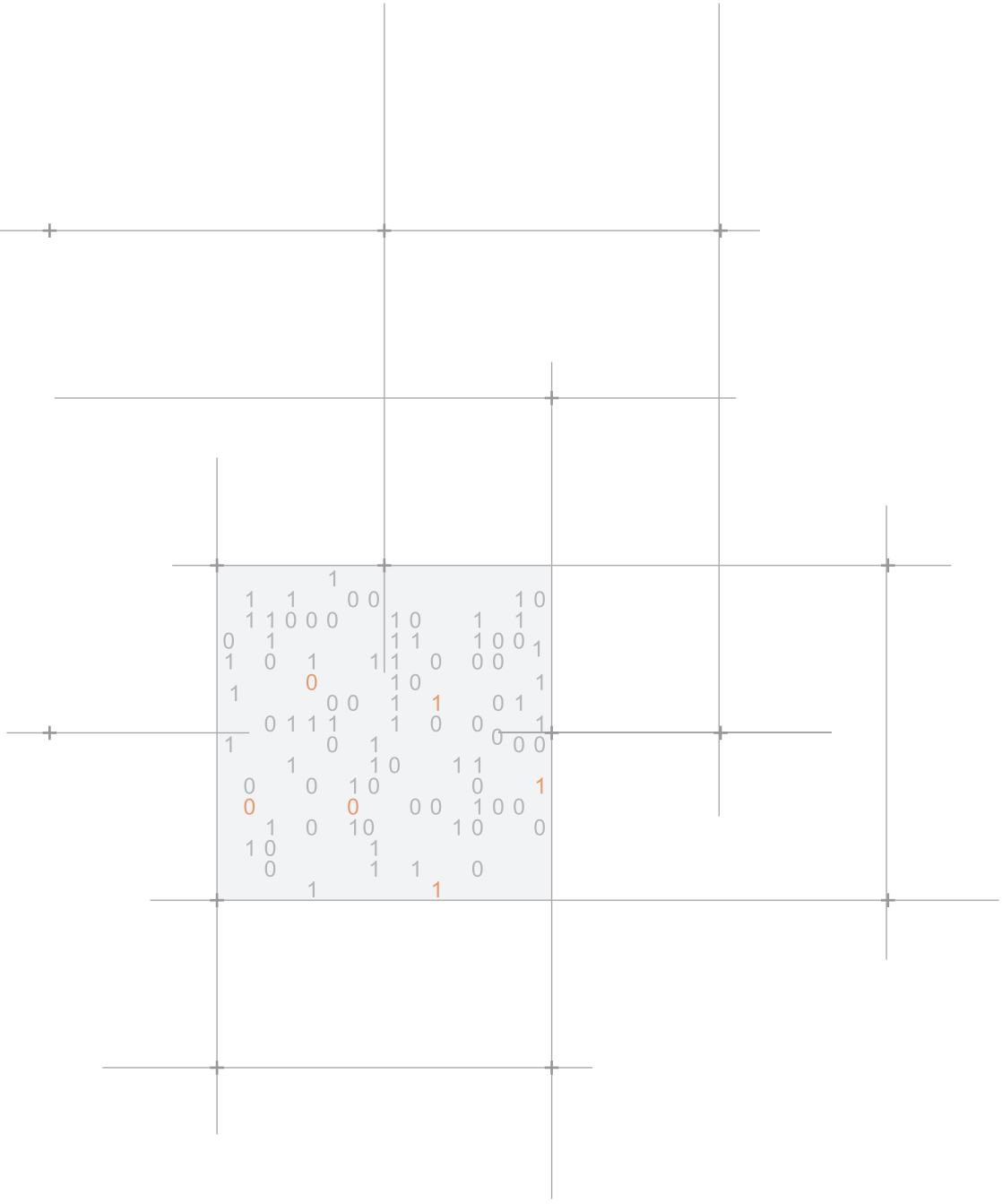
PANDALABS

THE EYE OF SECURITY

QUARTERLY REPORT

Q2 2014

PANDA SECURITY | *The Cloud Security Company*



INTRODUCTION

In this report we'll be taking a look at events in the world of IT security during the second quarter of 2014.

