PANDALABS QUARTERLY REPORT Q1 2016

panda

pandalabs

panda

pandalabs

1. INTRODUCTION

1 Introduction

So far, 2016 has been loaded with novelties in the world of security. The malware created continues to beat records, including more than 20 million new samples that were identified by PandaLabs during the first three months of this year, an average of 227,000 per day.

More and more companies are falling into ransomware traps. In detail, we will show you all of the new things occurring related to these types of attacks (including attacks on Linux, Mac, and even web pages). We will see how it is possible to rescue a few hundred to millions of euros, and analyze the hospital cyber-attacks that have happened during these past few months.

Critical infrastructures are a very sensitive area and focal point for cyber-criminals. One of the biggest attacks that occurred recently was in Ukraine. In the wintertime, the attackers were able to remotely cut off the power supply belonging to 200,000 customers, for hours.

Attacks have continued to grow in another area: Smartphones. In addition, with the Internet of Things, we learned how we might be able to attack something as seemingly innocent as a doorbell.

2. Q1 IN NUMBERS

2 Q1 in numbers

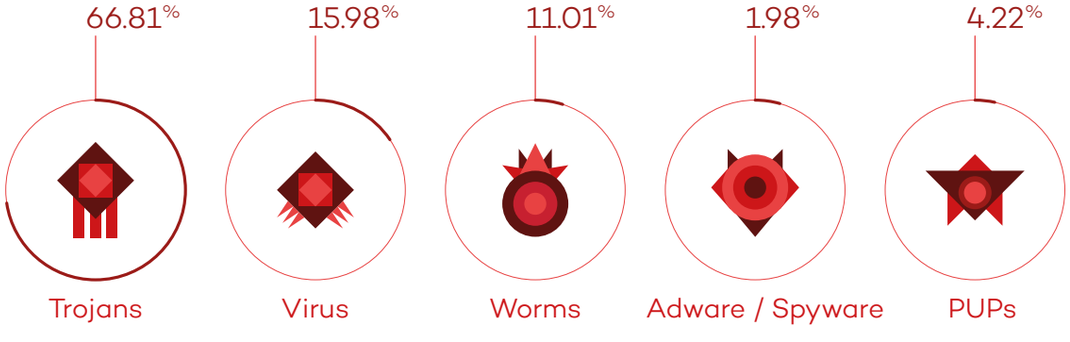
We started the year with more than 20 million new malware samples detected and neutralized by PandaLabs, Panda Security's laboratory (an average of 227,000 samples per day). This number is slightly higher than discovered in the same quarter in 2015, where the average was 225,000 samples per day.

Out of all samples, trojans were the most destructive type of malware and have been in the lead for years.

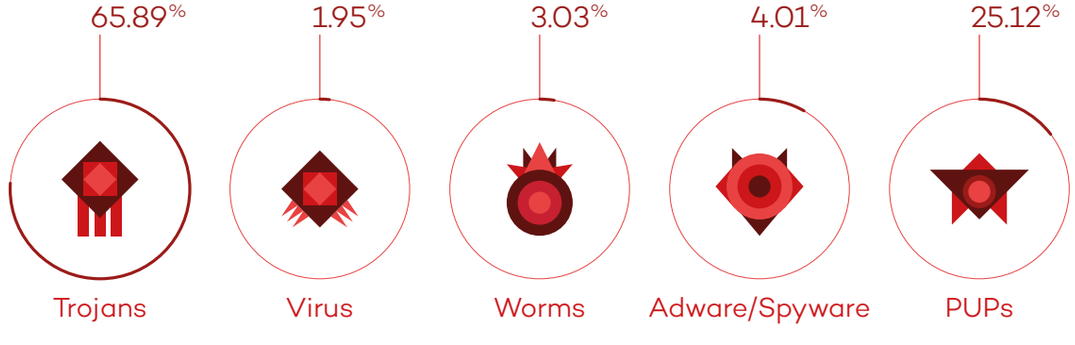
Note that the type of ransomware attacks that are covered in the same category have noticeably increased. The following data show the proportion of malware created in 2015 by type:

