PANDALABS QUARTERLY REPORT Q1 2017

panda

pandalabs

1. INTRODUCTION

1 Introduction

The Internet is, almost by definition, the mother of all networks, a great machine of decentralized information, storage, and data-sharing. The sheer breadth of its possibilities goes far beyond any phenomenon we've ever experienced, and yet, despite its many advantages, it is also largely ungovernable and can be a source of unexpected obstacles for institutions, businesses, and private users.

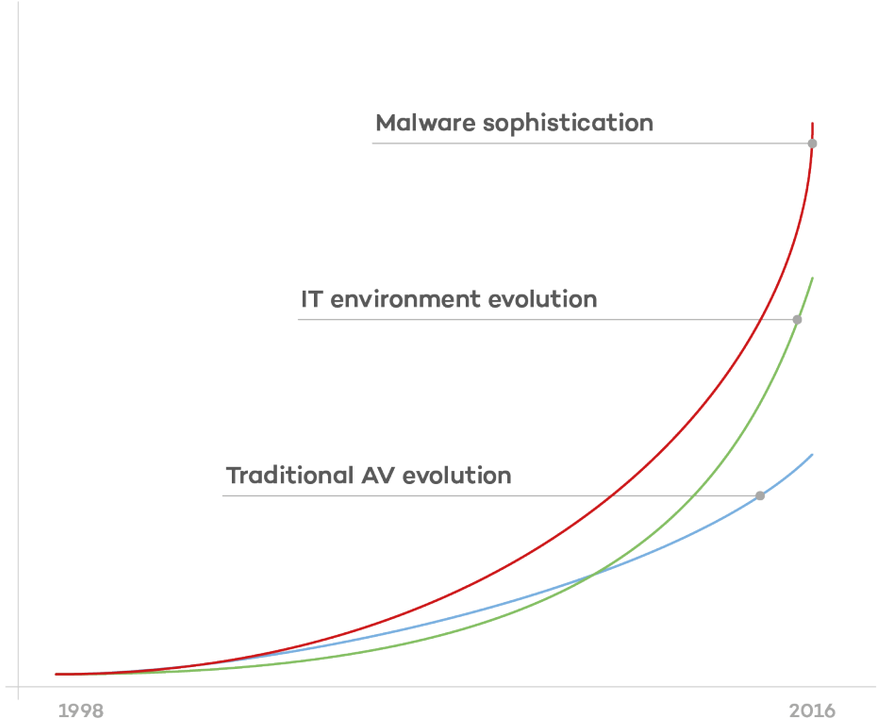
In the first quarter of 2017, we have seen some of the consequences of a world that increasingly relies on the Internet to control real world fixtures and manufacturing processes, most of them unprotected.