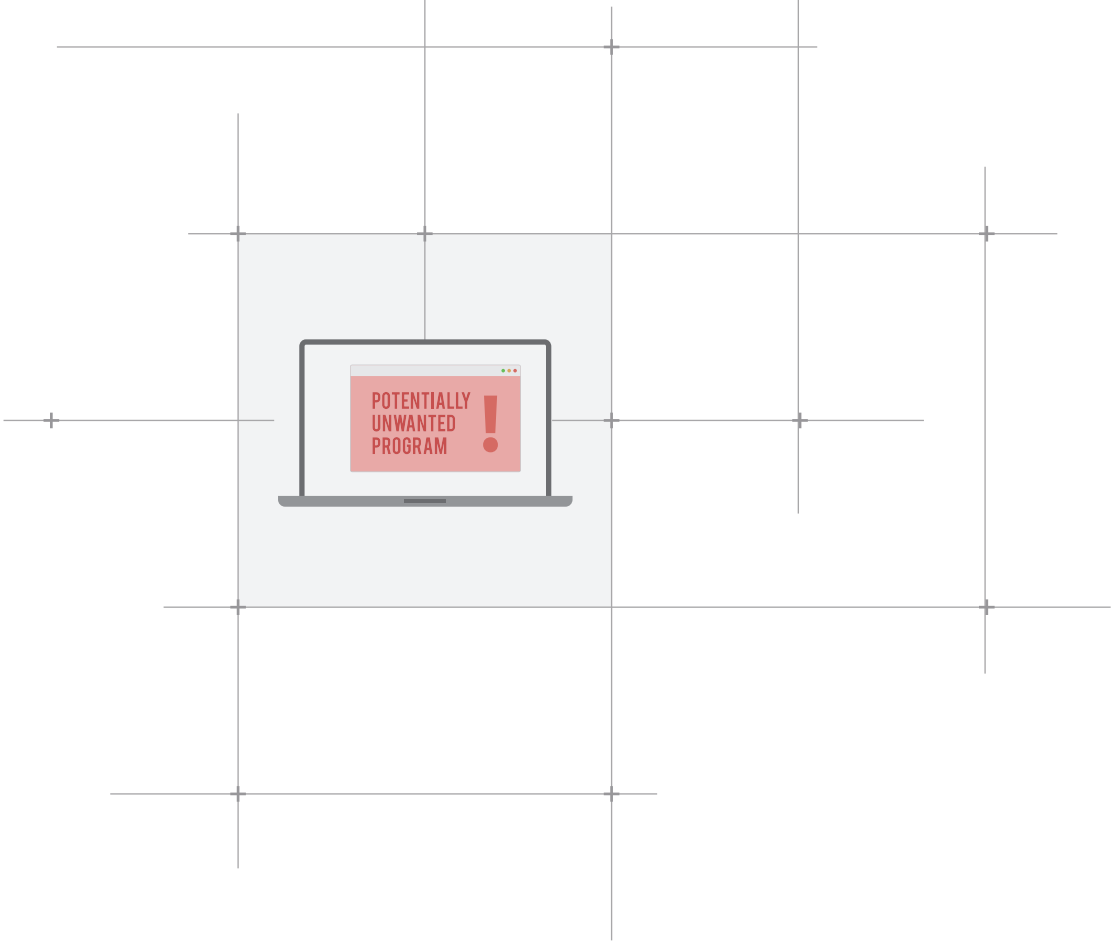
Malware continues to be created at the record levels we saw at the beginning of 2014

Users are under attack from many applications which although they may not install malware as such, are nonetheless unwanted by users. We will look at the impact of these **PUPs (Potentially Unwanted Programs)** in more detail later in this report.

We will also talk about the attacks suffered by companies such as **eBay, Spotify or Domino's Pizza**, as well as those launched by the cyber-hacking group the Syrian Electronic Army (SEA).

We will see how attacks on smartphones are no longer restricted to **Android**, but also **iOS,** which has been in the line of fire this quarter.