The following data shows the proportion of malware created in Q1 2016 by type:

NEW MALWARE CREATED
IN THE FIRST QUARTER OF 2016, BY TYPE



INFECTIONS BY TYPE OF MALWARE
IN THE FIRST QUARTER OF 2016



Trojans are the number one type of malware with 66.81% of the samples created during this quarter, an increase from the previous year. Then in second, are viruses (15.98%), worms (11.01%), PUPs (4.22%), and Adware/Spyware at 1.98%.

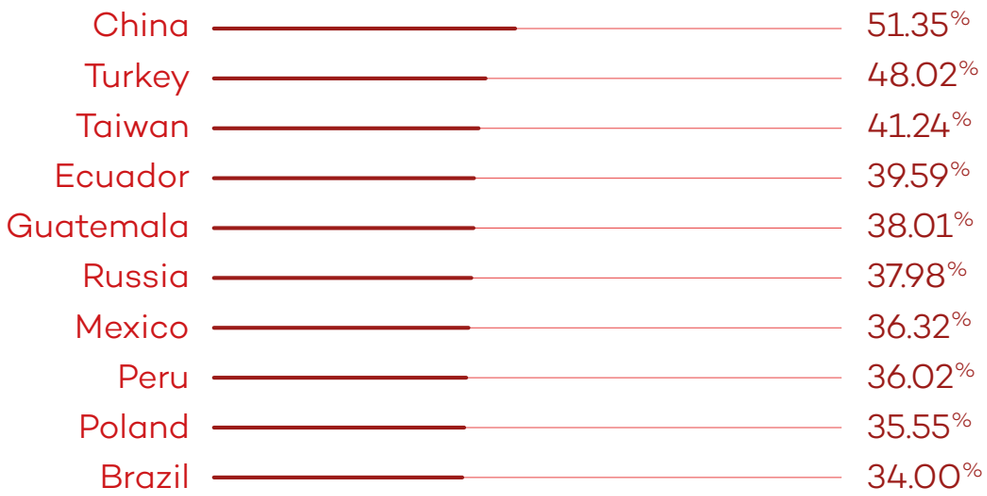
Thanks to the data provided by Collective Intelligence, we are able to analyze the infections caused by malware in the world. We can see that most infections are also caused by trojans (65.89%). Let's see how these infections have been distributed by category:

Taking into account the rise of ransomware infections, it makes sense that the trojans are in first place, which are one of the most popular cyber-criminal attacks since it allows them to make money in a way that is both simple and safe for them. The PUPs are positioned in second place with a quarter of the infections, well ahead of the Adware/Spyware (4.01%), worms (3.03%) and viruses (1.95%). The aggressive techniques used to distribute the malware include legitimate software programs used by PUPs. This makes it possible for them to achieve a high rate of installation in users' computers.

If we look at the overall percentage of infected computers, it is at 33.32%, somewhat higher than the previous year, increasing because of ransomware and PUP attacks. It should be noted that it is only a percentage of computers that have had some kind of "encounter" with malware, which does not necessarily mean that they have been infected. The world's infected countries are led by China, with 51.35% of infections, followed by Turkey (48.02%) and Taiwan with 41.24%.

Then we can see the 10 countries with the highest rate of infection:

