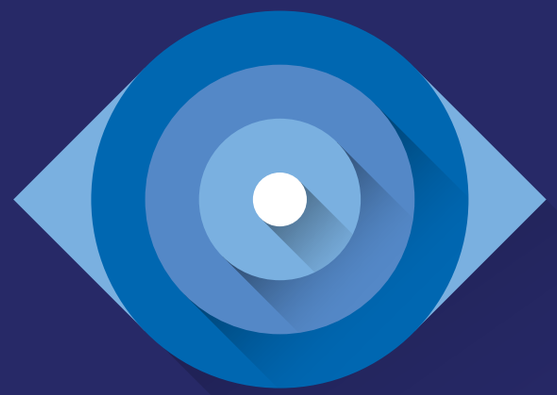
PANDALABS REPORT
Q3 2015



panda

pandalabs

1. INTRODUCTION

1 Introduction

The final few months of 2015 aren't seeing a let-up in the appearance of new malware, and the 21 million types of malware that were spotted during the third quarter of this year is a testament to that. During these months we've seen multiple cases of businesses being compromised, with the most famous cases being those of Ashley Madison and the Hacking Team.

The growing tension in the world of cyberwar and cyberespionage has come to light following the differing accusations made by large powers, such as the United States, Russia, and China.

On the other hand, we have to highlight the multiple security problems that we have seen this quarter in mobile devices, both in Android and iOS.

What's more, the Internet of Things is fast becoming a new vector of attack.

During the months of July, August, and September we have highlighted the vulnerabilities that have been found in different vehicles, one of which allowed for said vehicle to be remotely controlled.

2. THE QUARTER IN NUMBERS

2

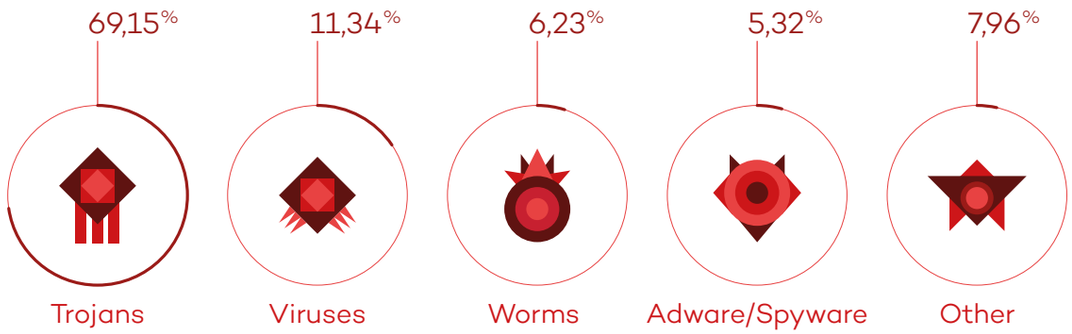
The quarter in numbers

During the summer months it is common to see a drop in the number of malware samples created, but this year has been an exception. We saw 21 million new threats, which resulted in an average of 230,000 per day.

Trojans are the most common type of malware, accounting for 69.15% of all samples that were registered during this period. In second place – by some distance – are the classic viruses, which account for 11.34%.

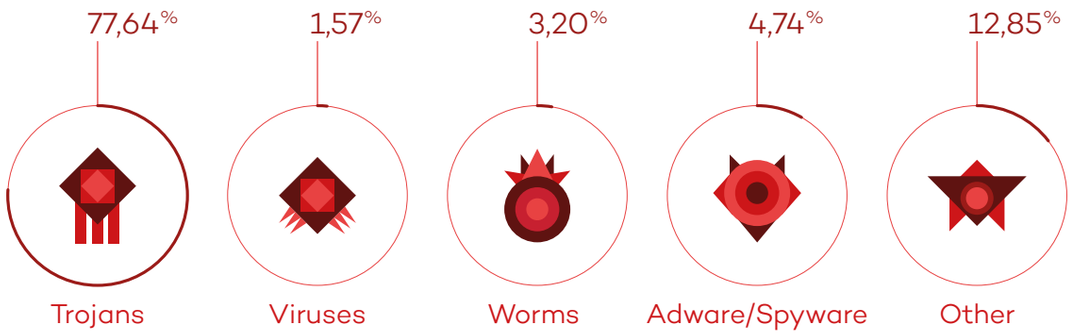
These are the details of malware created this quarter:

NEW MALWARE CREATED
IN THE THIRD QUARTER OF 2015, BY TYPE



The "Other" category is made up of different types of possible threats, the most common of which are the PUPs (Potentially Unwanted Programs). If we analyze the infections that have taken place in the world by malware type, we see that the figures are similar to those of new malware types created, except in the category of "Other", whose percentage is higher in this respect:

INFECTIONS BY TYPE OF MALWARE
IN THE THIRD QUARTER OF 2015



The rate of infection worldwide was 32.12%.

This reflects the number of computers that were protected by Panda Security and which encountered malware, but doesn't not mean to say that there were infected as a result. As regards to figures for specific countries, China, once again, is at the top of the list with an infection rate of 45.35%. Next in line are Peru (42.89%) and Turkey (40.99%), respectively.

Below are the 10 countries with the highest infection rates:

COUNTRIES WITH THE HIGHEST INFECTION RATES

China	45,35%
Turkey	42,89%
Peru	40,99%
Russia	38,32%
Taiwan	37,82%
Bolivia	37,13%
Guatemala	36,75%
El Salvador	35,32%
Ecuador	35,02%
Argentina	34,78%

As we can see, the list is mainly composed of countries in Asia and Latin America. Other countries that have a rate that is higher than the global average include Poland (34.54%), Slovenia (33.98%), Colombia (33.11%), Spain (32.50%), Costa Rica (32.33%), Chile (32.19%), and Italy (32.15%).

Below are the countries with the lowest infection rates:

COUNTRIES WITH THE LOWEST INFECTION RATES

Portugal	26,38%
Netherlands	26,22%
Belgium	25,96%
France	25,02%
Germany	24,87%
UK	24,17%
Switzerland	22,75%
Japan	23,57%
Sweden	21,33%
Norway	20,12%

Europe has the lowest rate of infection worldwide, with nine countries in this list.

Norway (20.12%), Sweden (21.33%), and Japan (22.75%) have the lowest rates in infection globally.

Other countries that have a lower than average infection rate include Denmark (26.50%), Finland (26.78%), Panama (27.01%), Canada (27.42%), Austria (28.53%), Venezuela (29.25%), Uruguay (29.54%), Australia (29.92%), United States (30.13%), Czech Republic (30.46%), Mexico (31.76%), and Hungary (32.02%).

3. THE QUARTER AT A GLANCE

3

The quarter at a glance

Cybercrime

One of the biggest attacks that took place in this period was, without a doubt, the one which affected Ashley Madison. The attackers, known as Impact Team, displayed a message on their website demanding the closure of the dating agency or they would publish all of the information that they had stolen. Not long after they published a torrent with 10GB of information as the Canadian company failed to give in to their demands.

Among the information that was released were the private details of 37 million customers, completed transactions, email address, sexual preferences, etc. Furthermore, the release also included internal documents relating to the business.

This quarter has also seen a whole host of new vulnerabilities used by cybercriminals as a means to access their victims.

Apart from the typical Flash or Java attacks, the Apple Mac OS X operating system has also seen a couple of incidents.

The first of these, which was discovered by Stefan Esser, allowed for access to the root and saw Adware being used to attack Macs.

The second vulnerability was discovered by investigators at MyK. It consisted of a vulnerability in the password administration system that allowed the attacker to obtain all of the stored information.

One of the methods of attack that is quickly becoming popular consists of intercepting routers, both in homes and businesses. By doing this, the routers remain under the attacker's control. It was brought to light that routers in businesses such as ASUS, DIGICOM, Observa Telecom, PLDT, and ZTE had predefined information in their access codes. This allows attackers to take control of them without needing to enter the premises, and we have seen examples of this where the attackers used a DDoS against Xbox Live and PSN last Christmas.

Adobe Flash, known for its numerous security issues, is facing its demise soon.

iOS didn't allow for it to be run on its operating system and Android followed suit. Now it's the turn of Google to put the final nail in its coffin, by banning it from its Chrome browser. Amazon has also announced that it is banning any advertisement that is based on this format from its website.