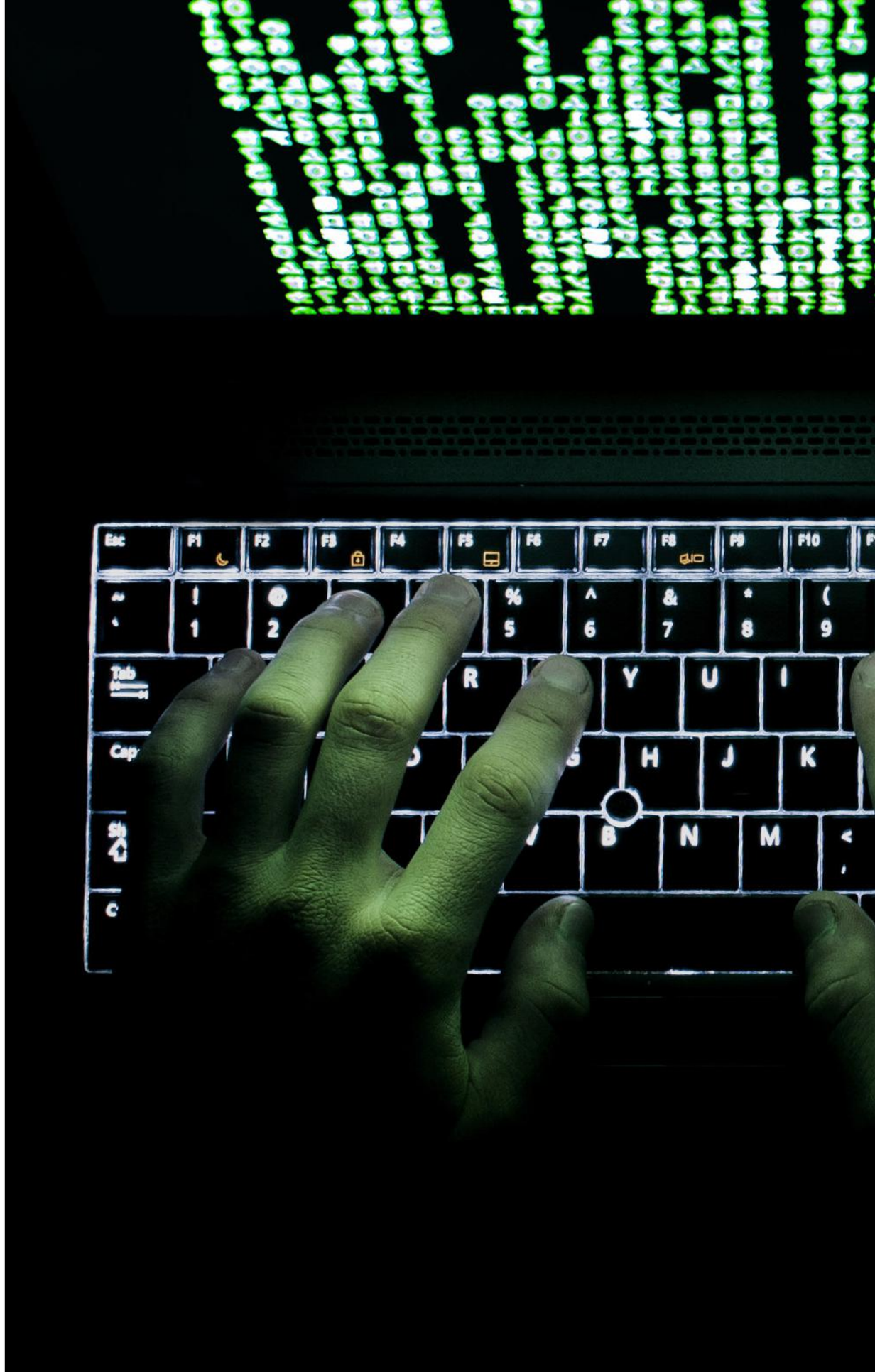
There has been a marked increase in the number of cyberattacks that happen every day, and they're more complex than ever before. Their constant evolution makes it necessary to stay one step ahead of malicious behavior. Taking into consideration the data collected in the first months of the year, we've singled out three main factors for a cyberattacker's success.

- More sophisticated threats, new attack vectors, and a higher number of offensives.
- More complex IT environments, with an overpopulation of devices, systems, and connections.
- Traditional antiviruses, which do not evolve as quickly as attacks

If we had to pick one tendency that sticks out above the rest, it would be that attacks are becoming increasingly customized, or “made to order”, according to the chosen victim. Attackers now interact with the victim’s network and defense systems in real time, adapting to them in order to achieve their goals.

In the year’s first months, the Internet of Things (IoT) gave us a bit of a surprise when Smart TVs were targeted with ransomware. LG televisions, operating with Android, were the first to be infected, demonstrating the way that Smart TVs could be compromised remotely using TDT signals.





2. ANALYSIS OF ATTACKS

2 Analysis of attacks

In our reports as well as in those of the rest of security solution manufacturers, we often see the same kind of figures on malware: how much new malware has appeared in a given period of time, types of malware, etc. Although these figures are interesting and can make for some great headlines, we asked ourselves at PandaLabs what we could show to measure the real risks of infection that users face in both domestic and corporate environments. We're looking for data points that provide real added value.

To get such data, we focus on the issues that all of our customers have to face. Firstly, we decided not to count any malware detected by signatures (a number that would reach the hundreds of millions), since it is known malware that, to a greater or lesser extent, every user with a basic antivirus is protected from. On the other hand, we also decided not to include heuristic detection, which is capable of detecting malware that is not previously known.