Regarding cyber-espionage, we will be reviewing the latest reported attacks, such as the one on the **Belgian Foreign Affairs Office**, and the impact of the most recent cases of Internet **spying** and the measures taken by some governments in consequence.

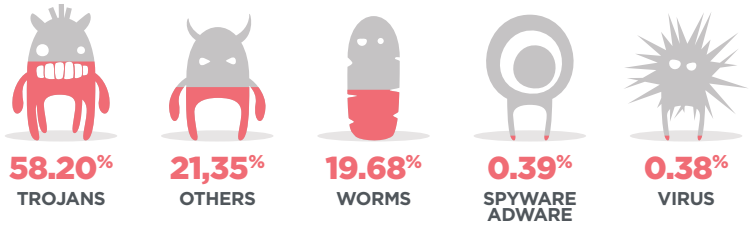


MALWARE FIGURES IN Q2

We started the year with malware creation reaching record breaking levels and the second quarter has been much the same. At PandaLabs we recorded 15 million new malware samples over the last three months, which represents an average of over 160,000 new samples created every day. While Trojans are still the most common type of malware, accounting for 58.20% of newly created threats, this is notably lower than the percentage recorded in the previous quarter. This, however, is not so much due to a drop in number of new Trojans rather to a substantial increase in PUPs (Potentially Unwanted Programs).

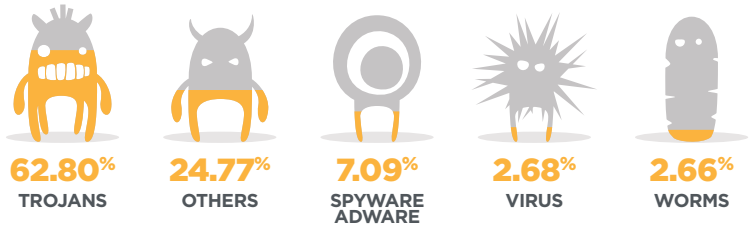
This increase in the number of PUPs is not by chance. Over recent months we have witnessed a significant increase in the creation of software bundlers, programs that install PUPs on computers along with the programs that the user actually wants to install -without asking for the user's consent. Although these bundlers have been around for some time, new companies have sprung up who exploit these programs and profit from installing unwanted software without properly informing the user. Panda Security has decided to protect our customers against this type of attack, which is why these programs are reflected in our data on newly created malware.

NEW MALWARE CREATED IN THE SECOND QUARTER OF 2014, BY TYPE



If we analyze infections around the world, the figures are similar to those for new malware created:

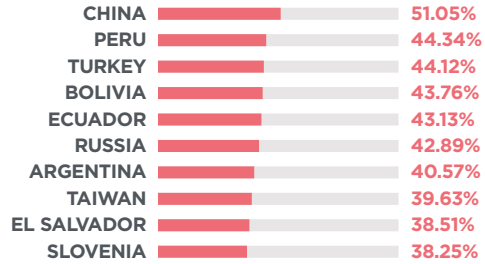
INFECTIONS BY TYPE OF MALWARE IN Q2 2014



Trojans continue to top the infections ranking, though PUPs also figure high up in second place, with a rate of 24.77%, which illustrates how these techniques are now being used massively. The global infection rate was 36.87%, a significant rise on recent quarters, once again due to the emergence of PUPs.

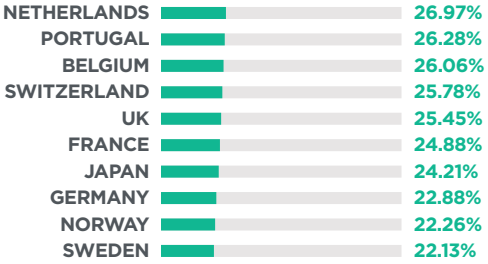
Regarding the data across different countries, China is once again in pole position, with an infection rate of 51.05%. This is followed by Peru (44.34%) and Turkey (44.12%).