COUNTRIES WITH HIGHEST RATE OF INFECTION IN THE FIRST QUARTER OF 2016

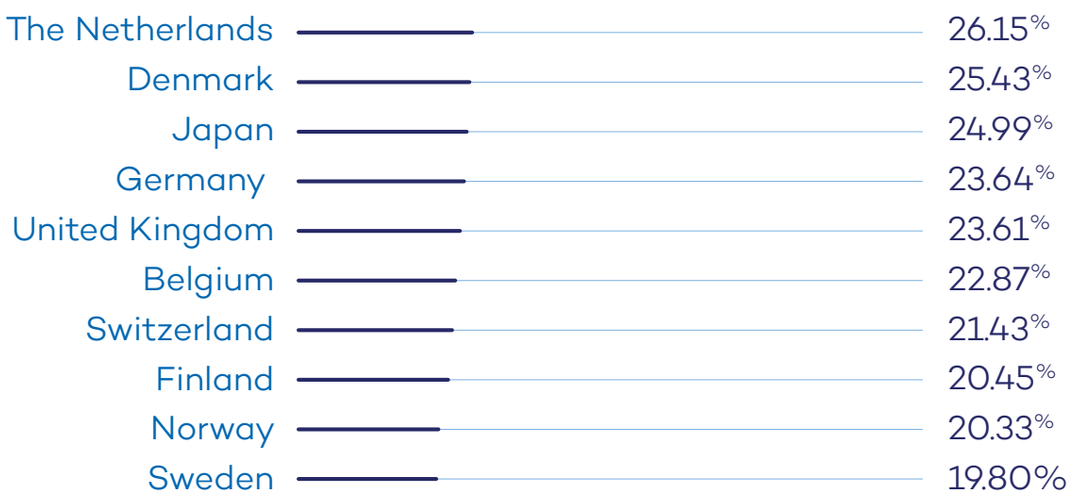


Asia and Latin America are the regions with the highest infections. Other countries with more than the world average, are Uruguay (33.98%), Chile (33.88%), Colombia (33.54%) and Spain (33.05%).

Analyzing the lowest infected countries, we can see that virtually all of them are European. The Scandinavian countries, as usual, are at the top: Sweden is in the lead, with 19.80% of infections, closely followed by Norway with 20.23% and Finland with 20.45% of infections.

Below you can see the 10 countries with the lowest rate of infection:

COUNTRIES WITH THE LOWEST RATES OF INFECTION IN THE FIRST QUARTER OF 2016



Other countries with a percentage lower than the world average are Australia (26.79%), France (27.20%), Portugal (27.47%), Austria (28.69%), Canada (30.30%), United States (30.84%), Hungary (31.32%), Italy (32.48%), Venezuela (32.89%) and Costa Rica (33.01%).

3. THE QUARTER AT A GLANCE

3

The quarter at a glance

Reviewing what happened during these past few months, we are able to inaugurate a new subsection devoted exclusively to ransomware. While it is true that we've already addressed these attacks in our reports, their prevalence continues to increase—especially in business—so we have decided to treat them jointly.

Ransomware

We can see how lucrative these attacks are by the way they attack diverse platforms: in addition to the usual (and mainstream) Windows attacks, we have seen new and improved variants of the Linux/Encoder using the Penguin operating system. Apple isn't even spared. We have seen a ransomware Encoder, named KeRanger, who managed to infect Apple-based users.

However, attacks are not only encrypting computers files, but they have also begun to attack websites by encrypting their contents.

In particular, we have seen cases where the attackers hack into websites based from Wordpress, then the files are encrypted and the index.php or index.html is modified with the contents of a message that says that a ransom must be paid in order to recover them. They have also included a chat feature to communicate directly with the robbers to "formalize" the payment.

The techniques have also advanced and in some cases have become especially aggressive, as in the case of Petya, where instead of encrypted documents it goes directly to the computer's Master Boot Record (MBR), leaving it unusable unless the ransom is paid.

The abuse of tools like PowerShell system is also increasing (as we predicted in the PandaLabs' Annual Report 2015), installed by default in Windows 10, and is being increasingly used in attacks that try to avoid detection by security solutions installed on victims' computers.

Attacks on companies are becoming more sophisticated. In recent times we have witnessed attacks where, after compromising a company server, they use lateral movements to infect as many computers on the company network as possible (with ransomware, so they can ransom more money).

Ransomware distribution has increased during these months and we have seen cases where they have even used top of the line websites (The New York Times, BBC, MSN, AOL, etc.) to infect visitors.