The rationale for this decision is that professional attackers are careful to do at least a minimal amount of testing with antivirus engines to make sure their new malware samples are able to go undetected, and these engines include both signature and heuristic detections. In other words, we can take these figures for granted, since users were protected at all times and there was never any real risk of infection. But if we're not talking about what we do detect … then what data can we bring into the picture?

At Panda Security, we've always been passionate about client protection, so a few years ago our laboratory created a layer of protection that we decided to add to all our solutions. This layer only comes into play when all other layers of protection

fail. That way, we know that everything we stop there is a completely new attack.

With this system in place, not only do we count attacks that use malware, but also add fileless attacks to the list, or those made through the abuse of legitimate system tools, something increasingly common in corporate environments.

This extra layer is what has allowed us to consistently maintain excellent detection ratios in tests conducted with methodologies that imitate attacks as they happen in the real world. In the AV-Comparatives tests conducted in the first quarter of 2017, we obtained a 100% detection rate in the two Real-World Test tests, and in the Malware Protection Test we received the highest acheivement, with a 99.89% detection rate and only 1 false positive, ahead of all our competitors.

Of all the devices protected by a Panda Security solution, 2.25% of them have suffered attacks from unknown threats.

If we look at the type of customer, domestic users have 2.19% of attacks while in the case of companies the figure is 2.45%. While it may seem counterintuitive, as corporate networks have a much more elaborate defense system than home computers, we must remember that companies are dealing with more professional attacks. Corporations possess information that is infinitely more valuable than what one might find on any given home PC.

Among our corporate clients, there are those who use traditional solutions and those who opt for our EDR solution (called Adaptive Defense), which goes far beyond an antivirus and offers extra functionalities, much more expansive levels of protection, classification, and monitoring in real time of all processes running on servers and stations throughout the IT infrastructure, forensic analysis, etc.

Since it adds higher security levels, the percentage of attacks that were blocked after skipping the rest of protection layers is much lower in Adaptive Defense than in traditional protection systems. 2.83% of devices protected by traditional solutions receive attacks from unknown threats. With devices protected by our next-generation solution, that number drops to 0.83%.

In terms of the geographical distribution of these attacks, we have calculated the percentage of machines attacked in each country. The greater the percentage, the greater the probability of being attacked by new threats when using computers in those countries:

COUNTRIES WITH THE HIGHEST RATES OF ATTACKED COMPUTERS IN THE FIRST QUARTER OF 2017

Asia and Latin America are the regions with the highest infections.

Below you can see the 10 countries with the lowest rate of infection:

COUNTRIES WITH THE LOWEST RATES OF ATTACKED COMPUTERS IN THE FIRST QUARTER OF 2017

Switzerland	1,03%
Slovenia	1,01%
France	0,98%
Greece	0,95%
Ireland	0,85%
Sweden	0,85%
Netherlands	0,66%
Denmark	0,65%
Czech Republic	0,55%
Finland	0,34%

Other countries with a percentage lower than the world average are Belgium (1,04%), Canada (1,12%), Latvia (1,19%), Germany (1,20%), Spain (1,27%), United Kingdom (1,29%), Australia (1,30%), and Slovakia (1,31%).

