PANDALABS QUARTERLY REPORT: Q2 2017

pandalabs

1. INTRODUCTION

panda

pandalabs

1
Introduction

From a cybersecurity standpoint, the second quarter of 2017 has been one of the scariest in years. Without a doubt, the WannaCry attack in May and the GoldenEye/Petya attack in June were the standouts, as they affected countries all over the globe and impacted a multitude of companies, a number of whom are still recovering their systems. Different estimates put the overall cost of these attacks at between one and four billion dollars.

These attacks are closely bound up with the growing field of cyberwarfare and countries' various efforts to counter it. Both took advantage of a vulnerability discovered by the NSA, and stolen by the hacker group known as the Shadow Brokers, who published it in April. There is some evidence that points to North Korea as the origin of the WannaCry attack, while the GoldenEye/Petya attack appears to have been aimed at sabotaging Ukrainian companies and institutions on the day before their Constitution day, suggesting that Russia may have been behind it.

While we can't officially say that an all-out cyberwar is being fought, in one way or another skirmishes and attacks like WannaCry or Petya affect us all. Amidst all the noise of these standout attacks, **others are quietly taking place under the radar**. But they are just as serious, and maybe even more so. **Emboldened attempts to manipulate elections in countries such as France or the United States using cyberespionage tactics** in favor of candidates whose political motives align with the perpetrators' (as was the case with Trump in the United States or Le Pen in France) are clear examples of the shadow warfare taking place in the cyber realm that has the ability to greatly affect world events.

Meanwhile, everyday citizens are coming face to face with a multitude of cybercriminals whose goal is to turn a hefty profit at the victim's expense.

pandalabs

2. THE QUARTER IN NUMBERS

panda

pandalabs

2

The Quarter in Numbers

In our reports, as well as in those prepared by other developers of cybersecurity solutions, we always provide similar types of statistics on malware: how much new malware has appeared over a period of time, kinds of malware, etc. Although that type of information is all well and good, and can make for some attention-grabbing headlines, for this year's reports we at PandaLabs have decided to go one step further and look for data that brings new meaning and real value.

To calculate the figures shown below we decided not to count the detection of any malware that we've already detected by signatures (which would be in the hundreds of millions), since it is malware that is already well known and to a greater or lesser extent every user with a basic antivirus is protected from it. Nor will we include heuristic detection techniques, which are able to detect variants of known malware or techniques.

The reasoning behind this decision is that professional attackers at the very least make sure to do basic tests with antivirus engines to make sure their new samples of malware are not detected, and these engines include both signature and heuristic detections. That is, we can take these figures for granted, since users were protected and were not at real risk of infection.

We are going to take into account only new malware data that was not detected either by signatures or heuristics — malware attacks, fileless attacks, and any attack made through the abuse of legitimate system tools, something which is increasingly common in corporate environments, as we saw in the case of GoldenEye/Petya back in June.

But how are we going to measure something that we are not able to detect?

The point is that we are in fact able to detect and stop these attacks, even though they have never been seen or detected by signatures or heuristics before. To do this, we use a series of proprietary technologies, encompassed in what we call "Contextual Intelligence", which allows us to reveal patterns of malicious behavior and generate advanced cyber defense actions against both known and unknown threats.

This layer of Contextual Intelligence gives us excellent detection ratios in tests that imitate attacks as they happen in the real world. In the tests carried out by AV-Comparatives during the first six months of 2017, Panda Security achieved excellent ratios in the Real-World Protection Test, receiving the maximum "Advance+" award with our Panda Free Antivirus, the most basic solution in our portfolio of cybersecurity products.

Next, we analyze the attack data that we have gathered. Out of all the machines protected by a Panda Security solution, **3.44%** of them were attacked by unknown threats, representing an increase of almost 40% from the previous quarter. If we look at the type of client, home users and small businesses make up **3.81%** of attacks, while in the case of medium and large companies the figure is **2.28%.**