COUNTRIES WITH THE HIGHEST INFECTION RATES



It's clear that the highest positions in the ranking are held by Asian and Latin American countries. China, once again, is the only country to have an infection ratio over 50%. Other countries with rates above the global average include: Brazil (38.19%), Poland (38.15%), Guatemala (37.99%), Colombia (37.86%), Spain (37.67%), Costa Rica (37.23%), Chile (37.05%) and Italy (36.88%).

COUNTRIES WITH THE LOWEST INFECTION RATES



Europe in general is the area with the lowest infection rates and nine European countries appear in this ranking. Sweden (22.13%), Norway (22.26%) and Germany (22.88%) are the countries with least infections worldwide. The only non-European country in the top ten most secure is Japan, which is in fourth place with 24.21%. Other countries still below the worldwide average are: Denmark (27.08%), Finland (27.19%), Panama (27.25%), Canada (27.58%), Austria (27.85%), Uruguay (28.45%), Venezuela (30.21%), Australia (31.45%), USA (32.17%), Czech Rep. (33.68%), Mexico (33.99%) and Hungary (36.05%).

THE QUARTER AT A GLANCE

This quarter has seen a lot of activity in the world of cybersecurity. In this report we will give an overview of the most important issues worldwide over this period. At the beginning of April, two stories generated a lot of concern:

- **Microsoft's decision to stop supporting one of the most popular operating systems of all time, Windows XP,** which is still used by millions of users around the world.
- The **discovery of an extremely dangerous security hole -dubbed Heartbleed- which affected many major websites**.

CYBERCRIME

Last April 8 was the date set by Microsoft to cease offering support for Windows XP

. In short, this means that users of this operating system will no longer receive security updates, so any new security hole discovered will not be patched. However, this coincided exactly with the appearance of a serious security hole affecting Internet Explorer and which could allow an attacker to infect a computer simply when the user visited a website that exploited this vulnerability. There was widespread panic, as attacks exploiting this flaw had already been detected, which led Microsoft to publish an update for the Windows XP version of IE even though it had stopped supporting the operating system.

Most security companies, including Panda Security, have opted to continue providing support and upgrades to all customers that still use XP. Nevertheless, users are strongly advised to consider migrating to a new operating system version that offers greater security, as it is not a question of 'if' new vulnerabilities will be discovered, but 'when'. And from that moment users will be running a risk that would be avoided if they were using a later version of Windows.

Heartbleed appeared in early April, just at the same time as support for Windows XP ended.

Basically, it was a security hole in the OpenSSL library, which is used for encrypting communications

Many Internet services, such as webmail, social networks, online banking, etc. encrypt communication to protect the data exchanged (bank login credentials, passwords, etc.). Servers using the vulnerable library were vulnerable to attack. The problem involved a module that allows open connections to be reused (called 'keep alive'), enabling up to 64 KB of memory on the compromised system to be repeatedly available to an attacker. However, it wasn't a complete disaster, as at least attackers weren't able to choose which part of the memory they had access to, and also a library was released to fix this bug.

Some days later, a 19-year-old Canadian student was arrested for exploiting Heartbleed to steal the data of 900 Canadians from the country's tax office. The Canada Revenue Agency had blocked public access to their online tax service a day after the security flaw had been discovered and made public, yet they did not manage to prevent this attack.

One of the biggest and most controversial attacks during this second quarter involved **eBay**. The online auction company asked all its users to change their passwords as a result of a cyber-attack.

It appears that the attackers managed to obtain the credentials of eBay employees and used them to access the company's network

They access to the database containing customer names, encrypted passwords, email addresses, postal addresses, phone numbers and dates of birth.

The controversy however was not due to the attack itself, rather how the company communicated it. At first it seemed that eBay was downplaying the attack, and the incident was not even mentioned visibly on its website.

Yet given the seriousness of events, the company was left with no choice but to change tack and release a highly visible notice on its home page asking all users to change their passwords.

Moreover, PandaLabs has detected that cyber-criminals, taking advantage of this incident, are sending phishing emails purporting to be from eBay notifying users of the security problem and providing a (malicious) link for them to change their passwords.