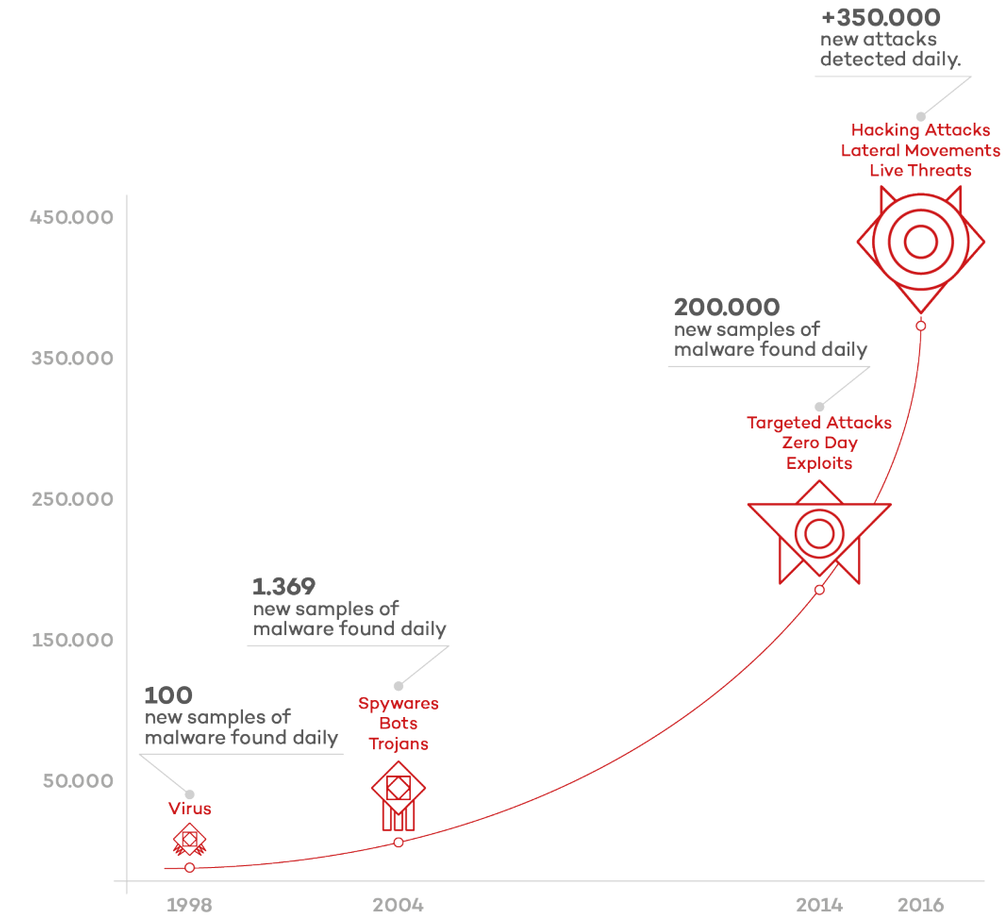
3. THE EVOLUTION OF THREATS

3

The Evolution of Threats

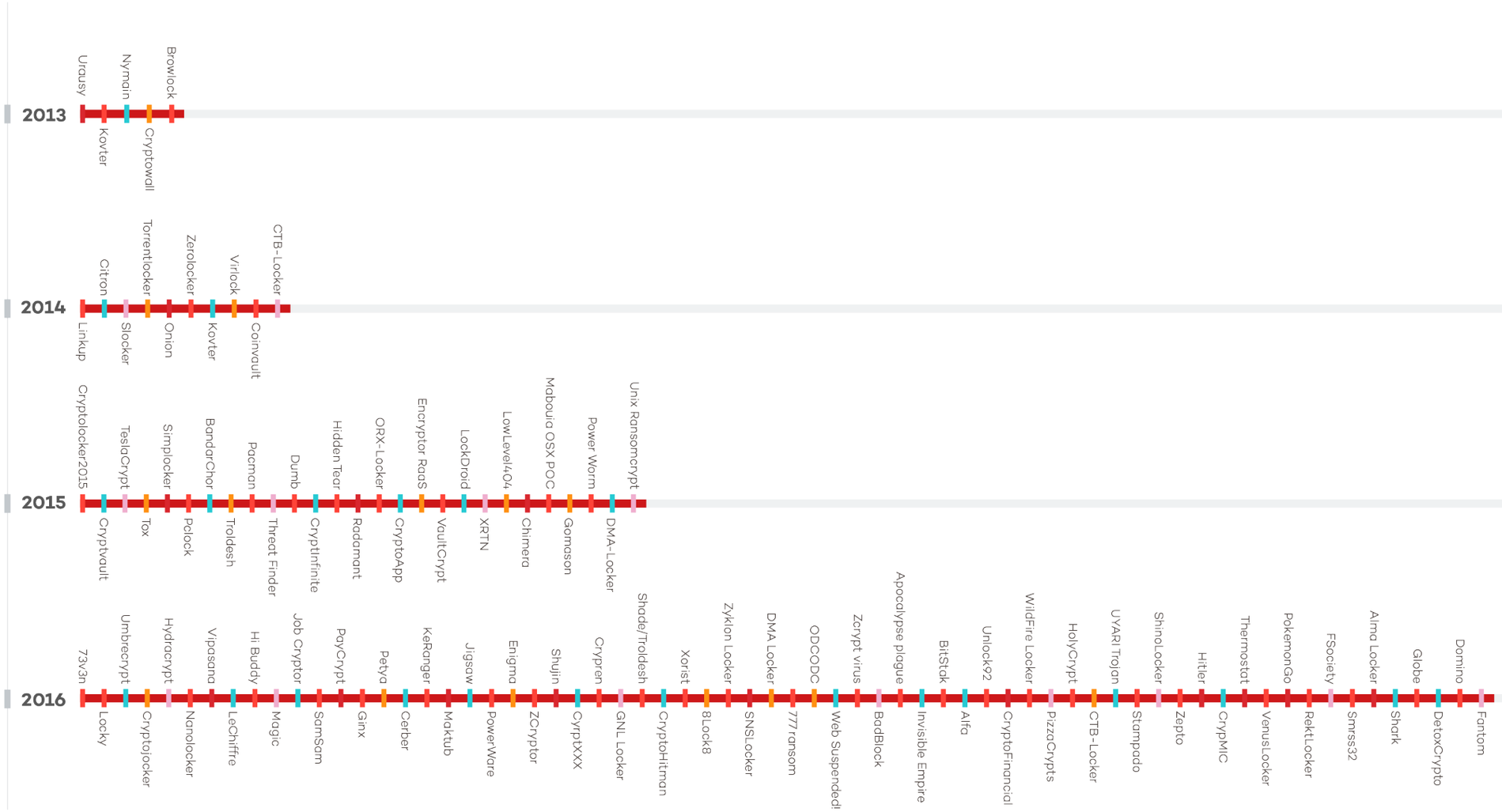
Are we living through a cyber-threat revolution? It would seem so. Malware is getting more and more sophisticated, and attack techniques are evolving. The target is no longer selected randomly — attacks are targeted, coordinated, and make use of different vectors.

