PANDALABS REPORT Q2 2015

April- June 2015

panda

pandalabs

1. INTRODUCTION

1 Introduction

The world of security doesn't give us a moment's rest as the number of new malware types is constantly growing. In the last three months alone 21 million new types of malware have been created.

The cases of ransomware keep on multiplying and every day new attacks are launched with thousands of users and businesses as the unsuspecting targets.

Businesses are constantly under attack and in this report we will tell you about some of the largest attacks that have been carried out during this period; attacks which have affected millions of people and resulted in massive information theft.

In the world of cyber-espionage and cyber-warfare there are all kinds of attacks happening.

We've seen the White House and the German parliament attacked, and other attacks perpetrated by the Islamic State or supporters of the Syrian regime.

2. THE QUARTER IN NUMBERS

2

The quarter in numbers

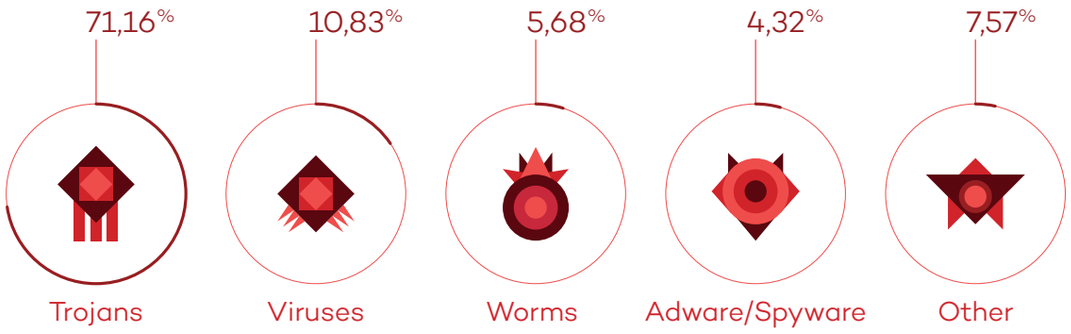
The growth in the creation of new malware continues to grow, and in the second quarter of 2015 we saw an average of 230,000 new types each day and a total of 21 million new threats during those three months.

A large number of the new types of are mainly variants or mutations of previously known malware and cybercriminals are multiplying the types of malware so as to avoid being detected by the antivirus laboratories.

The most common malware are Trojans, which account for 71.16% of all the samples spotted during this period. In second place, by a great distance, are the classic viruses, which accounted for 10.83%.

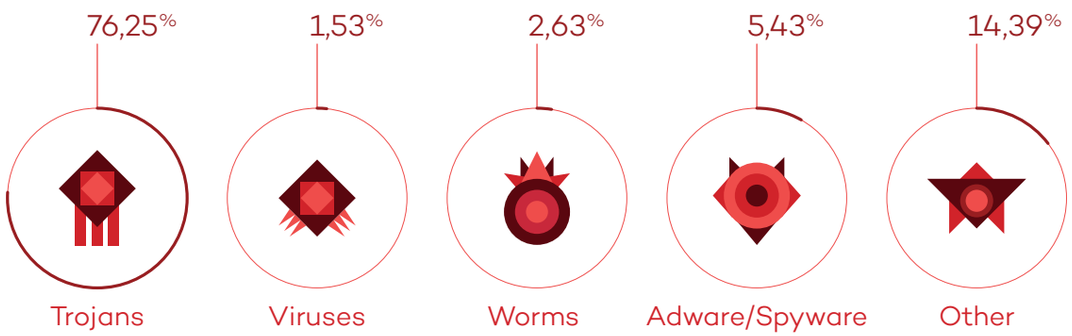
These are the details of the new malware created in the second quarter:

NEW MALWARE CREATED IN Q2 2015, BY TYPE



The category that is labelled others is comprised of different types of threats, with PUPs (Potentially Unwanted Programs) making up the majority. If we analyze the infections that have taken place globally and divide them by the type of malware, we can see that the numbers are similar to those of the newly created malware. The only exception that we see is that there is an increase in the types of others:

INFECTIONS BY TYPE OF MALWARE IN Q2 2015



The rate of infections on a global level was 32.21%.