The websites are not hacked, but the attacks are launched through advertisements displayed on them, controlled by cyber-criminals and calling a server with some sort of exploit kit (Angler, etc.) so they can infect those users who do not have all their applications updated.

According to a survey by the Cloud Security Alliance, some companies are willing to pay up to one million dollars to recover their data. Although it may seem like an exaggerated encryption, we must keep in mind that some of the attacks not only encrypt the company's information, but they take it, which explains why some companies are willing to pay even if they have backups in order to prevent their stolen information from becoming public.

In January, The Economic Times in India reported that three banks and a pharmaceutical company had been the subject of a ransomware attack.

The attack began compromising IT managers from different companies, and then infected other company computers, reaching a ransom of 1 Bitcoin per infected computer. The total bailout was about several million dollars.

If there is a specific business sector that is suffering from this kind of attack, it is the hospital sector. In recent months we have seen how cases have multiplied. Here, we'll review some of the most shocking cases:

Hollywood Presbyterian Medical Center in Los Angeles declared an "internal emergency" and left its employees without access to their patients' medical records, emails and other systems. As a result, some patients could not receive treatment and others had to be taken to different hospitals.

The bailout requested by cyber-criminals was 3.7 million. Finally, the hospital's CEO reached an agreement and paid about $17,000 to recover the hijacked files.

MedStar Health had to disconnect some of its systems in their hospitals in Baltimore because of a similar attack.

The Methodist Hospital in Henderson, Kentucky was another victim. In this case they paid a ransom of $17,000 (some sources said the payment was significantly higher than this figure).

Prime Healthcare Management, Inc. has also fallen into the cybercriminal network. They were attacked in two of their hospitals (Chino Valley Medical Center and Desert Valley Hospital). Many others were affected by this same attack. This time, the company did not pay a ransom.

American hospitals are not the only targets. In Europe, we have seen similar cases. The Deutsche Welle published that several hospitals were attacked by ransomware, like the Lukas Hospital in Neuss and Klinikum Arnsberg in North Rhine-Westphalia. Neither hospital paid the ransom..

Cyber-crime

Neiman Marcus reported that some of their clients' accounts were compromised by attackers. 5,200 accounts were affected. Apparently, the company did not suffer from credential theft, but the attackers used stolen credentials from other companies to see what would work on the online service. This reminds us of the importance of two-step verification.

The Rosen Hotel & Resort chain were victims of an attack from September 2014 until February 2016. The company warned its users that if they used their credit or debit card during that time in any of their establishments, then their data may have been stolen by the attackers.

A Chilean hacktivist group has stolen 304,189 Chilean data from the database CONADI (National Corporation for Indigenous Development), a public agency under the Chilean government. Attackers published the database along with a message that denounced poor safety systems and demanded resignation of the Chilean president.

The US service, Verizon, fell victim to an attack. Data belonging to a million and a half of their customers was stolen. According to Brian Krebs, who uncovered the case, cyber criminals sold the stolen information for a total of $100,000 (they also gave an option to buy “pieces” of it for $10,000).

A new vulnerability that affects OS X could give an attacker full access. The vulnerability can skip protection “System Integrity Protection” (SIP), first introduced in “El Capitan”.

When we talk about “phishing” we usually think of the typical emails trying to pass as our bank in order to cheat us and get our log-in information. However, there are more sophisticated and ambitious invasions, like the one that affected the Barbie and Hot Wheels manufacturer, Mattel.

A senior executive received a message from the newly appointed CEO requesting a transfer of three million dollars to an account in China. Once the payment confirmed what the CEO had done (who was surprised because he had not sent the order), Mattel contacted the US authorities and their bank but it was too late because the money had already been transferred.

They were lucky because it was a public holiday in China and there was enough time to alert the Chinese authorities. They froze the account and Mattel got their money back.

This type of attack has become extremely popular. The attackers pose as company executives and request money transfers to an employee in the company. Before requesting

the transfer, they trick the employee using information from social media to make the deceit more believable.

