories.

It has been revealed that Chinese hackers gained access to plans of more than two dozen US weapons systems. The Washington Post obtained an internal report of the Pentagon's Defense Science Board (DSB) detailing how they gained access to plans of **Patriot missiles** or **fighter aircraft such as the F-35**.

Chinese hackers stole **plans for the F-35 fighter** as well as other weapons systems

In any event, there is nothing new about such attacks aimed at the United States clearly originating from China. In fact, the Pentagon itself in its annual report to Congress accused China of being behind numerous attacks on U.S. intelligence data.

According to a report by Taiwan's National Security Bureau, the Chinese cyber-war machine continues to grow and now has about 100,000 personnel.

All these attacks have led to serious concerns from numerous governments, who are trying to implement security measures. Indonesia, for example, has recently announced the setting up of a military cyber-unit. The country's defense minister said that the main objective of the new unit will be to protect government portals and websites from cyber-attacks.

Usually when we talk about cyber-espionage we imagine two superpowers trying to access secrets from each other. This is sometimes the case, as we have seen in previous reports. Yet it would be a mistake to think that these are the only cases. Over the years, intelligence services have been keen to get information not just from 'enemies', but also from friends. Moreover, in some cases security agencies want to obtain as much information as possible from anywhere around the world, given that with globalization, people and information are moving faster than ever before and in order to maintain some control over what is happening means having access to all kinds of information, even about your own citizens, regardless of the legality or morality of such activity.

In June a story emerged that had spread around the globe in just a few minutes. On June 6 a Washington Post exclusive revealed that the U.S. **National Security Agency**, **the NSA**, had been spying on 'everyone' using a program called PRISM with the voluntary assistance of nine technology sector giants. Microsoft, Apple, Google, Yahoo, Facebook, Youtube, Skype, AOL, and PalTalk. The NSA had supposedly obtained any data they wanted on all of these companies' clients. This story was immediately echoed by media around the world.

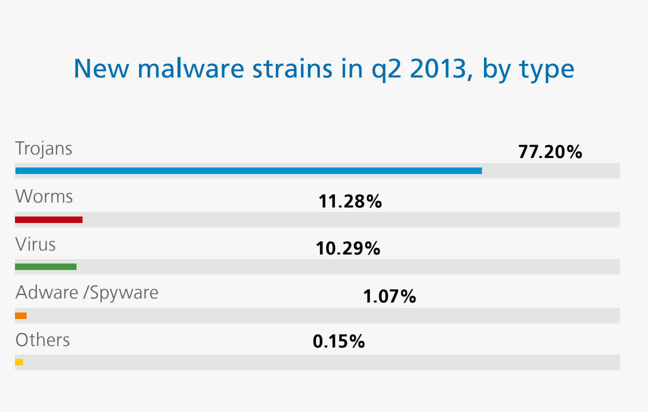
The NSA was reported to have used its PRISM program to obtain data from users of online platforms

These companies categorically denied the accusations. In fact, the Washington Post edited the story the following day, changing the title and deleting references to how the companies were voluntarily releasing all kinds of client data to the NSA. In a few days many media publications were questioning the *veracity* of the story and *suggesting* that it could stem from the misinterpretation of an internal presentation from the NSA.

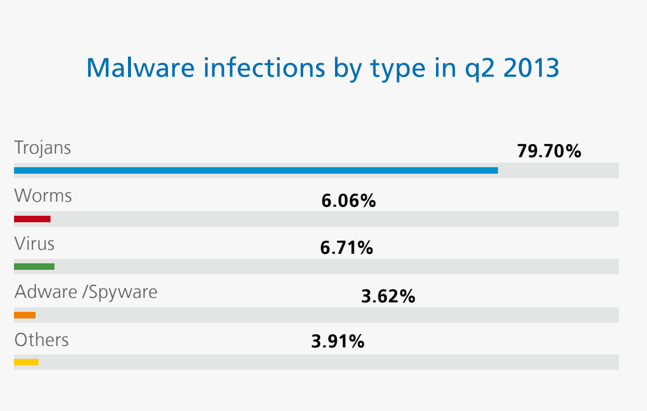
03| Malware Figures in Q2

The amount of new malware samples continues to rise. In the second quarter of 2013, 12% more malware was created than in the same period last year. When the data for the first and second quarter of 2013 is taken together, the increase on 2012 reaches 17%.

Regarding the different types of malware created, Trojans were the most popular accounting for 77.2% of all new malware created. This figure is even higher than the previous quarter.

