
PANDALABS REPORT

Q3 2016



1. Introduction

2. The quarter
at a glance

Ransomware

Cybercrime

Mobile Malware

IoT

Cyberwar

3. Conclusion

4. About PandaLabs

1. INTRODUCTION

1

Introduction

Cybercrime isn't slowing down anytime soon. This quarter, cybercriminals were increasingly more ingenious, using innovative technologies and new tools to spread their wares. PandaLabs, Panda Security's anti-malware laboratory, captured more than 18 million new malware samples this quarter alone, an average of 200,000 each day, proving that the alarming cybercrime problems from last quarter continued into Q3.

Trojans are in the lead as the most popular malware this quarter, with ransomware making up the majority.

Ransomware attacks have grown immensely this quarter and have cybercriminals are raking in millions of dollars.

Point of Sale terminals are becoming increasingly more desirable for cybercriminals who are targeting PoS terminals at hotels, restaurants and other establishments.

The information we've gathered from tracking malware behavior and new malware creation in the last three months shows **a number of massive DDoS (Distributed Denial of Service)** attacks that are taking place and, in many cases, are linked to a botnet whose members are not computers but smart devices such as IP cameras.

We will be going into depth about the latest attacks aimed at the Internet of Things (IoT), such as the hacks that **have affected connected cars** like reputable Jeep and Tesla models. Recently, one of the Tesla models became the victim of an investigation that demonstrated how it could be controlled remotely without physical contact.

In the mobile phone environment we will analyze different situations that involve attacks on Android devices and we will see how a wave of ransomware attacks are targeting iOS based devices.

2. THE QUARTER AT A GLANCE

2

The quarter at a glance

Ransomware

Ransomware is a business that promises high profits for its criminals. As this area matures and becomes more sophisticated, the higher the rewards will be. In July, the creators of the Petya and Mischa ransomware began developing malware and corresponding payment platforms, while they left distribution to third-parties. This is a new model known as **Ransomware as a Service (RaaS)**.

With RaaS, the developers create the ransomware while distributors are in charge of infecting the victims. As with distribution in the legitimate world, they can receive better margins on a large volume of activity. The more victims that are infected and ransoms that are paid, the bigger the paycheck for distributors. Their earnings usually start at 25%, but a distributor can potentially make up to 85% if they are able to **extort more than 125 bitcoins** (about \$75,000 US) per week.

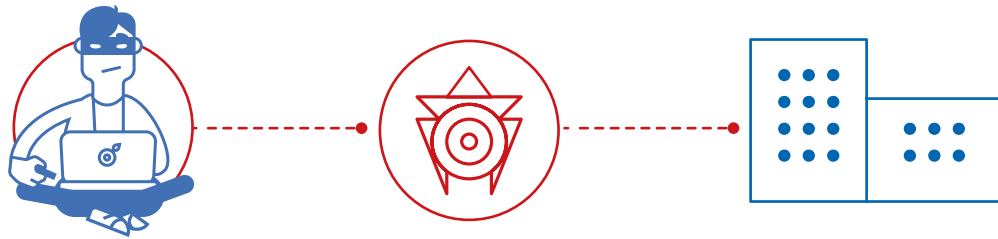
At PandaLabs, we are closely tracking the evolution of ransomware. Bi-monthly we publish a series of articles on the Panda Security Media Center, titled “Tales from Ransomwhere”, where we share the latest developments related to these attacks. We have analyzed how attackers use and abuse PowerShell, a program that comes by default with Windows 10, in order to launch ransomware attacks without the need to download files from the internet or from Word document with macros sent through emails. These attacks end up being a living nightmare for computer security businesses that primarily offer perimeter defense, especially since the ransomware is never present on the computer.

We have seen very clear examples of this with the Locky family, which implements an “offline” mode that allows it to

encrypt files when protection solutions may prevent it from communicating with the server that supplies the encryption password.

In addition to the traditional infection techniques via exploits and spam, there are some other extremely effective techniques, specifically directed at businesses.

We saw this in September when a group of attackers successfully installed the Crysis ransomware on a French company's server.



After investigating what happened, it was discovered that the server had the Remote Desktop Protocol service connected to the Internet. The attackers were trying to enter the server using a brute-force attack over the course of four months. After more than 100,000 attempts, they were finally able to discover the credentials.