Home users have far fewer protective measures in place, and they are therefore more exposed to attacks. Many attacks that successfully run their course in a home setting are easily detained in corporate networks before they can have an effect.
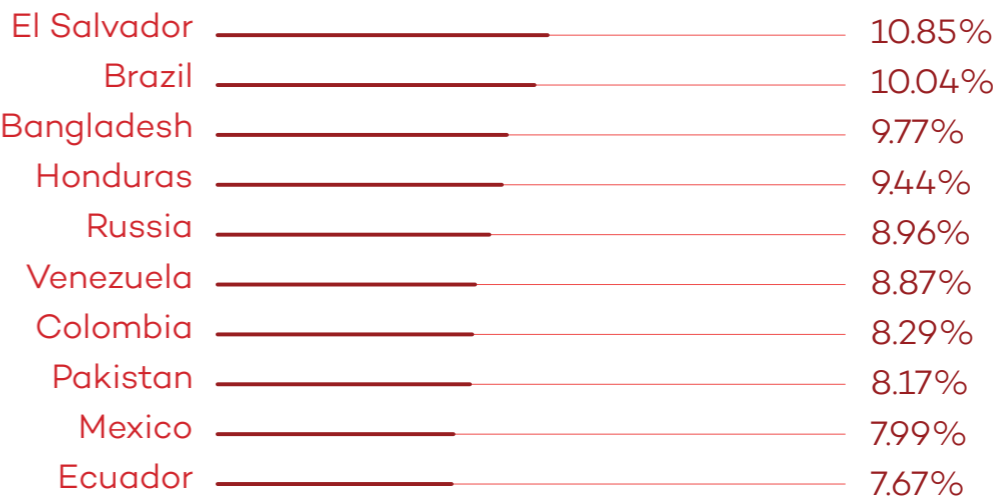
Among our corporate clients, we have those who use traditional solutions, and those who opt for our EDR solution (Adaptive Defense), which goes far beyond an antivirus and offers extra functionality, much broader levels of protection, classification and monitoring in real time of all processes running on servers and workstations, forensic analysis, etc. It only makes sense that the number of attacks that manage to skip all layers of protection in the EDR of Adaptive Defense is much lower than the corresponding number for traditional security technologies alone.

2.67% of the devices protected by traditional solutions receive attempts by unknown threats, while in devices protected by Adaptive Defense that number drops to **1.21%**. In both cases, Panda Security's solutions successfully neutralized these attacks in time, before they were able to have an effect on the systems.

How are these attacks geographically distributed? We have calculated the percentage of machines attacked in each country — the higher the percentage, the greater the likelihood of being exposed to a new threat when using a computer in that country.