The FBI has detained 5 individuals that were involved in the hacking that JPMorgan suffered in 2014.

In this attack that managed to get the credentials of an employee, and later used these to access 90 of the company's servers to steal information belonging to 76 million individuals and 7 million businesses, all of which were clients of the company.

Microsoft has decided to improve the security of its products and solutions by doubling the reward available to investigators that are able to discover critical new errors in its solutions. The amount has increased from $50,000 to $100,000.

Although this is becoming a common feature in IT companies, it hasn't yet filtered down to all sectors, although more and more businesses are offering incentives to their investigators

in the hope that they will be informed first, as opposed to them selling the information to an outside source. In the case of United Airlines, which offers air miles as a reward, they have decided to offer up to one million air miles to their investigators who discover and inform them of errors.

The FBI also offers incentives, although in this case they are aimed at those who offer information on the suspected criminals. The highest reward offered is three million dollars for anyone who can help capture Evgeniy Mikhailovich Bogachev, the mastermind behind the network of Gameover ZeuS bots.

Social media

Facebook announced that it was looking into adding a "Dislike" button to its website, and as expected, cybercriminals jumped on this opportunity.

A few hours after the announcement different types of false links appeared offering the "Dislike" feature which were actually just traps looking to trick users into giving away private information.

Mobiles

In July, Zimperium recognized a massive vulnerability for Android that affected 950 million devices that used the operating system.

The problem wasn't just the amount of mobiles, tablets, or other devices that were affected, but rather how easy it was to remotely endanger them. By just sending a malicious MMS it is possible to take control of any telephone just by knowing the victim's number. It isn't even necessary to open the MMS, as Android automatically processes images, meaning that receiving the MMS was enough to cause the damage.

Although the problem has since been corrected, the large number of manufacturers and versions of the operating system means that there could still be some versions out there that haven't been updated with the latest safety measures.

Google has since made a large number of the manufacturers (Sony, LG, Motorola, etc.) include the latest updates and Samsung announced that they would offer monthly updated to their customers to keep ahead of new vulnerabilities that keep on appearing.

In fact, not long after, two investigators from IBM's XForce published another security problem that allowed an attacker to replace a legitimate application with a malicious one, which would then allow the attacker access to permission controls for the replaced app. Google has since updated its software to take care of this security problem.

We are now used to seeing ransomware attacks on PCs and it is becoming more common to see them taking place on Android, too. In fact, during the previous three months these attacks have been marked out for their originality and simplicity.

What a malicious app does is change the PIN of the device and demand a ransom of 500 dollars.

For example, the users of our antivirus for Android can change the PIN code of their mobile from their web control panel, thus rendering this type of attack ineffective and saving themselves 500 dollars.

Apple's operating system has also suffered various attacks during these months.

The company Appthority has discovered a vulnerability called Quicksand that affects corporations that use MDM (Mobile Device Management) services and could put confidential information relating to the company at risk. Apple has taken care of this vulnerability with its new version of iOS 8.4.1.

Another vulnerability that has been taken care of is Ims0mnia, which allowed a malicious app to avoid the running restrictions of Apple, permitting the activation of the microphone or camera and allowing the user to be spied on.

Apple had to remove a number of applications from its Apple Store owing to an attack known as XcodeGhost. The attackers published a modified version of the software that developed apps for iOS, which led to app creators using it to include malicious features in their apps without knowing.

Another attack targeted at Apple users managed to get off with iCloud credentials of more than 225,000 users. The attack affected users who had previously jailbroken their device so as to install apps without using the official App Store, but which resulted in the security controls installed on iOS being deleted.

Internet of Things

In July, HP Fortify published the results of a study on smartwatches which found that 100% of the devices analyzed were vulnerable to attack and shed light on the main problems that smartwatches face.

For example, none of the smartwatches offered a double authentication when linked to a mobile device and allowed for incorrect passwords to be entered repeatedly.

Security investigators Charlie Miller and Chris Valasek carried out a demonstration in July which left the world in shock.

They convinced Andy Greenberg, a journalist at Wired, to drive a Jeep Cherokee while the two of them hacked the car from their homes.