Cybercrime

Measuring cybercrime is very complex. Cybersecurity professionals who combat these threats on a daily basis understand its mass and know that it is an industry that continues to grow and evolve.

But is it really that dangerous?

Some people may think that large security companies, like Panda, are particularly interested in the growth of cybercrime because these problems benefit our business. However, the data speaks for itself. More and more independent bodies provide statistics that help us form an idea of the current cybercrime situation.

The National Crime Agency of the United Kingdom published a report showing that cybercrime is currently involved in more than 50% of the crimes committed in the UK.

One of the largest bitcoin robberies in history occurred on August 2nd. The equivalent of 60 million dollars in bitcoins was stolen from Bitfinex, a trading and crypto-currency exchange company. This money belonged to clients who deposited bitcoins at this “bank”. There is still no evidence of who carried out this attack and Bitfinex has not given any information on how this attack might have occurred. Enforcement agencies are currently conducting an investigation.

In September, the famous cybersecurity journalist Brian Krebs uncovered vDOS, a “business” that offers DDoS attack

services. Shortly after his discovery, the vDOS attackers were arrested (they were able to launch 150,000 attacks and make a profit of \$618,000 in two years). Not long after their arrest, Krebs' site received a massive DDOS attack which led him to abandon his website for a week. In the end, Google stepped in and protected his website through Project Shield and it began working again. Krebs went into detail about the possible consequences of these attacks in his article that is published as The Democratization of Censorship.



Blizzard's Battle.net servers were attacked by a group called PoodleCorp that compromised three games (World of Warcraft, Overwatch, Diablo 3). Throughout this quarter there have been a lot of similar attacks. We will go further into detail in the IoT subsection since a large part of them were launched using botnets composed of smart devices like IP cameras, routers, etc.

During the last three months there were many data thefts that affected millions of users worldwide. In July, the Ubuntu forums, where users discuss all aspect of the open-source operating system based on GNU/Linux, was hacked and the email addresses, usernames and IP addresses, belonging to two million people were stolen. Black Hats also had their eyes set on forums linked to the popular mobile game, **Clash of Kings**, seeing as they could compromise it the same way. On this occasion, the **attackers made off with personal data belonging to 1.6 million users.**

Users of the Valve game, Dota 2, were also victims of an attack this quarter. Their forum was hacked and private information was stolen, such as credentials and email addresses pertaining to 1.9 million of their users. The same attackers stole 9 million steam game codes after compromising the DLH.net website.



Cybercriminals struck gold when they started compromising game sites.

Let's add to this list: data was stolen from 200,000 GTAGaming.com users, and www.minecraftworldmap.com was attacked and the attacker published information pertaining to 71,000 users.

Another controversial attack targeted the **pornographic website Brazzers**, who suffered a security breach where **800,000 users' data** was stolen. Yet another standout attack was suffered by the instant messaging service QIP.ru and data belonging to 33 million users was stolen.

Not even Dropbox is able to escape the grips of cybercrime. The well-known file sharing service recently discovered that they suffered a cyberattack in 2012. The result: a loss of user data pertaining to 68 million users. But if there is one robbery we cannot forget, it's the one **Yahoo** suffered. Although it actually happened in 2014, it was not known about until now. A total of **500 million accounts were compromised, making it the biggest theft of its kind in history.**



Point of Sale (POS) terminals are another area cybercriminals are focusing today.

PandaLabs discovered an attack in which **200 American establishments** were compromised, most of them restaurants, and credit and debit card data was stolen using the **PunkeyPOS malware**.



The popular Wendy's fast food chain fell victim to a similar attack where PoS terminals were infected by another variant of PunkeyPOS across more than 1,000 establishments.

Our laboratory discovered another similar attack. Once again the victims were American restaurants, but in this case, **300 POS terminals** were infected with the **PosCardStealer malware**.

H **Another critical area that we have reviewed in a previous PandaLabs reports is the hotel industry.**

In this quarter, a number of the HEI Hotels were attacked and the crooks used malware to steal credit card data from the hotels' POS terminals. Amongst the affected hotels were the Sheraton, Westin, Hyatt and Marriot establishments.

But cybercriminals have their eyes set on something more ambitious than Point of Sale terminals. In July, dozens of First Bank ATMs in Taiwan were cleaned out. This crime was done in an organized fashion. The attackers waited next to each ATM, while they withdrew a total of 2 million dollars. We know that the assailants installed malware on these ATMs (surely after compromising the internal bank network) and then they extracted the money without physically touching the ATMS by using remote commands, as demonstrated by the security footage.