Most Attacked Countries

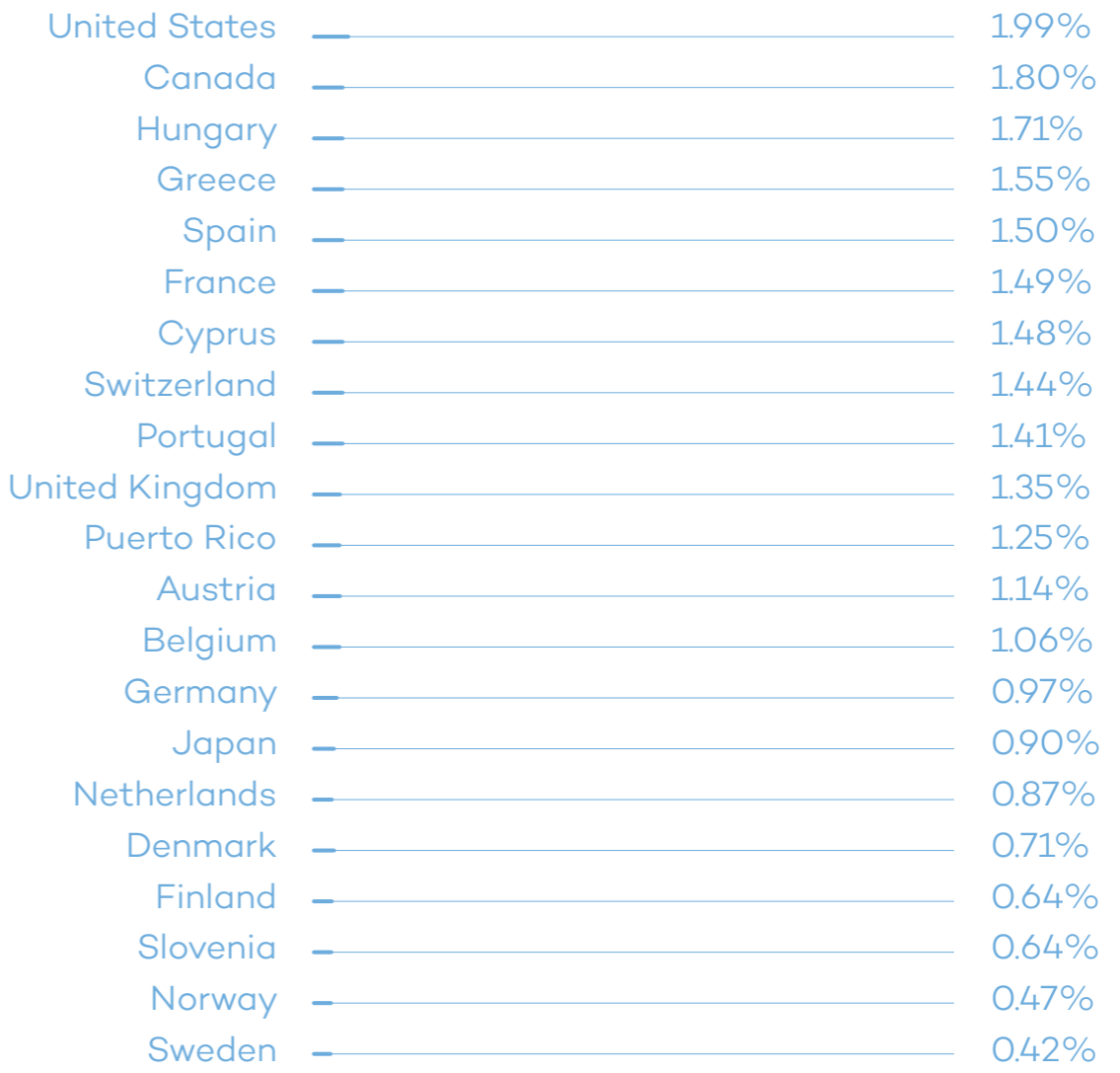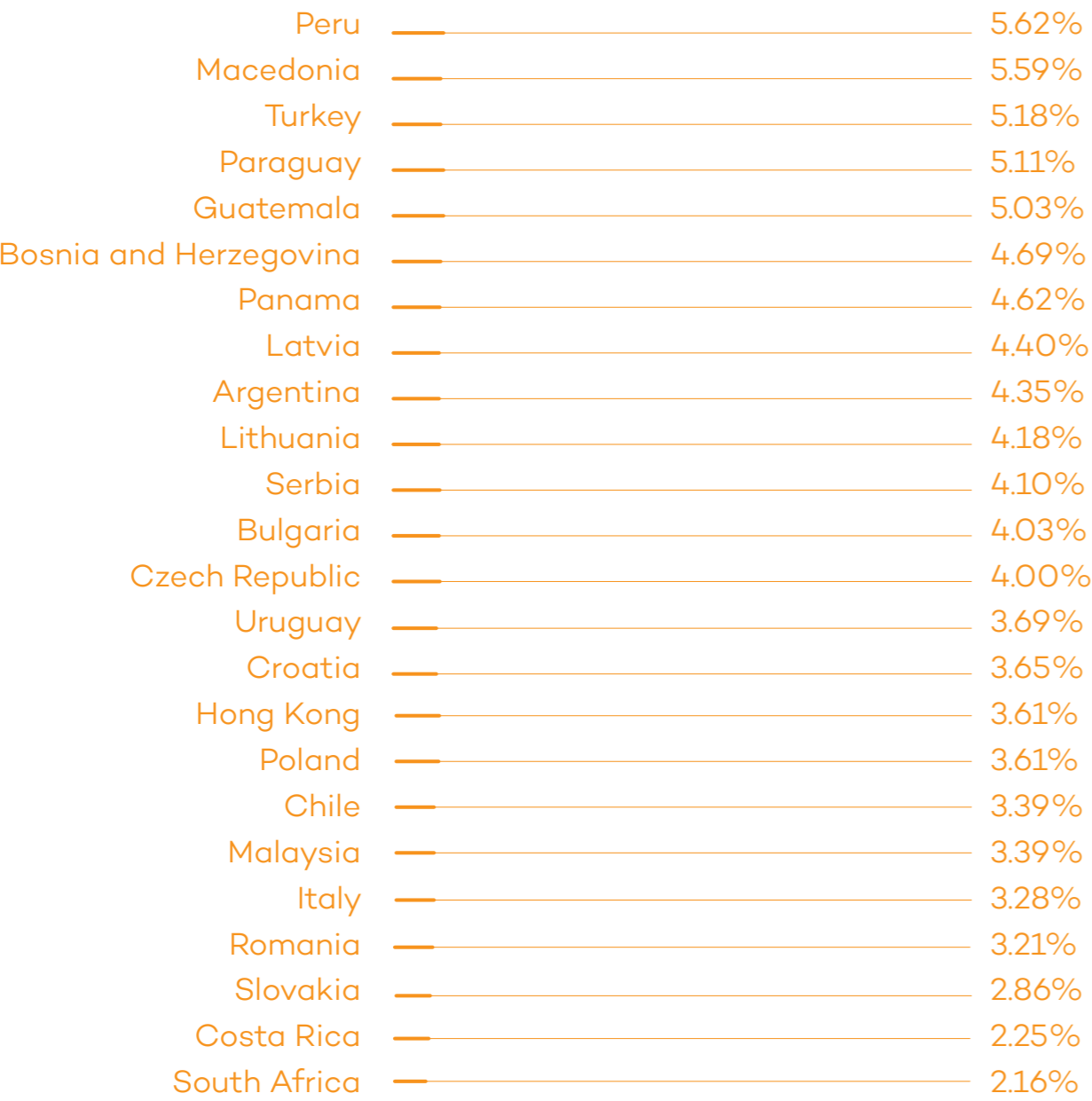| Country	Percentage
El Salvador	10.85%
Brazil	10.04%
Bangladesh	9.77%
Honduras	9.44%
Russia	8.96%
Venezuela	8.87%
Colombia	8.29%
Pakistan	8.17%
Mexico	7.99%
Ecuador	7.67%