This data reflects the number of computers that were protected by Panda and that detected a malware, but doesn't mean to say that they were infected. Looking at data from other countries, we see that China, yet again, registered the highest percentage of infections (47.43%). Next in line were Peru (43.11%) and Turkey (41.97%).

Following on, here are the top 10 countries with the highest rates of infection:

COUNTRIES WITH THE HIGHEST INFECTION RATES

As we can see, the countries that are most at risk of infection are located in Asia and Latin America. Other countries with a rate above the global average include: Poland (38.48%), Brazil (38.21%), Slovenia (38.05%), Colombia (37.86%), Spain (36.37%), Costa Rica (35.19%), Chile (34.05%), and Italy (33.97%).

COUNTRIES WITH THE LOWEST INFECTION RATES

Netherlands	27,83%
Portugal	27,39%
Belgium	26,96%
France	26,52%
Germany	25,87%
UK	25,17%
Switzerland	24,41%
Japan	23,57%
Norway	22,22%
Sweden	21,57%

Europe has the lowest rate of infection in the world, with nine countries appearing on this ranking.

SSweden (21.57%), Norway (22.22%), and Japan (23.57%) are the countries with the lowest infection rates worldwide.

Other countries that have achieved a rate of infection lower than the global average, but which fall outside of the top 10, are: Denmark (28.18%), Finland (28.95%), Panama (29.57%), Canada (29.95%), Austria (30.53%), Venezuela (31.15%), Uruguay (31.35%), Australia (31.54%), United States (32.02%), Czech Republic (32.46%), Mexico (32.76%), and Hungary (33.01%).

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

Here we will look over some of the most relevant news that has occurred in the world of security during the second quarter.

Cryptolocker is still roaming freely, causing havoc, especially for companies that are at the mercy of cybercriminals because many of them choose to pay the ransom to retrieve their information.

We will also talk about WhatsApp, the popular instant messaging application that cybercriminals are increasingly using as a way to deceive their victims, the growing number of companies that are being compromised, and the latest news on cyber-espionage.

Cyber-Crime

One of the “new” techniques (brought back from the past, as the first such attacks occurred almost 20 years ago) used by cybercriminals to trick users and infect them with ransomware is the use of macros in Office documents (especially Word).

Most users have a false sense of security that a text document will not contain any threat.

Knowing this, and being aware that the perimeter filters do not act against such files, there has been a sharp increase in the types of attacks by this method.

The weak point of this attack is that the user must enable macros, yet cybercriminals are well aware of this and have successfully developed some ingenious social engineering techniques.

One such example which was discovered by PandaLabs was a Word document containing a blurred image.

At the top of the document in bold capital letters there was a message that indicated that the image was blurred for security reasons. If the user wanted access to the information then they had to enable the macros, with an arrow pointing to the button to be pressed. Once enabled, it showed you the clear image while simultaneously infecting you with a type of Cryptolocker.

Another ransomware which has proven to be popular, especially in Australia, although it had previously been seen in other countries, was one which used images from the popular television series Breaking Bad.

Ryanair, the low-cost airline, was the victim of an attack which saw the company lose $5 million. Despite not revealing the details on how the perpetrators carried out the attack, it is known that it arose from a transfer to a Chinese bank. The company reported the crime and announced that it had managed to freeze the stolen money and was hopeful of recouping it soon.

CareFirst BlueCross BlueShield, a medical insurer, was the victim of a cyberattack in which information was stolen from 1.1 million customers.

With each day the threat of attack from these criminals is growing, and this is merely one example of the hundreds of information thefts happening around the world.

AdultFriendFinder, an online dating service, suffered an attack which saw the theft of private user information. The attackers offered the stolen information to the first one to pay them 70 bitcoins, equivalent to $17,000 at the time. Not long after, the complete database was published online.

LastPass, a leading password management company, was another victim of information theft. Luckily it seems that the attackers didn't get sensitive password information, but only the hashes of the users' master passwords.

The complexity of these hashes (jumbled up and hard to understand) makes it very difficult for attackers to get the real password. Despite this, it is recommended to change the password if the one you are using is a weak one.