A successful attack on a financial entity can have a juicy reward—millions of dollars.

In August, SWIFT released a statement that revealed that many attacks similar to the Bangladesh one are taking place. They did not include exact amount stolen and number of attacked banks in their statement. What is mentioned, however, is that these financial entities did not have adequate security measures in place.



Rewards programs for those who find vulnerabilities.

The tech giant **Apple** is one of the latest businesses to start a rewards program. They are offering up to **\$200,000** to researchers who are able to find vulnerabilities in Apple products. What is surprising is that they did not have this type of program in place when other tech giants have had similar programs for years.

Interestingly, there are many types of organizations that have these rewards programs. Although they normally offer cash prizes, there are some companies that prefer payment in kind, like **United Airlines**. It was revealed this August that the company awarded a security researcher with a million miles from their fidelity program for discovering 20 security holes in their software. White hat hackers at Offensi.com were also rewarded with **1,000,000 air miles**, which they generously donated to three charities.

This July, five members belonging to a money laundering gang were arrested in London. Amongst the five Russians were the gang's leaders, 30-year-old Aslan Abazov and 29-year-old Aslan Gergov. Abazov was sentenced to 7.5 years in prison and Aslan received to 7 years and 3 months.

Edward Majerczyk pleaded guilty for stealing celebrity photographs, then reached a settlement condemning him to 9 months in prison (initially, the prosecutor requested 5 years). Majerczyk admitted that he gained access the victims' iCloud accounts after launching a phishing attack to get their log-in credentials.

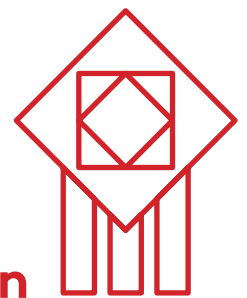
For some, hacking those people who are in the public eye is seen as an accomplishment. This is the case of Marcel Lehel Lazar, a 44-year-old Romanian, who was sentenced to 52 months in prison for hacking several influential people. Some notables from his 100 victims include Hillary Clinton, George Bush (father and son), Colin Powell, Nicole Kidman, and Robert Redford.

Mobile Phones

Android devices are in the line of fire. People continue to purchase Smartphones, and cybercriminals continue to target them. Since the Android operating system has the greatest market share and it allows users to install programs from outside of the official store, it makes it an easier target for criminals, but fortunately, Google is reinforcing security. Different defense measures (that stem from the latest versions of Linux kernel) will be activated in Nougat, Android's 7th version.

However secure, on many occasions these protection measures are not always enough. The security company **Checkpoint discovered four security problems that could potentially compromise 900 models of Android devices powered by Qualcomm Snapdragon processors.**

Gugi, an Android Trojan, is able to jump over the Android 6 security barriers; this means it can steal bank credentials and information from other applications installed on these devices.



How can it do this? When users are using a legitimate application, Gugi superimposes another screen and asks for information that will be directly sent to the cybercriminals without their victims' knowledge.

Lately, the ransomware attacks on iPhones and iPads are increasing. But in contrast to their Windows counterparts, the cybercriminal did not use malware for these attacks. Instead, they used wit to get ahead. To carry out the attack, they used the AppleID of the victim and their password (which he probably obtained through phishing or by reusing passwords from different web sites) and then activated the Lost mode from the “Find my iPhone” application and added a message that asked for a rescue payment in bitcoins instead of giving the password required to unlock it.

In August, Apple urgently published the iOS version 9.3.5 for its mobile device operating system. This version fixes three 0-Day vulnerabilities that are used by the spyware software known as Pegasus. Pegasus was developed by the NSO Group, an Israeli business that offers products similar to those offered by Hacking Team.

IoT

During the DefCon conference that occurs in August in Las Vegas, investigator Andrew Tierny showed a proof of concept where he demonstrated how to hijack a thermostat that he had modified himself. After taking control of the thermostat (inserting an SD card in it), the temperature rose to 99 degrees Fahrenheit that could only be deactivated with a PIN number. The thermostat connected to an IRC channel, gave up the identifying MAC addresses for each compromised device, requested a bitcoin to obtain the PIN—and all of this changes every 30 seconds. Although it was only a proof of concept and physical access to the device was needed, we can get an idea that the attacks we will face in the coming years directly amount to the household appliances connected in our homes.