Least Attacked Countries

Country	Percentage
Austria	1.14%
Belgium	1.06%
Germany	0.97%
Japan	0.90%
Netherlands	0.87%
Denmark	0.71%
Finland	0.64%
Slovenia	0.64%
Norway	0.47%
Sweden	0.42%

Full List of Countries

Country	Percentage
El Salvador	10.85%
Brazil	10.04%
Bangladesh	9.77%
Honduras	9.44%
Russia	8.96%
Venezuela	8.87%
Colombia	8.29%
Pakistan	8.17%
Mexico	7.99%
Ecuador	7.67%
Bolivia	7.58%
Indonesia	7.57%
Taiwan	7.46%
Thailand	7.30%
Iran	6.58%
Singapore	6.30%

panda

pandalabs

Country	%		Country	%
Peru	5.62%		United States	1.99%
Macedonia	5.59%		Canada	1.80%
Turkey	5.18%		Hungary	1.71%
Paraguay	5.11%		Greece	1.55%
Guatemala	5.03%		Spain	1.50%
Bosnia and Herzegovina	4.69%		France	1.49%
Panama	4.62%		Cyprus	1.48%
Latvia	4.40%		Switzerland	1.44%
Argentina	4.35%		Portugal	1.41%
Lithuania	4.18%		United Kingdom	1.35%
Serbia	4.10%		Puerto Rico	1.25%
Bulgaria	4.03%		Austria	1.14%
Czech Republic	4.00%		Belgium	1.06%
Uruguay	3.69%		Germany	0.97%
Croatia	3.65%		Japan	0.90%
Hong Kong	3.61%		Netherlands	0.87%
Poland	3.61%		Denmark	0.71%
Chile	3.39%		Finland	0.64%
Malaysia	3.39%		Slovenia	0.64%
Italy	3.28%		Norway	0.47%
Romania	3.21%		Sweden	0.42%
Slovakia	2.86%			
Costa Rica	2.25%			
South Africa	2.16%			

3. THE QUARTER AT A GLANCE

3

The Quarter at a Glance

This quarter was clearly defined by two major attacks. The first to occur was WannaCry in May, which tore across corporate networks in every corner of the globe.

WannaCry is one of the largest attacks in history. Although there have been attacks in the past where the number of victims or the speed at which the attack spread were greater (such as Blaster or SQL Slammer), the damage these attacks caused was mostly collateral as they spread. However, WannaCry is a ransomware with worm functionalities, which means that no infected network was spared from being encrypted. Keep in mind that we're talking about more than 230,000 computers, with losses estimated between one and four billion dollars. That's an average loss of $4,300 per victim at the low end, or more than $17,000 at the top end. So it's safe to say that this was one of the most damaging attacks in history.

For a detailed analysis of what happened and recommended measures to be taken, you can watch the webinar on the WannaCry attack given by Luis Corrons, Technical Director at PandaLabs, here.

The second attack to have a major impact this quarter was GoldenEye/Petya, a sort of aftershock of the WannaCry earthquake. Despite the fact that the majority of its victims were found in a limited geographic area (specifically, Ukraine), **it ended up affecting companies in more than 60 countries**.

The carefully-planned attack was carried out using an accounting software application called MeDoc, very popular in Ukraine. The attackers compromised the software's update server, so any computer with MeDoc installed could be automatically infected when the time came to install the update.

pandalabs

This attack was as sophisticated as it was harmful. It not only encrypted files, but also the hard drive's MBR (Master Boot Record) in cases where the logged in user had admin permissions. At first it appeared to be a ransomware similar to WannaCry, but after performing a deep analysis of the malware we saw that the attack's authors had no intention of allowing the encrypted data to ever be recovered.

