PANDALABS REPORT Q1 2015

January - March 2015

panda

pandalabs

1. INTRODUCTION

1 Introduction

We are at the start of a year that promises to be really exciting in the IT security arena. If you thought that the Internet and everything that surrounds it only affects small, everyday things, think again. An example of this is the historic decision taken by the U.S. government to impose sanctions on North Korea in response to last year's attack against Sony Pictures.

The world of cyber-crime is continually evolving but companies remain the number one target.

Most ransomware attacks that occurred over the last three months were aimed against big corporations. Even some public institutions had to give in to this form of blackmail, paying a ransom to have their computers unlocked.

There continued to be massive data breaches on large enterprises. We learned that the infamous Target breach, which resulted in stolen data on more than 40 million credit cards, will cost the company a staggering $191 million. U.S. company Anthem also fell victim to a hack attack that could cost it approximately $100 million.

Meanwhile, malware creation continued to set new records,

With over 20 million new malware samples put into circulation in the past three months, an average of 225,000 new malicious files every day.

2. THE QUARTER IN NUMBERS

2 The quarter in numbers

The first quarter of 2015 began with a significant increase in malware creation.

The first quarter of 2015 began with a significant increase in malware creation. We finished 2014 with an average of 205,000 new malware strains detected every day, the figure grew to 225,000 over the last three months, reaching a grand total of over 20 million threats put into circulation from January to March 2015.

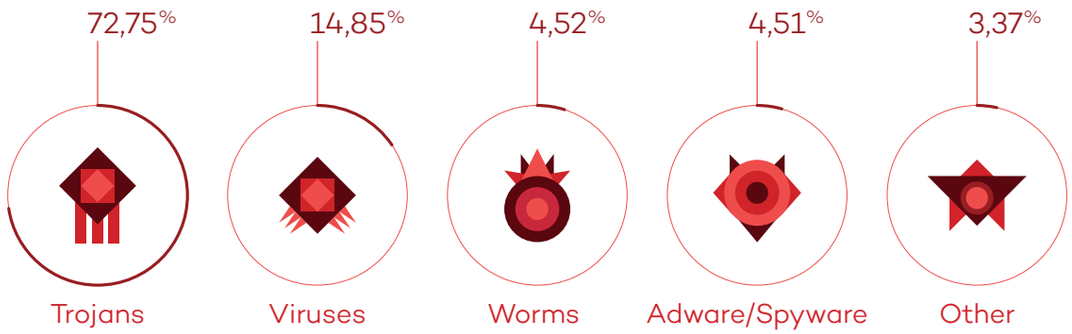
As is usually the case, most of these specimens were variants of known malware conveniently modified by virus writers to evade detection by antivirus laboratories.

Trojans continued to be the most common type of malware.

Accounting for 72.75% of the new malware strains put into circulation, while viruses were a distant second at 14.85%.

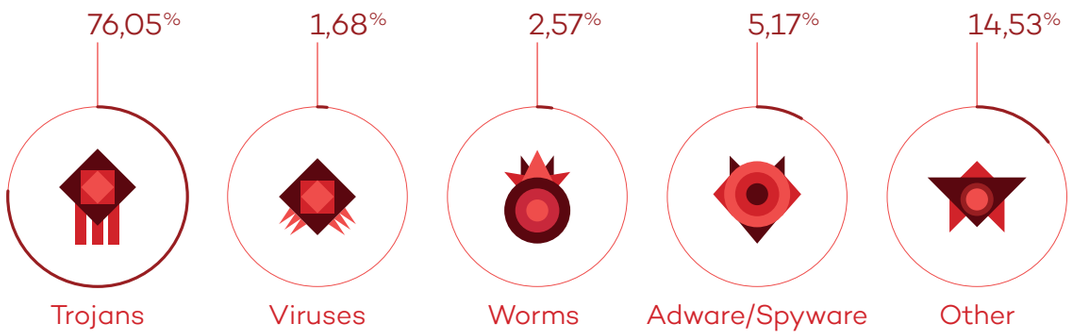
This is a summary of the new malware that appeared during this quarter:

NEW MALWARE CREATED IN Q1 2015, BY TYPE



If we analyze infections around the world, the figures are similar to those for new malware created. However, it should be noted that the infections caused by the malware included in the `Other´ category more than double the percentage of new malware created in the same category:

INFECTIONS BY TYPE OF MALWARE IN Q1 2015

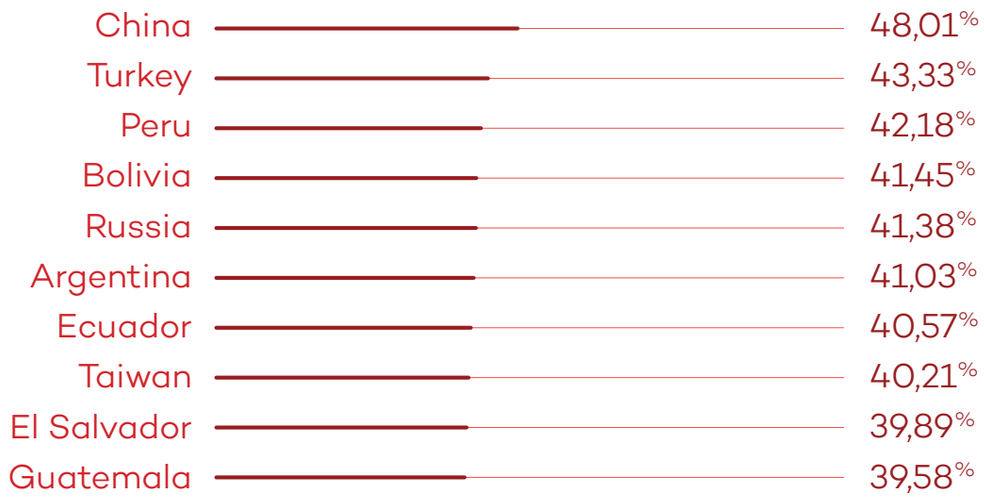


The global infection rate was 36.51%.

This figure indicates the number of Panda-protected computers that came in contact with malware, which does not mean that they were infected. Regarding the data across different countries, China is once again in pole position, with an infection rate of 48.01%, followed by Turkey (43.33%) and Peru (42.18%).

Below we list the 10 countries with the highest infection rates:

COUNTRIES WITH THE HIGHEST INFECTION RATES



It's clear that the highest positions in the ranking are held by Asian and Latin American countries. Other countries with rates above the global average include: Poland (39.48%), Brazil (39.21%), Slovenia (39.05%), Colombia (38.86%), Spain (38.37%), Costa Rica (38.19%), Chile (38.05%), and Italy (37.97%).

In contrast, below is a list of the countries with the least infections:

COUNTRIES WITH THE LOWEST INFECTION RATES

Portugal	27,83%
Belgium	27,39%
Netherlands	26,96%
Germany	26,52%
France	25,87%
UK	25,11%
Switzerland	24,61%
Japan	23,97%
Sweden	22,42%
Norway	22,07%

Europe in general is the area with the lowest infection rates and nine European countries figure in this ranking.

Norway (22.07%), Sweden (22.42%) and Japan (23.97%) are the countries with the least infections worldwide.

Other countries which, although they haven´t made the Top 10, are still below the worldwide average include: Denmark (28.18%), Finland (28.59%), Panama (29.77%), Canada (30.03%), Austria (30.55%), Uruguay (32.15%), Venezuela (33.35%), Australia (33.54%), USA (34.03%), Czech Rep. (35.46%), Mexico (32.31%) and Hungary (35.99%).

This is the heat map according to the infections suffered in the whole world:

It is clear that the warm points of the map are in Asia and South America. Whereas the safest zones are Europe and Japan.

3. THE QUARTER AT A GLANCE

3

The quarter at a glance

In this section we will give you an overview of the most important events that occurred in the cyber-security world during the first quarter of the year.

Cyber-criminals continued their neverending campaign of cyber-attacks with a single purpose in mind: to make money.

An objective that can be achieved through data theft (which explains the emergence of intrusion attacks on companies with the aim of stealing corporate and customer data), or sheer extortion (which explains the rise in ransomware attacks).

Cyber-Crime

If we had to single out the most dangerous cyber-attack of Q1 2015, it would be ransomware, and CryptoLocker in particular.

This type of attack is affecting all types of users, although companies seem to be the preferred target as they store valuable information that they are ready to pay ransom money for. It is a known fact that some companies have finally succumbed to this form of blackmail, especially those that didn't have some type of backup system in place to protect their data.

In February, it was made public that a police department in Illinois had paid a $500 ransom to unlock a computer after it was infected by ransomware.

Cyber-criminals use different types of techniques to infect systems and steal user information. One of the most common infection techniques is the use of exploits, which are programs that take advantage of software vulnerabilities on the victim's computer.

In January, it was revealed that cyber-crooks were actively exploiting a flaw in Flash Player. In this case, the security hole was a zero-day vulnerability, which is a previously unknown flaw for which no patch was available.

Flash is a prime target for cyber-criminals, just like Java, another software that is often compromised by attackers.

When we talk about phishing we often think of email messages purporting to come from banks and financial institutions.