There’s no need to wait because there are millions of devices in the Internet of things that are already being compromised. The botnet LizardStressed, created by the group Lizard Squad, launched a devastating DDoS attack against Playstation and Xbox services back in the day, and was mainly composed of these types of devices.

According to Arbor Networks, the majority of these devices are IP cameras and they can be compromised simply by trying different username-password combinations. As the vast majority of users do not change their default manufacturer set credentials, obtaining access to them is easy. In fact, attacks up to 400 Gbps have already been launched. Another favorite device used for these type of attacks are routers, and have been used for this type of attack for a long time.

At the end of September, the French hosting company **OVH** began receiving massive DDoS attacks. The largest one hit at 799 Gbps and was the largest recorded measure to date. They have since been on the receiving end of attacks with traffic exceeding 1 Tbps. Looking at the data given by OVS, the attack was launched from 152,000 devices and most of them belonged to the IoT (IP cameras, video recorders, etc.).



In the automobile sector, investigators at the **University of Birmingham** demonstrated how they were able to **compromise the door opening systems on all vehicles sold by the Volkswagen Group** from the last 20 years. Through reverse engineering they were able to do it with the cryptographic key that is used by all VW cars. Oddly, once the key was obtained they had to stand 300 meters away from the affected vehicles, and wait for the far-off command on a radio device, in order to intercept another key, each one unique for each car. Once they had this information they could easily clone the remote control that opens and closes the car.

Investigators **Charlie Miller and Chris Valasek**, who demonstrated last year how to remotely hack a **Jeep Cherokee**, have gone even further this year by showing how they could override signals and tell the parking brake not to activate, disable the steering wheel, and make the wheel turn at any speed on command. Contrary to the previous situation, in order to have this type of control they had to connect a computer directly to the car. It is very important that we pay special attention to these life-threatening hacks—yours could be in danger if they can manipulate the car you drive.

This September, Chinese investigators from Keen Security Labs demonstrated how to compromise a Tesla car by remote, both in park or in drive mode. In their video, you can see how the car can be controlled remotely without physically touching it; the car can be opened and closed, the trunk can be opened while the car is in drive, and demonstrators can even control the breaking from miles away. The investigators sent the information to the manufacturers in advance so they could correct the detected problems with the latest version of firmware.