The motive has changed, and cybercriminals are no longer seeking notoriety, but rather economic gains.



Hacking attacks are tending to veer toward a further professionalization of cybercrime. In the final months of 2016, we analyzed the specialization of black hats, both in the development of what could be called Ransom as a Service (RaaS) and the establishment of businesses offering DDDoS attack services, such as Vdos, whose directors had launched upwards of 150,000 attacks and raked in a profit of $618,000.

Last year, it became a billion dollar industry:



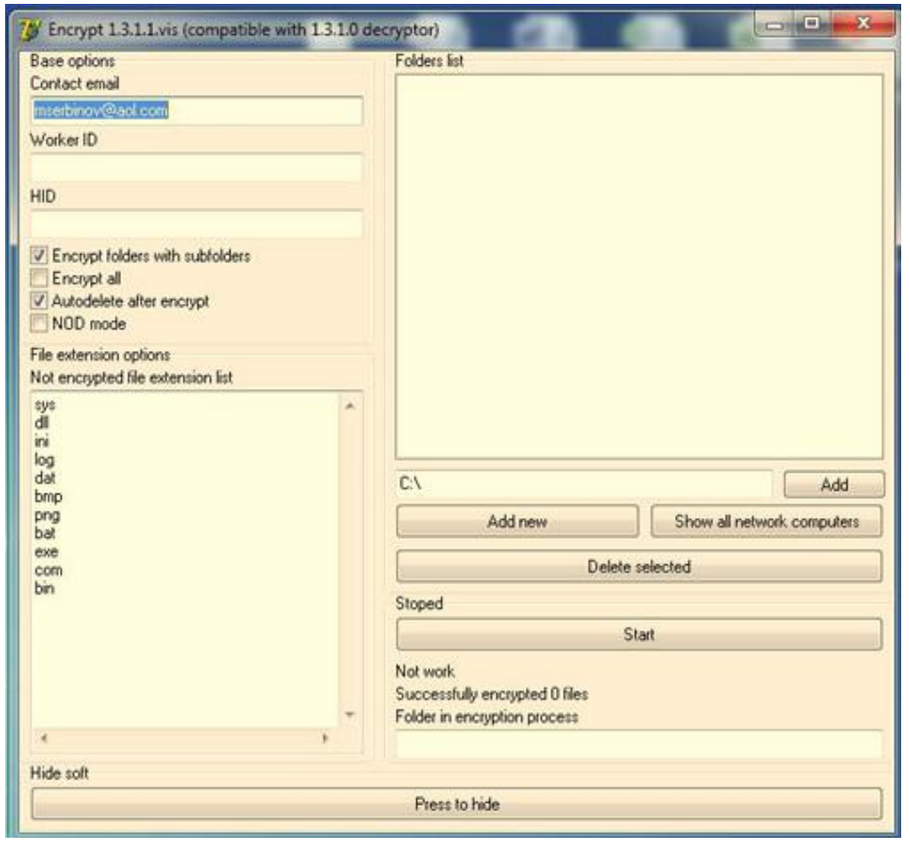
4. THE QUARTER AT A GLANCE

Ransomware

Ransomware attacks are still on the rise and will continue to be as long as victims keep paying hefty ransoms. There are estimates that over the course of 2016, cybercriminal groups specializing in ransomware earned a billion dollars. Concern is growing in all areas, and legislation is being passed to combat this type of crime. It is already officially a crime to deploy ransomware in California.

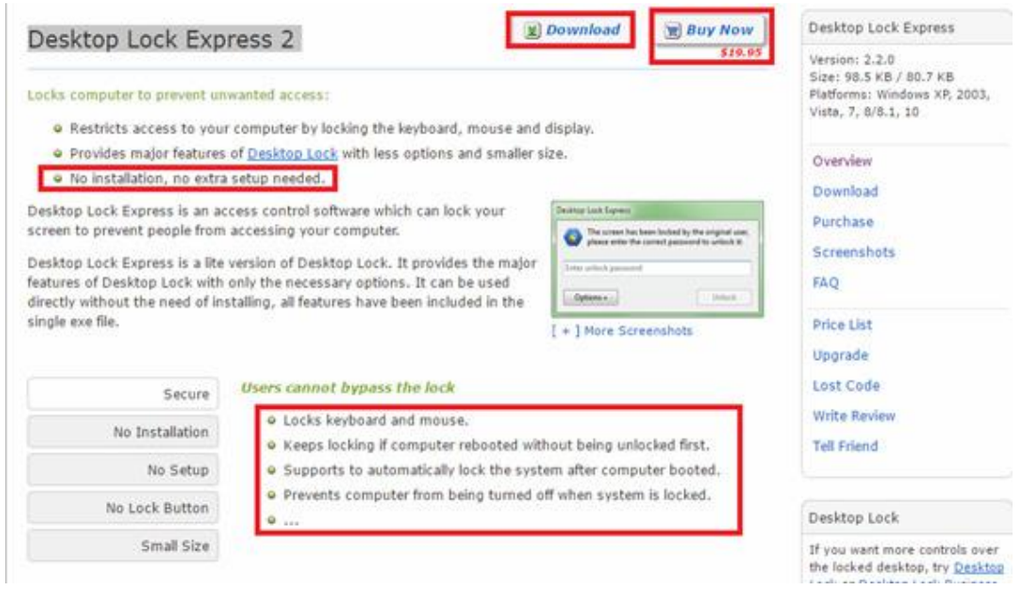
However, new legislation has done little to deter the ongoing attacks and the creation of new families of ransomware. One of these new families, Spora, began to be distributed at the beginning of the year, in this case seeking out its victims mainly in Russia.

Attacks targeting companies also continue to increase in frequency. In addition to very-well-known families of ransomware (Locky, Cerber, etc.), there are now more personalized kinds of attacks that adapt to their victims. One of them was discovered by PandaLabs this quarter: a ransomware with its own interface — dubbed WYSIWYE — that allows the offender to select the different folders whose contents will be encrypted and on which network computers, activate the autodelete feature, input the email address that the victim will have to contact for payment, etc .:



One of the most popular — and relatively straightforward — methods of penetrating a corporate network is through brute-force attacks using RDP, the popular Remote Desktop application that comes with Windows. Attackers are scouring the Internet for computers that have this feature activated, and once they find a potential victim they launch a brute force attack until they get the correct credentials. Once inside, they have free reign to do as they please on the system.