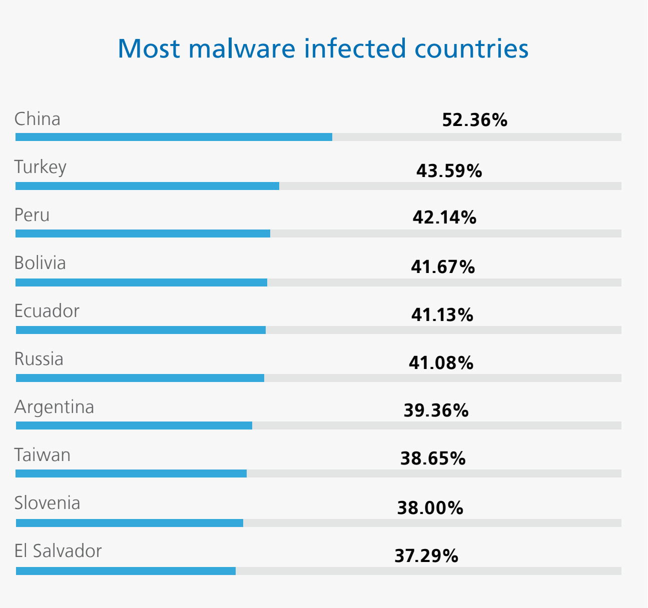


New malware strains in q2 2013, by type

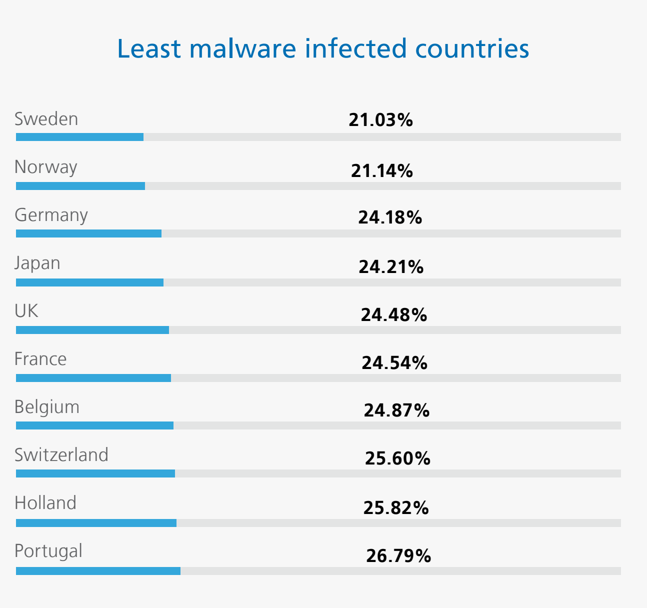


Trojan infections have reached record levels. Cyber-criminals use Trojans as a key tool to infect users, continually introducing changes to avoid detection and in many cases, automating the process of changing the Trojan. They use scripts and special tools in order to change the binaries run on victims' computers to evade the signature-based detection used by antivirus firms.

We will now look at how infections were distributed geographically. **In the second quarter of 2013, the global infection ratio was 32.77%, which was up on the first quarter.** As for the data for individual countries, China once again tops the table, and was the only country in the world with an infection rate over 50%. It was followed by Turkey (43.59%) and Peru (42.14%).



In this "Top 10", although there are countries from many regions, there is a **strong presence of Latin American countries**. In addition, the following countries have an infection rate over the global average. Brazil (35.83%), Poland (35.59%), Guatemala (35.51%), Colombia (33.86%), Spain (33.57%), Costa Rica (33.33%) and Chile (33.22%).



Europe continues to have the lowest infection rates. Sweden (21.03%), Norway (21.14%) and Germany (25.18%) are the countries with the lowest infection rates. **The only non-European country in the Top Ten was Japan**, in fourth place with 24.21%. Other countries outside this Top 10 but with infection rates below the average are: Denmark (27.08%), Finland (27.16%), Panama (27.52%), Canada (27.54%), Austria (28.74%), Uruguay (28.89%), Venezuela (30.11%), Australia (30.45%), USA (31.16%), Czech Rep. (31.58%), Mexico (32.35%), Hungary (32.74%) and Italy (32.76%).

04| Conclusion

This second quarter of 2013 has closed with malware creation at record levels. Figures for the first six months are 17% up on the same period in 2012.

Cyber-criminals continue to attempt to trick users with all kinds of tactics, exploiting any tragedy, such as the Boston Marathon. There have been major steps forward in the fight against these gangs, such as the closing of Liberty Reserve by the U.S. government after an investigation lasting several years.

China continues to occupy many of the headlines regarding cyber-espionage, although in this quarter, the USA has been in the eye of the storm after revelations about the PRISM program that the NSA used to obtain data from users of platforms such as Facebook, You Tube or Skype.

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/

06| 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

linkedin
http://www.linkedin.com/company/panda-security