21st Century Oncology Holdings, a Florida-based clinic specializing in cancer treatments, warned 2.2 million of their patients and workers in March that their personal data may have been compromised.

The attack took place in October 2015, but the FBI requested that they keep the information private until the investigation progressed further. The attackers gained access and stole personal data (name, social security numbers, diagnosis, treatment, health insurance data, credit cards, etc.).

Some will remember the famous “police virus” and forerunner to the current ransomware, that posed as security forces in the country where the computer was and asked for €100 fines. One of these cyber-gangs was dismantled by the Spanish police, and in this quarter we learned their sentence. The gang was made up of 12 people: the head of the organization, Alexander Krasnokutsy, was sentenced to six years, and his deputy Dmytro Kovalchuk, will serve a three-year sentence. The others, brothers Sergey and Ivan Barkov, have agreed to two years. The rest of the organization will have penalties of up to 6 months in jail.

If Flash is the number one browser plug to infect new victims—with more holes and more attacks—then Java follows closely behind in second place. In this respect we have good news:

Oracle, the company behind Java announced it will discontinue the product.

The latest and last version of the plugin will be published in September this year. Major browser manufacturers have stopped supporting the technology plugins because of the problems caused (mainly security). Some have already scheduled to stop using them.

In an unprecedented move, the FBI was able to identify 1,500 people who trafficked child pornography.

Last year, they seized Playpen servers, a page in the Dark Web, published in August 2014 that allowed users to register and upload or download images related to this subject. This site has grown to 225,000 registered users. What the FBI did was go on the website for two weeks, using their own servers and using tools that allow them to identify the IP address they visited, among other things.

While finding a visitor's IP address on a normal web page is something trivial, in the Dark Web it is much more complex. In fact, Playpen visitors were hacked through vulnerabilities existing in some specific browsers for the Dark Web. Once you access the computer visiting the page, the tool captures the same information (IP address, MAC address, version, user name, etc. operating system).

Speaking of hacks done by security forces, in Germany, the Ministry of Interior has authorized the use of trojans to access both computers and smartphones of suspects. The trojan was developed by the police themselves and it gives them access to both communications that occur as files.

Mobiles

As expected, we will talk about vulnerabilities in phones. We have seen vulnerabilities affecting these devices from different angles: software installed by a manufacturer, the device processor, the operating system...

SNAP is the name of a vulnerability affecting LG G3 phones. The problem comes from an error in the notification application called Smart Notice LG, which allows any type of JavaScript to run.

BugSec researchers, who discovered the vulnerability, reported it to LG, which quickly released an update to resolve the issue.

Metaphor is the name of a vulnerability given by the company NorthBit. It's a vulnerability that allows Android terminals to be hacked in only 10 seconds after visiting a Web page containing a malicious media file.

Many techies recognize the name Snapdragon, which is probably the best known Qualcomm processor that is used in more than one billion devices (mainly mobile). Trend Micro colleagues found two vulnerabilities in these processors that allow an attacker to gain root access to the device. Google has released an update that fixes the problem.

Apple has been the protagonist during these past months. First, an open letter was published by CEO Tim Cook regarding customer privacy, after the FBI requested that they provide a back door in order for them to have access to iPhones in case of national security matters. But really, it all started from the terrorist attack in San Bernardino, where the FBI seized an iPhone belonging to one of the terrorists and wanted access to

the messages. Many technology companies supported Cook's letter (Facebook, Google, Microsoft, Twitter, LinkedIn, etc.). In the end, the FBI managed to hack the terminal with the help of a third-party.

Internet of Things

As we have seen in previous reports, the Internet of Things have a high chance of being attacked. Some manufacturers are aware of this problem. General Motors has just launched a new rewards program for hackers who are able to find vulnerabilities in their vehicles. This is normal in technology companies (Microsoft, Google, Facebook, etc. have had programs like this for years) but it is a novelty in traditional companies like automakers. It's great news that General Motors is taking initiative.