The Hard Rock Hotel and Casino in Las Vegas made it known that their security had been compromised during an eight month period in which the attackers were able to steal client information such as names, credit and debit card numbers, and the CVV of the cards. Those affected were the clients who used their cards in the complex's restaurants, bars, and shops, but did not affect those who made purchases in the hotel or the casino.

This attack is reminiscent of others that we have seen in the past (Target, Home Depot, UPS, Neiman Marcus) where the sales point terminals were targeted with the aim of stealing the clients' credit card information.

There were rumors that Uber had been a victim of an attack after detecting that users of the service had witnessed unusual activity in their accounts. However, it appears that this was a case of phishing, whereby the users provided their ID to the attackers after being tricked.

At the end of June, 1,400 passengers of the Polish airline LOT were stranded in Warsaw Chopin Airport after an attack on the ground system that was used to make the flight plans.

Social Networks

All user connections to the servers of Facebook, including messages sent and received, are transmitted via secure HTTPS protocol. If this wasn't enough, the social media giant established a service on the Tor network so that users can be further assured of their online privacy. However, apart from the connections established by users via its own service, there are other indirect forms of communication carried out on Facebook by mail. They are the notifications that you receive when a friend sends you a private message (unless you have deactivated the feature).

Due to the security of these messages being at risk, Facebook has announced that from now on, all users will receive them – if they choose – protected by the popular encoding software Pretty Good Privacy (PGP).

PGP hides the mails from potential intruders with a system based on a public key (which the message sender must have) and a private key (which only the receiver must have).

The configuration process is easy – access your profile, enter into the part named "Information" and go to "Contact and Basic Information", where you will be able to enter your public PGP key (if you don't know what it is or how to get it, you can read the tutorial). It will then be visible on your profile, available for anyone who wants to send you a coded mail.

Underneath the chart there is a box that you will have to tick if you want all of the mails that Facebook sends you to be included in this new security measure. It is important to remember the key that you use to protect your mail with PGP. If you forget it, you won't be able to read your notifications and you may even lose access to your account on the social network.

WhatsApp is a popular way to attract and try to infect users. We have discovered a hoax, in which they try to trick users of the instant messaging application, called WhatsApp Trendy Blue.

It passes itself off as a "new version" of the application with extra features when, in reality, the only thing it does is sign the user up to an expensive billing service.

This fraudulent program also asks you to invite at least 10 of your contacts to sign up for its services.

Mobile Malware

Fujitsu, in collaboration with the Japanese operator NTT Docomo, has launched Arrows NX F-04G, which is based on Android and is the first Android mobile to include an iris scanner as part of its security features. This is a measure that is a lot more secure than the fingerprint method that is popular with its rivals such as Apple's iPhone 6 or Samsung's Galaxy S6.

In June we detected a phishing campaign that was directed at Android developers who published their creations on Google Play, the official app store of the operating system. The message was sent from an entity named "Play Developer Support" and was titled "Update Your Account Information". Once the link was clicked, you were directed to a webpage that looks like Google, where they would ask you for your details.

Phishing attacks are designed to steal the user's identity and personal details, this is why attacks aimed at financial entities and any type of payment platform are so popular.

This case, however, is different because they weren't looking to empty the victim's bank account, but rather use their details to spread malware via the Google Play store.

The most worrying aspect of all this is how easy it would be for the criminals to automate the whole process. All they need to do is the following:

- Create a spider or crawler (there are various open source projects available to help them with this) in order to download information in all of the apps published on Google Play.
- Analyze the information to get the email addresses of the different developers.
- Send a customized phishing campaign in which even the webpage is tailored to the developer. This makes the trick seem even more plausible and helps achieve a better "conversion rate".
- Because the attacker has information on all the apps

published by each developer, it is possible to create a system that alerts him every time a publisher with a popular app (millions of downloads) falls for the trap.

With this in mind, one of the easiest and least sophisticated attacks would be the publishing of apps from that account. Imagine if someone managed to steal the details of one of the developers of Candy Crush and published Candy Crush 2 from the same account – if the attackers were cleverer and found a way to modify the application without using the private key (which can't be obtained with stolen ID information), they could publish and update any application they desire.