It seems obvious that with GoldenEye/Petya, we're dealing with a targeted attack aimed at sabotaging company computers at Ukrainian institutions. But like with any weapon of mass destruction, collateral damage is inevitable. Once GoldenEye/Petya had infiltrated the corporate network, it spread using a wide array of very effective techniques. Foreign companies with offices in the Ukraine were therefore also infected.

Days after the attack, the Ukrainian government openly accused Russia of perpetrating the attack.

In a presentation, which you can view here, PandaLabs parses through the key points of this attack and its authors.

Ransomware

WannaCry and GoldenEye/Petya have stolen the spotlight, **but ransomware in general is on the rise**. Web hosting company Nayana of South Korea was attacked and ransomware encrypted data on 153 Linux servers.

The attackers demanded a ransom of $1.62 million. The company negotiated with the criminals and lowered the figure to $1 million, paid in three installments.

Cyberwarfare

The two major attacks of 2017 have given rise to suspicions that governments could have been behind them (North Korea in the case of WannaCry and Russia in the case of GoldenEye/Petya). But these are only a couple of cases within a much broader, and more or less covert, war taking place in cyberspace.

The main players in this game of cyberwar are the usual suspects: the United States, Russia, North Korea... but surprisingly, China has been absent from this list over the last few months, as it has not been involved in any recent scandals. One explanation for this could be the cybersecurity agreement signed between the US and China in 2015, although it could very well be that they are indeed carrying our attacks that simply have not been identified.

The US is clearly concerned about attacks targeting American institutions. Samuel Liles, Acting Director of the Cyber Division at the Department of Homeland Security (DHS), testified before the Senate Intelligence Committee that Russian government-backed hacking attacks targeted systems related to the presidential elections in more than twenty-one states.

The Congressional Intelligence Committee held a hearing to discuss the impact of Russia's hacking of the 2016 presidential elections. It was there that Jeh Johnson, former DHS Secretary under the Obama administration, reiterated that Russian President Vladimir Putin had ordered the attack **with the intention of influencing the outcome of the US presidential elections**. He also asserted that they had failed to manipulate votes in these attacks.

In June, the US government issued an alert blaming the North Korean government for a series of cyberattacks carried out since 2009, warning that they are likely to commit further strikes. The warning, which came from the DHS and FBI, referred to a group of attackers, "Hidden Cobra", who have targeted the media, the aerospace and financial sectors, among others, as well as critical infrastructures in the US and others countries.

While the name "Hidden Cobra" is not widely known, this group is also known as the "Lazarus Group," which has been associated with such attacks as the Sony hack in 2014.

If you follow the trail of evidence leading to the Hidden Cobra/Lazarus Group, their activity will take you right up to WannaCry itself, making stops along the way at attacks on financial institutions like the attack on the Central Bank of Bangladesh.

During the Gartner Security & Risk Management Summit held in Washington in June, former CIA director John Brennan said the alleged alliance between the Russian government and cybercriminals to carry out Yahoo's theft of accounts is only the tip of the iceberg, and that future cyberattacks by governments will follow this type of formula and become more frequent.

In the same talk, he said that Russian intelligence services

are not really reined in by laws, while US agencies are. Some might find these statements paradoxical, as it has become widely known (via WikiLeaks) that the CIA has been hacking home, business, and public Wi-Fi routers for years to carry out clandestine surveillance.

In our last report, we commented on how France had discarded the use of electronic voting methods by their citizens residing abroad in the face of the "extremely high" risk of cyberattacks. It turned out that there was at least one cyberattack, and just two days before the elections, a trove of private information was published by Emmanuel Macron, who quickly sent a press release indicating that they had been hacked.