The Japanese car manufacturer Nissan has disabled an application that allows owners of Nissan LEAF electric cars to control heating and air conditioning.

An Australian researcher discovered that he could control these functions in any Nissan LEAF simply using the VIN (vehicle identification number).

Gradually, we have introduced new smart appliances in our home. The company Ring has a doorbell with a camera, motion sensor, and Wi-Fi connection built-in. Pen Test Partners Company was studying one of the units and found that, by accessing the device setup button, one could get to the Wi-Fi network log-in information to which it was connected. The manufacturer responded quickly with new firmware which solved the problem.

Cyber-war

Russian investigators from the Industrial Controls Systems Supervisory Control and Data Acquisition (ICS / SCADA), have published a list of industrial equipment that come with the same default passwords in order to force manufacturers to implement better security controls. The list has been dubbed "SCADAPass" and contains the default credentials of more than 100 products from manufacturers such as Allen-Bradley, Schneider Electric, and Siemens.

These products are mostly used in critical facilities. At the end of 2015 there was a cyber-attack in Ukraine to an electrical infrastructure. Specifically, 225,000 customers in a part of Ukraine were without electricity (in midwinter) because of this cyber-attack. This attack has been linked to a group of Russian cyber-criminals known as "Sandworm".

The US Defense Department has introduced a rewards program called “Hack the Pentagon,” where rewards are offered to hackers who find security flaws in web applications and networks belonging to the Pentagon program pages.

Everyone can be a victim of information theft, including terrorist groups like ISIS. A deserter took a USB with data from 22,000 members of ISIS (before joining, the members had to fill out a form with all of their information.)

Three groups of Latin American attackers were able to compromise servers belonging to Bolivian army mail, downloading emails that were later published.
They managed to access information easily through an old security hole in VMWare Zimbra service that the army’s security officials had not patched.

In March, the intelligence agency of South Korea admitted to being victims of an attack in which mobile phones had compromised 40 security agents in the country, accusing North Korea of the attack. Days after, the North Korean government denied they were responsible.

4. CONCLUSION

4 Conclusion

As you can see, this year has been tough so far. We will closely monitor the evolution of ransomware because it looks like it will be with us for a long time. Also, we must be very attentive to the advancing Internet of Things and the multiple security issues surrounding these devices.

I hope that this report has been helpful.
We will continue to report from our blog at
http://www.pandasecurity.com/spain/mediacenter/
and in future reports.

5. ABOUT PANDALABS

5 About PandaLabs

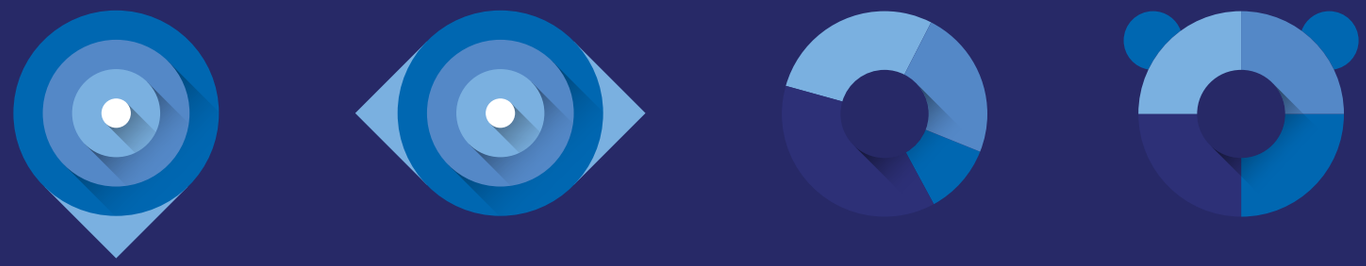
PandaLabs is Panda Security's anti-malware laboratory, and malware treatment center where:

PandaLabs creates real and uninterrupted time necessary to protect Panda Security clients from all types of malicious code countermeasures worldwide.

PandaLabs is 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.



panda

pandalabs