In the previous example, imagine that the attackers created an updated version of Candy Crush that contained a Trojan – millions of people would download and install it without realizing that they are being endangered.

Google has created a new program called Android Security Awards that will compensate those who investigate and discover new weaknesses in Android's security.

The amount paid depends on the seriousness of the security weakness with a sum of $2,000 for a critical weakness, $1,000 for a high-level weakness, and $500 for a moderate-level weakness. That said, depending on the seriousness of the problem and the details of the finding, that figure could reach as much as $38,000.

Cyber-War

Ben Rhodes, Assistant to the President of the United States and Deputy National Security Advisor for Strategic Communications and Speechwriting, stated that the White House had fallen victim to an IT attack.

In an interview with CNN, Rhodes confirmed that the attackers obtained unauthorized access to an unclassified system of computers and stole highly important information, even though the classified system wasn't hacked. Despite not wanting to reveal whether the attack was perpetrated by Russian hackers nor when it occurred, Rhodes did give the impression that the attack hadn't taken place during the previous days. Without giving much more information, he stated that they had already taken "a series of security measures to evaluate and minimalize the damage caused".

In June we found out that the Office of Personnel Management (OPM), the human resources agency for the federal government of the United States, had been attacked and that confidential information relating to at least four million public sector workers had been stolen.

This attack took place two months before then, at approximately the same time as the attack on the White House. However, it appears that the attacks weren't connected, given that the former appears to be linked to Chinese hackers, although the US government hasn't officially confirmed this.

ISIS sympathizers attacked the French television station TV5MONDE, managing to sabotage its transmission. On top of that, they also took over its Facebook page and website.

The well-known group Syrian Electronic Army managed to infiltrate the website of the US Navy, publishing propaganda promoting Bashar Al-Assad and his regime in Syria.

The German parliament was the victim of an attack in which they managed to infiltrate and steal information from various computers. It is believed that the attack came from Russia, but it is difficult to prove exactly who was behind it.

We already know that the NSA used a modified version of Stuxnet to try and sabotage a nuclear program by North Korea. Although on that occasion they weren't successful, it must be noted that with Stuxnet they managed to destroy at least one thousand centrifuges of uranium in a plant in Natanz, Iran, a few years ago.