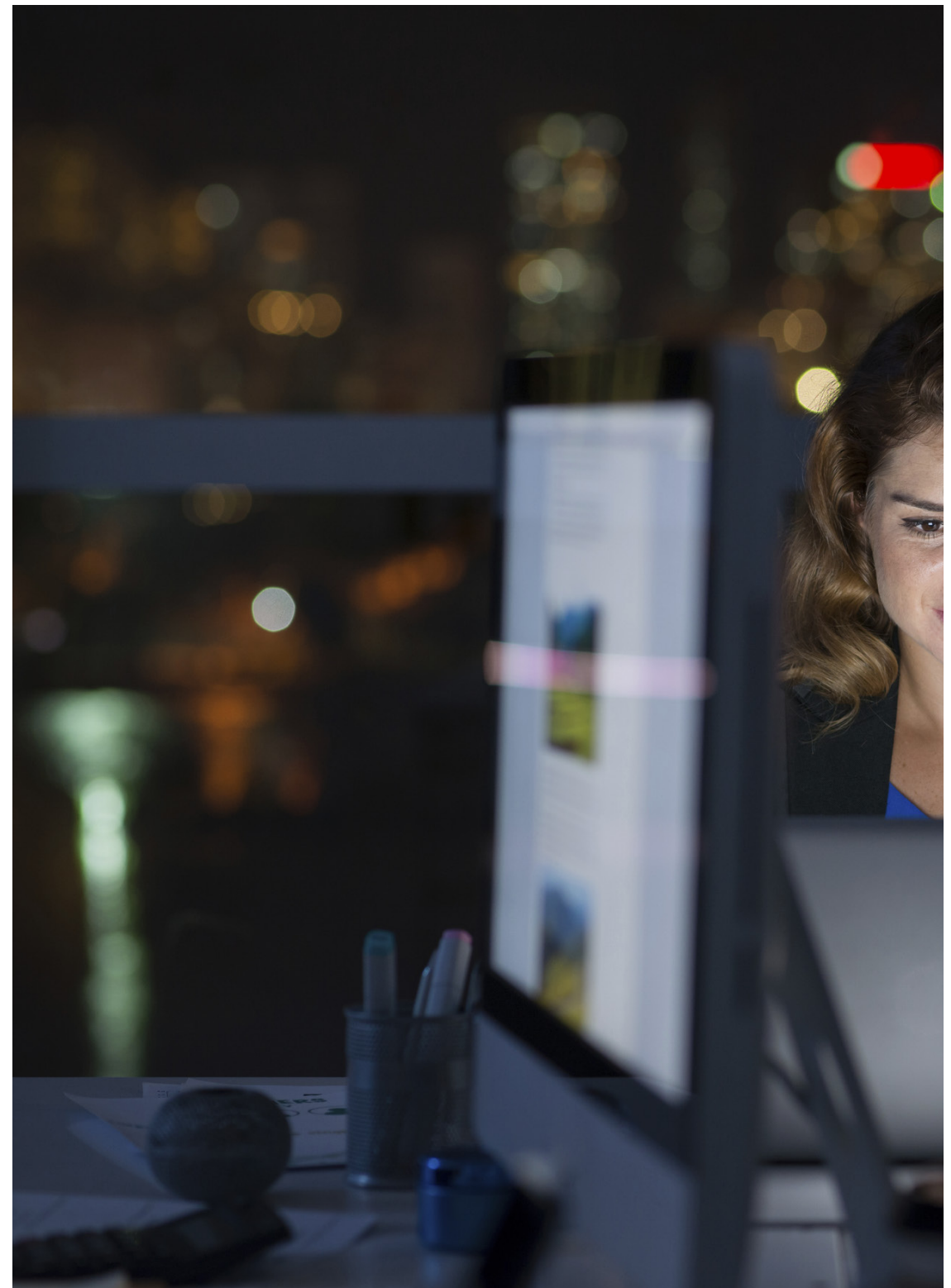
Cyberwar

In the middle of the US Presidential campaign there was an attack that targeted the **Democratic National Committee (DNC)**. During this cyberattack **all sorts of highly sensitive information was stolen and publicized**. While attempting to discover who's behind these attacks is very complicated and sometimes impossible, in this case it seems clear that the attackers are Russian, leading to accusations over the Russian government's attempts to harm the DNC campaign. Apparently there were two different attackers (both were Russian) and one of them **published 20,000 emails on WikiLeaks**.

Following the theme of elections, **the FBI sent out an alert stating that two electoral websites had been hacked**, and at least one of the foreign attackers could have obtained the voter registration information.

Governments are realizing how essential cybersecurity is. President Obama recognized that there is still a lot of work to do, especially remembering that the White House's network was broken into in the past. In September he named **the first Chief Information Security Officer (CISO) in US history**.