Later investigations linked the hack to the group "Fancy Bear", suspected of being backed by the Russian government.
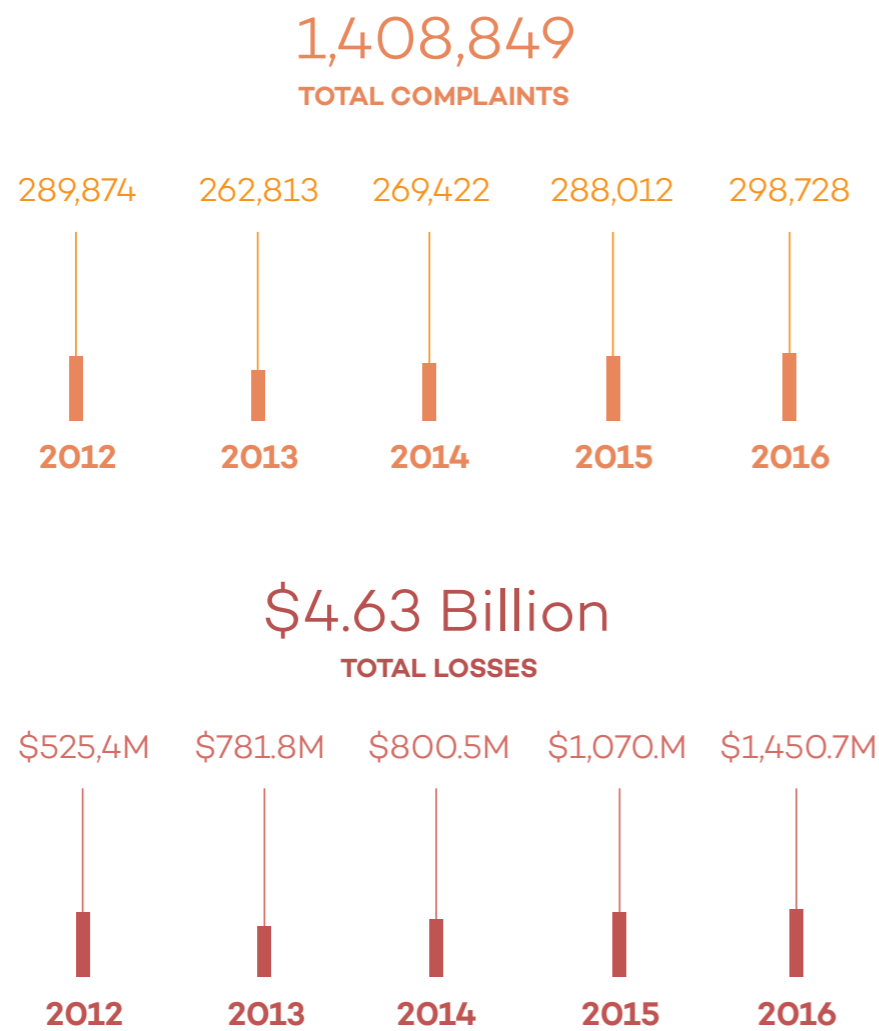
Members of the British Parliament have been targeted in attempts to brute-force hack their email accounts, according to the Financial Times, in what is believed to be an attack sponsored by a foreign power.

This vortex of subterfuge and international conflict is affecting technology companies. The Russian FSB is asking companies like CISCO, SAP and IBM for the source code of their security solutions to look for possible backdoors. Days later the US government banned all federal agencies in the country from using Kaspersky solutions because of its proximity to the Russian government and the FSB.

Cybercrime

According to the 2016 Internet Crime Report published by the IC3 (Internet Crime Complaint Center), a branch of the FBI, **losses due to cybercrime were up 24%, surpassing 1.3 billion dollars.**

And we have to keep in mind that this number only takes into account losses reported to the IC3, which estimates that this is only about 15% of real total losses, which would mean that in the US alone there were 9 billion dollars of losses in 2016.

1,408,849
TOTAL COMPLAINTS

2012	2013	2014	2015	2016
289,874	262,813	269,422	288,012	298,728

$4.63 Billion
TOTAL LOSSES

2012	2013	2014	2015	2016
$525,4M	$781.8M	$800.5M	$1,070.M	$1,450.7M

The most sought-after exploits are used for launching zero-day attacks, which by definition the manufacturer of the software is unaware of and which allow attackers to compromise computers, even if their software is updated. In April, a vulnerability was discovered which affected various versions of Microsoft Word,

and we know that it was being used by attackers from at least January. In that same month of April, Microsoft published a corresponding update to protect Office users.

The medical records of at least 7,000 people were compromised by a security breach at the Bronx Lebanon Hospital Center in New York.

There were other security incidents in which no attackers were directly involved. In these cases, due to a technical error or simple negligence, data that should be protected is in fact exposed to anybody who cares to access it. This happened to the **Automobile Association (AA)**, which left 13 GB of data "out in the open" for a few days in April, among which could be found over 100,000 email addresses associated with credit card information.

A similar case occurred at an even higher level in the US. **Marketing firms hired by the Republican Party exposed the data of 198 million voters for anyone to access**, accounting for nearly all registered voters (which totals just over 200 million). The data was accessible for at least a couple of days and contained all kinds of voter information: names, dates of birth, addresses, etc.

In China, trafficking of Apple customer data ended with the arrest of 22 people. All signs point to an inside job, as some of the detainees worked for companies subcontracted by Apple and had access to the data that was being sold.