If users follow this link and enter their details, they will be handing over their eBay credentials to cyber-criminals

Another well-known technology company, **Spotify**, was also the victim of an attack that compromised its corporate network. The interesting thing about this incident however was that it only targeted a single user, something really quite unusual. It either could have been an attack aimed at obtaining information from a single user or an attempt by cyber-criminals to see how far they could get.

Similarly, the **Reuters** website was attacked by the Syrian Electronic Army. In this case it wasn't a Reuters' security problem that led to the attack, instead the victim of the attack –and the route of entry for the hackers– was a service provider used by the company.

The **Domino's Pizza** fast-food chain was also targeted by a group called Rex Mundi, who stole the data of 650,000 customers in France and Belgium, and then asked for a ransom for the information. Company officials however said they refuse to give in to blackmail.

Hector Xavier Monsegur, alias Sabu, was arrested by the FBI on June 7, 2011. Many of you will remember him as one of the leaders of Anonymous and Lulzsec. Sabu pleaded guilty to a series of offences and is now facing up to 124 years in jail. Since his arrest however, he has been working with the FBI helping to collect evidence leading to the arrest of other cyber-criminals. As the prosecution acknowledged, with the help of Sabu they have prevented some 300 cyber-attacks over a period of three years. After his arrest he spent seven months in prison and is now awaiting sentence. In May this year Sabu was finally released, having repaid his debt to society thanks to the help he has offered security forces

This second quarter has also witnessed one of the heaviest sentences handed out to a hacker. **David Ray Camez**, one of the ringleaders of a page which traded in stolen credit cards was sentenced to 20 years in prison and ordered to pay $20 million in damages.

A huge worldwide police operation, headed by the FBI, neutralized the Blacksades group

This group used a RAT (Remote Access Tool) -of the same name as the group- to carry out a series of crimes related with stolen user credentials. This was one of the biggest security operations in history against these types of criminals.

Another major action against cybercrime, once again featuring the FBI, was the bringing down of the **GameOver Zeus** botnet, a family of malware that used P2P communication, which made it really difficult to combat as it didn't rely on servers that could be neutralized.

Moreover, the FBI has now pressed charges against the person who controlled the botnet, Russian citizen **Evgeniy Mikhailovich Bogachev**. Bogachev, who is now on the Bureau's 'most wanted' list has also been accused of infecting systems with CryptoLocker.

SOCIAL NETWORKS

The Syrian Electronic Army hijacked four Wall Street Journal (WSJ) Twitter accounts

The accounts were those of WSJ Africa (@wsjafrica), WSJ Europe (@wsjeurope), WSJ Vintage (@vsjvintage), and WSJ.D (@wsjd). WSJ rapidly discovered the incident and deleted tweets published by the attackers.

The Twitter account for **British Gas** customer support was also hijacked. In this case the hackers started releasing tweets with links that took users to a replica of the Twitter page asking users to enter their login credentials. If they entered them, they would be handing over their details to the cyber-criminals who could then access and use their accounts.

June 12 marked the opening of the World Cup finals in Brazil. A cyber-criminal took advantage of the opportunity to try to steal the Facebook credentials of players of **Top Eleven: Be a Football Manager**, one of the most popular fantasy football games, with over 10 million followers on Facebook.

The attacker used Windows malware disguised as an application. Supposedly, having downloaded the application users could earn tokens for Football Manager that can be used to buy players. Obviously, this wasn't really the case, and those who followed the instructions in the application, apart from not earning tokens, would also risk losing access to their email or Facebook accounts.

SMARTPHONES

When we talk about security incidents affecting smartphones we normally talk about Android, as it is the most popular operating system. This quarter however we saw several notable attacks on the Apple operating system, iOS.

In April, a malware campaign was uncovered that targeted jailbroken iPhones/iPads

I.e. those that have been modified by their owners to install applications on them without having to go through the official App Store. The malware, apparently from China, is designed to steal user credentials.