4. CONCLUSION

4 Conclusion

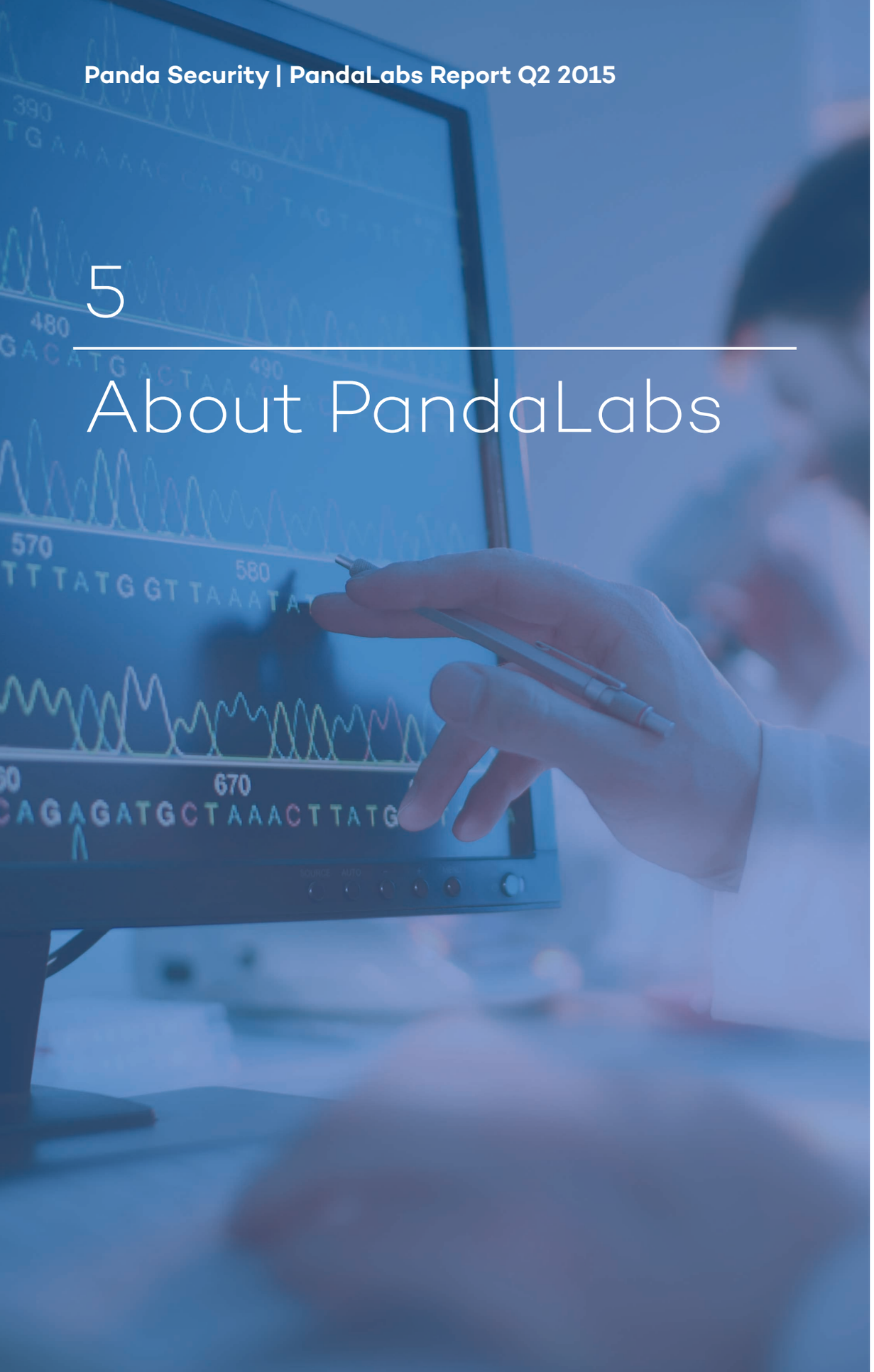
Attacks have become commonplace and, more than ever, businesses need to be prepared for this massive avalanche of information theft. They need to reinforce their systems and security solutions, and understand that a simple antivirus is no longer enough to safely protect themselves from an attack. Now is the time to adopt advanced defenses that block and detect any type of intrusion, and that gather forensic information on any type of attack on their workstations and servers.

The economic costs associated with these attacks is steadily increasing and in the coming months / years we will see a change in the mindset of businesses in respect to security; something which the most savvy among them are already implementing.

We will be back with our next report within the next three months, until then you can keep yourself up to date with the latest news at

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

5. ABOUT PANDALABS



5 About PandaLabs

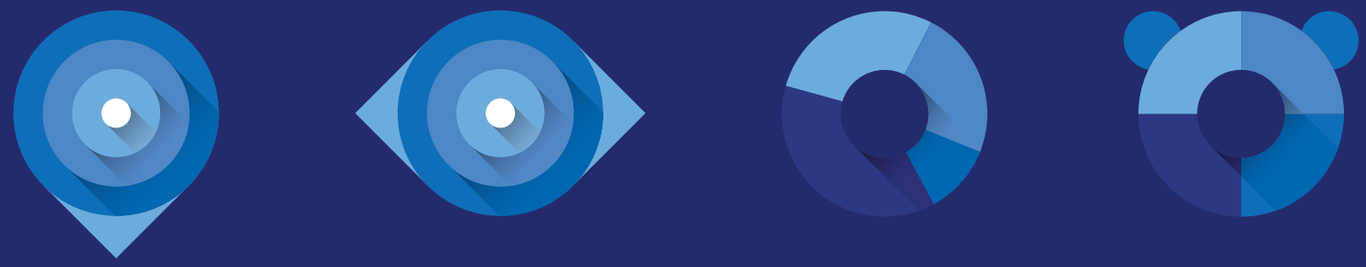
PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

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