InterContinental Hotels Group (IHG) made the news when it fell victim to data theft affecting its customers. Although the company said in February that the attack had only affected a dozen hotels, it has now become known that the POS terminals in more than 1,000 of their establishments were infected. In a statement, the company confirms that the cards corresponded to

overnight stays between September 29 and December 29, 2016. It also explained that although there is no evidence of unauthorized access to payment information after December 29, 2016, confirmation that the malware had been eradicated did not come until March 2017. Among the different hotel chains owned by the group are Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels, and Crowne Plaza.

OneLogin, a service that offers users a single sign-on for all types of platforms in the cloud, offering a more convenient and secure usability, was, ironically, hacked. The company announced through its blog that it had been attacked and that intruders had managed to enter its data center in the United States, accessing databases and leaving user information, applications, and passwords exposed to hackers.

Mobile Devices

Starting on June 1, Google began offering higher rewards for anyone finding the most serious security flaws in their products (so far, none have been found). The first reward has risen from 50,000 to 200,000 dollars, the second from 30,000 to 150,000.

A vulnerability (CVE-2017-6975) in the firmware of the Broadcom Wi-Fi HardMAC SoC chips, which occurs when renegotiating a connection to a Wi-Fi network, forced Apple to release an iOS (10.3.1) update.

This vulnerability, however, not only affects iPhones and iPads, but also third-party mobile devices such as Samsung or Google's own Nexus, which received its security update in April to address this security issue.

IoT

We've become very comfortable living in a connected world. But the conveniences that come with it are just one side of the coin. Another aspect of it, more sinister, can lead to an attack like WannaCry having a much wider reach than it could have.

Smart Cities, hyperconnected cities that are made up of networks of millions of devices, are a prime example of the embedding of technology in our daily lives. Cities around the world are increasingly "smart", and it is estimated that by 2020 there will be more than 50 billion devices connected to the Internet. This comes with immense security risks affecting cities' infrastructure, such as traffic lights or the city's water supply. Last June, WannaCry infected 55 cameras located at traffic lights and speed control points in Australia after a subcontractor connected an infected computer to the network where they were located. Police had to cancel 8,000 traffic fines following the incident.

At 11:30 pm on April 7, 156 emergency sirens began to sound in unison in Dallas, Texas. Officials managed to shut them off 40 minutes later after taking the entire emergency system offline. Investigators still don't know who was behind the hack that triggered this incident.

A new vulnerability affecting Mazda cars recently came to light. However, unlike other cases that we have seen in the past, in order to compromise the car's system it is necessary to insert a USB while the engine is running in a certain operating mode.

4. CONCLUSION

4

Conclusion

The Shadow Brokers plan to continue publishing stolen NSA data, and the cyberarms race is coming to a boil. Individuals and companies should take extra security precautions.

Home users and small businesses have the greatest risk of infection. Countries most prone to suffering infections from new threats include El Salvador, Brazil, Bangladesh, Honduras, Russia, and Venezuela.

WannaCry and Petya show us that governments are not hesitating to "push the button" when it comes to launching a cyberattack. Everyone who uses the internet or connected devices could end up being a collateral victim on the global stage of cyberwarfare. Every angle should be considered in finding a way to create an international treaty — such as the Geneva Convention — to limit states' capabilities when it comes to cyberattacks.

Ransomware attacks are still on the rise, and the only explanation is that there are still victims willing to pay. Otherwise, attacks of this sort would eventually be phased out. It is up to all of us to put an end to these attacks, on the one hand protecting ourselves against becoming victims, and on the other to always keep a backup of our data so as to never pay a ransom.

The most sought after exploits to launch attacks are those known as "zero-day" attacks, which are vulnerabilities that are completely unknown by the manufacturer of the affected software. Insider attacks are also among the greatest risks facing individuals and companies, as well as attacks on POS terminals.

pandalabs

Having an ever-growing number of connections to the Internet, ranging from mobile to all types of IoT devices, increases the reach of attacks to levels far greater than what we've been accustomed to in the past.