Another case featuring Apple's mobile devices took place in Australia. An Australian newspaper reported that some of the country's Apple users had discovered that their devices had been hijacked, although it's not clear how many users were affected. The story revealed that a number of users discovered a message asking them for $100 in exchange for handing back control of their devices. It would appear that cyber-criminals had somehow managed to get hold of the Apple credentials of these users, and had impersonated them to remotely lock the devices using the Find my iPhone option which can locate and lock lost or stolen phones. The hackers would only send the new password needed to unlock the phone once the ransom was paid. What seems most likely is that cyber-criminals have hacked the database of the Apple fan forum, and, having stolen login credentials for the forum, have tried to see whether users had the same password for iCloud services. If the passwords matched, they hijacked the device and demanded a ransom.

In the world of **Android** there have been all kinds of stories and attacks, though the most striking are related to fake antivirus software and ransomware. One so far unique case was that of an app called Virus Shield, which rose to the top of the most popular apps on Google Play. It appeared to be a paid antivirus application, costing $3.99 However, it offered no protection whatsoever, but had an interface that simulated scans and smartphone protection. It reached more than 10,000 downloads before Google removed it and reimbursed the scammed users.

This quarter we also saw a new family of Android malware emerge, called **Android/Koler.**

This attracted coverage in the media as it was an attack similar to that of the Police Virus that previously affected Windows computers

In this case however the malware cannot encrypt data. It's still quite annoying nevertheless and difficult to remove if you don't have an antivirus on your phone, as the message it displays obscures everything else, and users only have a few seconds to try to uninstall it.

While we were analyzing it in PandaLabs, we came across a new variant, identical to the first one, but which connected to a different server. And this server was still active… In this case the cyber-criminals had made a small mistake, and had left the door ajar while configuring it. Sadly we couldn't access all the information there (a mysql database with data on infections, payments, etc.), though we were able to download files from the server and take a look at how it operates.

The way it works on the server side is similar to the malware that targeted Windows computers: several scripts geotag the device and display a message in the local language along with localized security force images. Information

from all **infected devices** is saved in the database along with the MD5 of the corresponding malware. This makes it possible to track the number of infections with each variant of the malware and measure the success of different infection campaigns.

The malware is designed to attack users in 31 countries worldwide, 23 of them in Europe: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Slovakia, Spain, Sweden, Switzerland and the UK. The remaining countries where users could also be targeted are: Australia, Bolivia, Canada, Ecuador, Mexico, New Zealand, Turkey and the USA.

Another type of ransomware appeared this quarter, this time originating in Russia. This malware really did encrypt information (images and videos) on devices and demanded a ransom to release them.

As if it wasn't enough to have malware for smartphones lurking in app stores or on any web page, there has even been a case where the malware came pre-installed. This was the case with a Chinese manufacturer, who included a data-stealing Trojan that sent information to a server in China.

CYBERWAR

One of the most interesting cases that occurred during the last quarter was in Belgium.

The Ministry of Foreign Affairs had been compromised by hackers

Russia was once again suspected of being the source of the attack, though we have to reserve judgment, as the investigation is still ongoing and it may take time to find out what really happened.

In the UK, a senior government official confirmed that an attack originating from a 'foreign power' had been detected. The attackers managed to access the account of a system administrator of the Government Secure Intranet, although the attack was nipped in the bud and no data was stolen.

Regarding internal espionage, **Charles Farr**, Director General of the Office for Security and Counter-Terrorism has said that communications over **social networks** or foreign search engines are understood by the British Government as being "external", meaning they don't need a court order to obtain access to information or communications across Google, Twitter or Facebook.

Such statements, along with all the recent scandal regarding the NSA is leading to a change in the way users behave. In fact, according to a recent study, there is now more than twice the amount of encrypted traffic circulating on the Internet than there was before these massive espionage cases were leaked. And this is not the only consequence, the German Government has canceled a contract with US telecom company Verizon, as part of its reshaping of internal communications, after revelations of spying by the US government, who had even tapped the phone of Chancellor Angela Merkel.

CONCLUSION

The second quarter of 2014 lived up to expectations, and despite numerous attacks, there was also a lot of good news in the fight against cybercrime, mainly involving the FBI. Among the main conclusions of this report is the fact that that malware is still being created at the record levels reached in the previous quarter.