The attack started off with them taking control of things such as the air conditioning in the car, activating windscreen wipers, changing the radio station, and playing around with the volume... and ended with them taking complete control of the car, including its braking system.

The spent months working on these attacks and even informed the manufacturer before the test, hoping that they would install new security updates to cover this vulnerability. The pair gave more information on how they carried out the tests in an interview that they gave at the BlackHat conference in August.

Land Rover was also informed in July of a fault in software that affected 65,000 vehicles that had been on sale since 2013. The fault allowed for the unlocking of the doors by outside sources.

Kevin Mahaffey and Marc Rogers, two investigators, showed how to hack a Tesla Model S. as the BlackHat conference. Despite needing physical access to the car to carry out this attack, they discovered 6 new vulnerabilities that allowed them to stop the engine when it was travelling at slow speeds. The manufacturer has since taken action to cover up this problem.

Cyberwar

Hacking Team is a business known for providing cyberespionage and cyberattack tools to a multitude of governments worldwide.

In July it suffered a massive hack which saw the theft of all types of data. The attack was made known via the Hacking Team's Twitter account, which was also taken over by the attacker who changed the name of the account to Hacked Team and attached a link to download all of the stolen information.

They made public lists of clients (police and intelligence agencies of various countries, from the United States to Uzbekistan). They also made public a corporate certificate used by Hacking Team, passwords they were used on their most protected systems, lists of products that they sold, source codes for their applications, financial data, etc. They even published a website with a search function that allowed for all of the email addresses stored by Hacking Team to be searched through.

A few days later a Zero-Day was discovered on Adobe Flash thanks to the information stolen from Hacking Team.

James Comey, the director of the FBI, spoke at a security forum and told of how they had detected a growth in interest on behalf of terrorists in strategies for launching cyberterrorist attacks against the United States. He didn't specify the types of attacks and said that they still appeared to be in the planning stages and that the terrorists were still looking into how effective they could be.

On July 25, Russian hackers managed to access a non-classified email system pertaining to the Pentagon. Official sources have stated that it was a sophisticated attack and that they were sure there was a government entity behind it.

In September, investigators at DGI published a study on the 78020 unit of the Chinese army, where they showed that it was behind a group known as Naikon, which was responsible for different military, economic and diplomatic cyberespionage attacks in the area. Its victims included Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, Vietnam, The United Nations Development Program, and the Association of Southeast Asian Nations.

4. CONCLUSION

4 Conclusion

2015 is drawing to a close and we can confirm that we are achieving the predictions that we made a year ago. For the first time we have included a section in the report where we highlight security problems for IoT devices, with smartwatches and smart cars as the protagonists.

Information theft for businesses is continuing to happen and we can only focus on the most important cases. Businesses should be prepared and ready to protect themselves against attacks that they are being subjected to.

We'll be back with our next report in three months, until then you can keep up to date with the latest news at

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

5. ABOUT PANDALABS

5 About PandaLabs

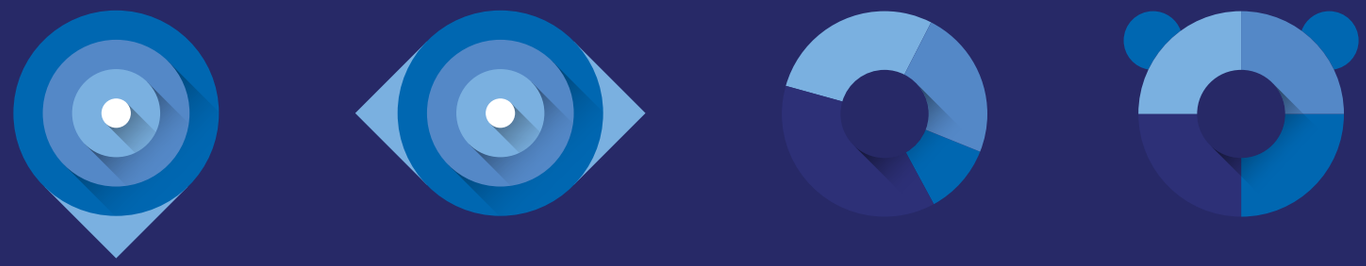
PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

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