Although it is true that phishing attacks can be started like that and this technique is still used on many occasions, phishers no longer target the customers of banks and online payment services solely.

In January, a hacker group launched a phishing attack impersonating Apple.

The malicious message came from "Apple Support" and used a recurrent tactic: citing a supposed security problem to scare the victim: "Your Apple ID has been suspended."

The message warned the user that an unauthorized person had tried to access their account, and as a result the account had been disabled. The email included a link that took the user to a page that had Apple's look and feel and requested a lot of information: full name, address, phone number, credit card data, etc.

In February, U.S. company Anthem acknowledged being victim to an attack that led to the theft of data from 80 million customers. In this case, the attackers managed to access one of the company's databases using a stolen name and password. It is estimated that the attack could cost Anthem over $100 million.

In March, U.S. company Slack sent a message to all of its users informing them that it had detected unauthorized access to a database storing user profile information. Although no sensitive information was stolen (in fact, Slack informed users that it was not necessary to change their login credentials), the company immediately enabled a two-factor authentication system, encouraging users to use the security feature to improve protection.

Social Networks

In January, at the same time that U.S. President Barack Obama announced a series of measures to combat cyber-crime, a group claiming to be ISIS hacked the Pentagon's social media accounts.

On a different note, we'd like to draw attention to one of today's most common Facebook scams: bogus posts announcing giveaways of gift cards from popular companies.

In January, a group of scammers created a Facebook event promising to give away 430 Zara gift cards valued at $500. To participate in the event, users simply had to join the event, write 'Thank you Zara' on their wall and invite 50 of their contacts to do so as well. The scam spread like wildfire. In just a few hours over 5,000 people had joined the event, and more than 124,000 invites had been sent out.

Mobile Malware

We began the year with a threat that reminded us of old-time email and instant messaging worms, conveniently modernized to make use of SMS messages.

The attack begins when the victim receives an SMS message with a link to a supposed picture of themselves.

The problem with the link is that it actually downloads an APK (Android application package) file. If the victim installs it, the malicious app sends an SMS message just like the one received to all of the victim's contacts.

Cyber-War

For the first time, the United States imposed sanctions on a country in response to a cyber-attack. The country in question was North Korea, and the sanctions were in response to the December hack on Sony Pictures over 'The Interview', a comedy film in which a couple of journalists are instructed by the CIA to assassinate the North Korean leader.

Additionally, new revelations came to light from the documents leaked by Edward Snowden to the press. In January, German magazine Der Spiegel published that China had stolen many terabytes of data relating to the F-35 jet fighter, including radar design information, engine schematics, etc.

4. CONCLUSION

4 Conclusion

The year 2015 has started in full swing in the IT security sector, just as we expected. The number of new malware specimens unleashed during the first quarter of the year reached the astronomical figure of 225,000 every day, and it shows no signs of slowing down.

Targeted attacks on businesses with the aim of blackmailing them with ransomware or directly stealing sensitive information are on the rise, and it is clear that companies must step up their defense. Keeping your IT assets up-to-date and protected with antivirus is no longer enough, and it is necessary to adapt protective measures to the new types of attacks received. Organizations today need to know the security status of their network, and be able to monitor and take control of all applications running on their endpoints.

We'll be back with our quarterly report in three months' time, and meanwhile, you can keep yourself up to date with the latest IT security news at:

http://www.pandasecurity.com/mediacenter/

5. ABOUT PANDALABS

5 About PandaLabs

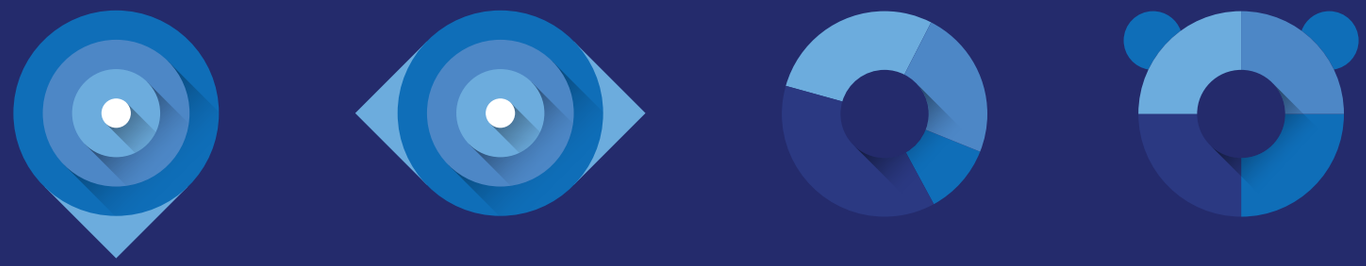
PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

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.



panda

pandalabs