This trend will continue to be on the rise, as we will soon have tens of billions of devices connected to the internet, a number which will only increase.
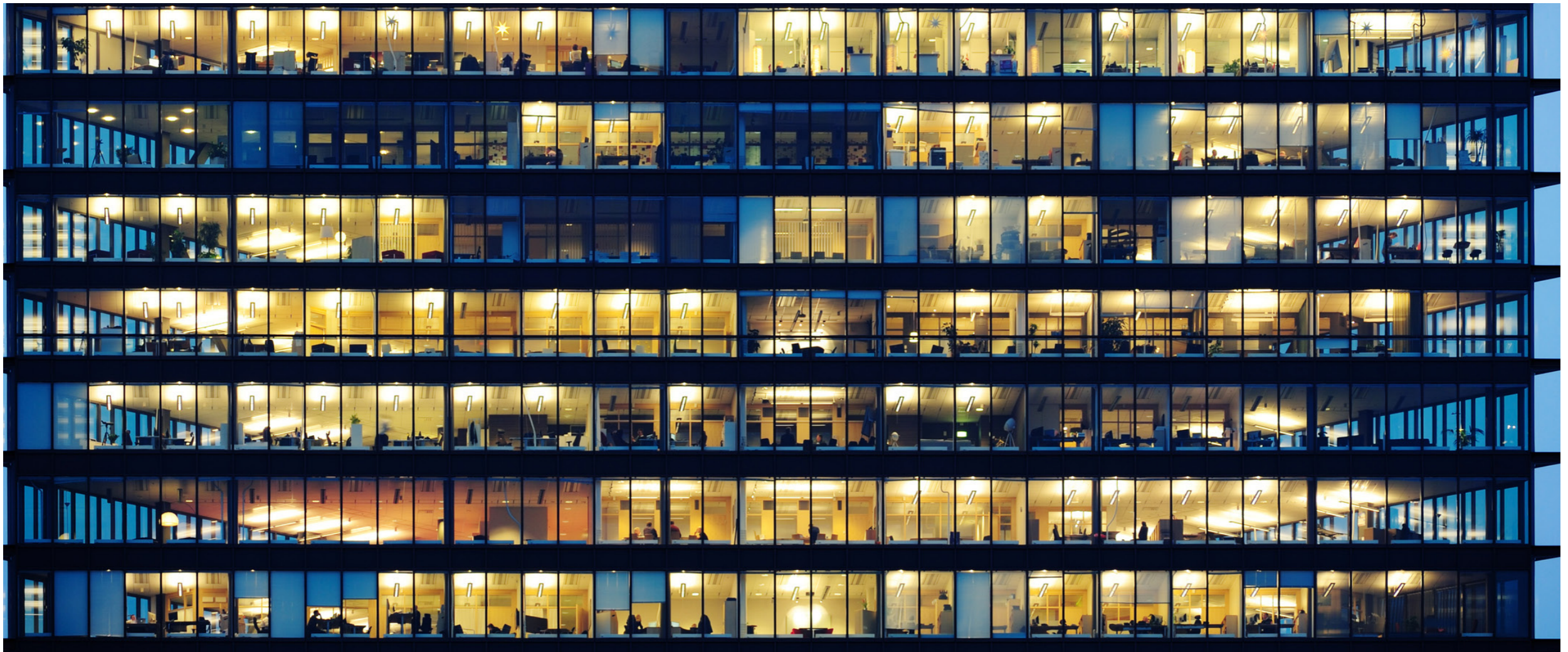
05.
RECOMMENDATIONS

panda

pandalabs

5
Recommendations

Traditional security solutions, while effective in protecting against malware, are not capable of dealing with attacks where non-malicious tools and other advanced techniques are used.

It is imperative to use security software appropriate to the level of threat that we are facing. EDR (Endpoint Detection & Response) solutions like Adaptive Defense are the only ones that provide us with the necessary tools to protect us from sophisticated attacks.

The most important thing when dealing with an attack is to have all of the information you can on it: what happened, when, how, whether there had been data theft or not, etc. The security solution we use must be able to provide all of this data, both in real time and afterwards, so that we can perform detailed analysis of incidents. This is especially important with the imminent enforcement of the General Data Protection Regulation (GDPR) in May 2018.

We must also have contingency plans in place. Sooner or later, we may fall victim to an attack, and being able to react can minimize the damage dramatically.

Governments and large public and private companies are already betting on this strategy, making Adaptive Defense the best-selling security solution in the history of Panda Security. Multinationals in all types of strategic sectors (financial, telecommunications, military, energy, etc.) rely on Panda Security to protect their systems with Adaptive Defense.

PandaLabs will keep you up to date with news from the world of cybersecurity in our Media Center.

pandalabs

6. ABOUT PANDALABS

6

About PandaLabs

PandaLabs is Panda Security's Security Operations Center and anti-malware laboratory. It is the company's nerve center for everything malware related. At PandaLabs, we:

Provide uninterrupted countermeasures in real time to protect Panda Security's customers from all types of malicious code on a global scale.

Perform detailed analysis of all types of malware in order to improve our protection solutions, as well as to keep the general public informed.

PandaLabs maintains a continuous state of vigilance, closely following the different trends and developments in the field of malware and security.

Our purpose is to alert the public to imminent dangers and threats, as well as to formulate forecasts for future threats.

pandalabs