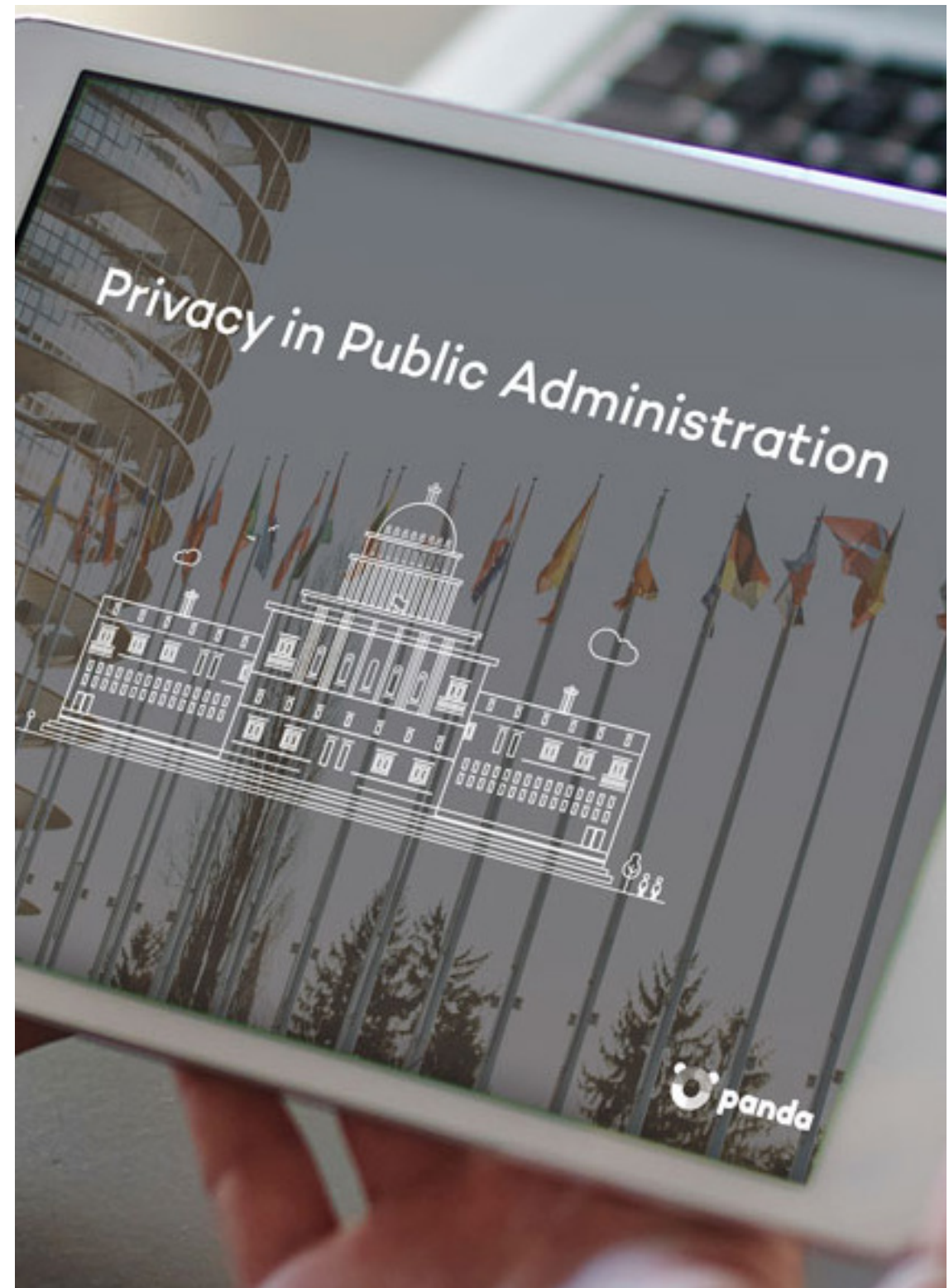
Last August, a group who call themselves **"The Shadow Brokers"** announced that they hacked the **National Security Agency (NSA)**. They publicized some of the stolen cyber weapons and promised to sell them to the highest bidder. It is still unknown who is behind this group but it has been speculated that they are from Russia. In any case, it seems that they used the same tools to launch their attack on the NSA.



On many occasions we discuss attacks that are government sponsored, but the truth is that, like with cybercrime, it is practically impossible to identify the criminal. We were surprised to hear that **Google** notifies their customers when they detect this type of attack, as stated by senior executive, Diane Greene. Currently they send **4,000 notifications per month**.

Prosecutors in **South Korea** believe that North Koreans were responsible for **hacking dozens of email accounts belonging to government officials**.

Once again, these critical infrastructures became front page news after it emerged that **Iran removed malware from two petrochemical plants**. **It is public knowledge that there were several fires in these plants** previously so they are investigating to see if the malware is related.



3. CONCLUSION

3

Conclusion

The end of 2016 is near and **we must keep paying attention to the evolution of DDoS attacks.** The combination of millions of **hackable IoT devices,** and the increasingly fast Internet connection we have at home, could turn one of these attacks into one of the biggest Internet-nightmares with the potential to affect everyone especially businesses that are targeted by these professional extortionists.

Data theft is increasing and has even surpassed last quarter. In Q3, data was stolen from 500 million Yahoo users. **Taking action today is more important than ever: never forget two-step verification** when you register for services because this will prevent your account from being compromised, even if your log-in credentials are stolen or leaked.

At PandaLabs, we will keep you informed of all the cybersecurity developments through our Media Center, and we will see you in three months to analyze what happens in Q4 of 2016.



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

4. ABOUT PANDALABS

4

About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory and R&D center where:

-  PandaLabs creates automated and real-time systems 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.



This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Panda Security.

© Panda Security 2016. All Rights Reserved.