15 million new samples were generated, at an average rate of 160,000 every day

Along these lines, while Trojans are still the most common type of malware, accounting for **58.20%** of new malware, this figure is significantly lower than the previous quarter **(71.85%)**. This is not so much due to a drop in number of new Trojans, but more to a **substantial increase in PUPs** (Potentially Unwanted Programs).

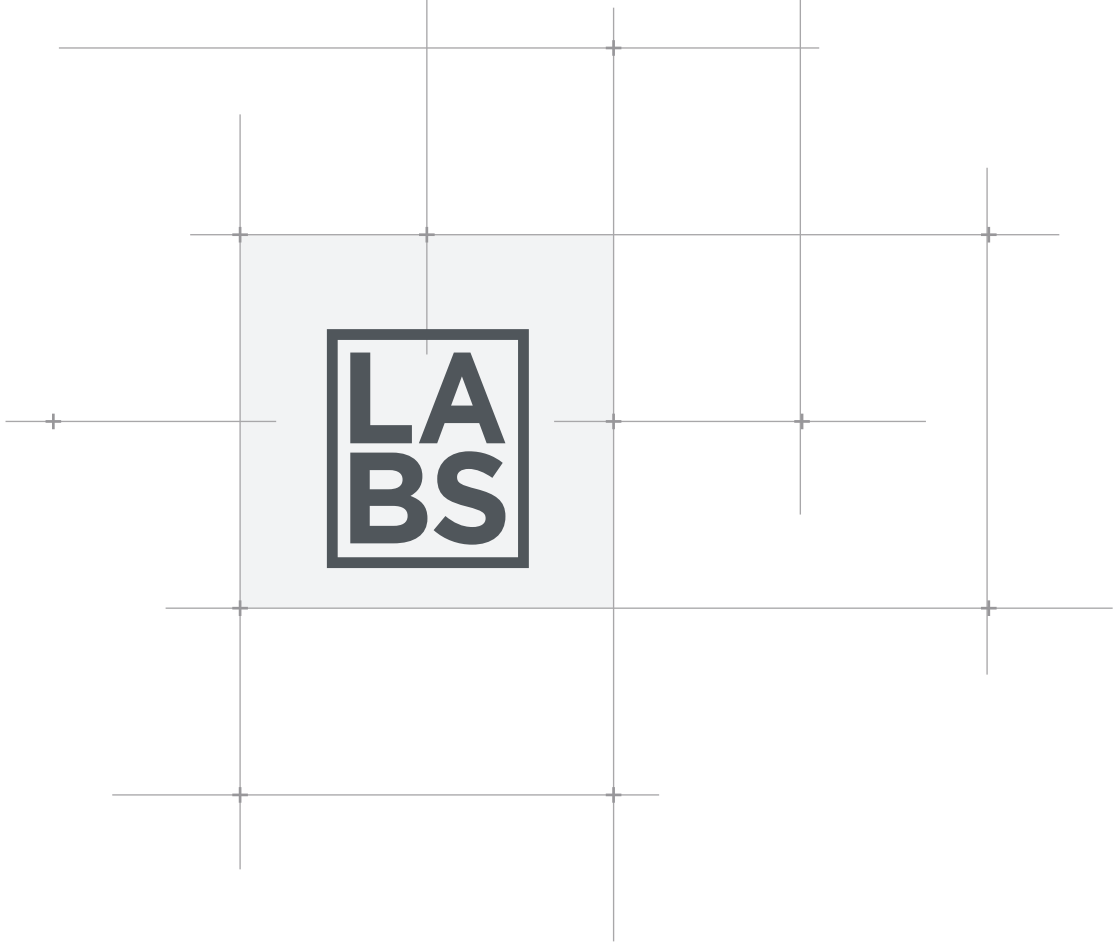
We are now half way through 2014 and in the coming six months we will be watching out for news and developments in the world of IT security, where we will no doubt witness new attacks targeting companies in strategic sectors and which we will discuss in future reports.

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.



https://www.facebook.com/PandaUSA
https://twitter.com/Panda_Security
https://plus.google.com
http://www.youtube.com/pandasecurity1
http://www.linkedin.com/company/panda-security
http://mediacenter.pandasecurity.com