During these first months of 2017, we have seen quite a few cases of attackers of Russian origin. All of them follow a similar pattern: once they access the computer via RDP, they install bitcoin mining software as a method to obtain an added profit, and then either encrypt files or block access to the computer. They do not always use malware for this — for example, in one of the cases we analyzed, they used the commercial application "Desktop Lock Express 2" to lock the computer:



We also witnessed an especially insidious ransomware known as Popcorn Time. The novelty here lies in the morbid way that it propagates, as it aims for its victims to collaborate with cybercriminals to infect new users. Aside from demanding payment of 1 bitcoin (about 800 euros) for returning access to the user's encrypted files, it offers the possibility to recover them for free if he or she contributes to its propagation. It spread very much like a meme in the way users were meant to share it with their contacts.

The immediate consequences of a ransomware attack are clear: you lose access to your files. However, cases of digital hijacking can go far beyond this, as verified by customers of a hotel in Austria. Cybercriminals remotely blocked all the hotel's electronic keycard readers, making it impossible for lodgers to enter their rooms. This happened in the opening week of the season, with 180 clients holding reservations. The people in charge of the hotel decided to pay the €1,500 and thus regain control of their systems.

Cybercrime

The business of cybercrime is more professionalized than ever, which means that there are highly specialized groups in every corner of it: the creation of malware and exploits, distribution of malware, information theft, money laundering, etc. We can see a clear example with RDPatcher, an attack discovered by PandaLabs whose purpose is to prepare the victim's computer to be rented to the highest bidder on the dark web. Once they've infiltrated the computer, the attackers proceed to create a full profile of it, collecting all types of hardware data, installed software, security solution, connection speed, web pages visited, etc. It is then put on the black market to be purchased and conscripted for a botnet.

The ingenuity of the cybercriminals appears to have no end. In one case discovered by PandaLabs, we saw how attackers avoided detection by using "goodware" to perpetrate their attacks. After entering the computer's system, the attackers

left a backdoor open with the help of “Sticky keys” so as to enter the system without having to install malware.

DDos attacks also deserve to be mentioned. In the second half of 2016 there were several high-profile attacks of this type, and in this quarter we have seen much of the same, although these latter have not been quite so brutal in their nature. Just as the year began, for example, Lloyds customers had trouble accessing their accounts as a result of a DDoS attack.

In January, Italian state police disbanded a cyber espionage ring called Eye Pyramid, created by two Italian siblings, whose mission was ostensibly to compromise institutions and public administrations, professional studios, entrepreneurs, and politicians. The perpetrators accessed their victims’ confidential information by installing a virus on their computers, stealing sensitive financial data and confidential homeland security information. Those affected included former Prime Ministers Matteo Renzi and Mario Monti, as well as European Central Bank President Mario Draghi, among others, including mayors, cardinals, regional presidents, economists, businessmen and police commissioners.

The hacking of social media accounts is now commonplace, and one of the most striking cases of this quarter happened in January when the official Twitter account of the New York Times was compromised. As soon as they regained control, they deleted the tweets the attackers had posted:

This is an example of one of the tweets that was posted from the compromised account, claiming that Russia was about to launch an attack against the US:

The same group is known for having hacked other business accounts, such as those of Netflix and Marvel.

Data theft has also figured prominently in these past months. Sanrio, the company that owns "Hello Kitty", had the personal data of 3.3 million of its customers stolen from them, including such information as the customer's first and last name, user name, date of birth, security questions for password recovery, etc.

We analyzed cases that were somewhat ironic, such as that of Cellebrite, an Israeli company that facilitates the hacking of telephones — more specifically the extraction of data from them — which was itself hacked and robbed of 900GB of data. This information contained customer data, databases, and technical information on the company's products.

Even Apple has been the object of cybercrime in the first part of this year. A group of cybercriminals named "Turkish Crime Family" blackmailed the company, demanding a ransom or the hackers would remotely wipe data from iPhones, iPads and Macs, affecting 250 million users. While this group was allegedly in possession of valid user credentials, Apple denies that it had been compromised, chalking up the problem to the re-use of credentials and hacking of third-party sites. Of course, the technological giant refused to give in to the blackmail attempt.

Mobile Devices

While the amount of new malware created for mobile devices is still much lower than what we see on PCs, malware for mobiles follow the same patterns. Ransomware, for example, is a technique that carries over perfectly to mobile devices and is givin cybercriminals excellent results. A new malware for Android, known as "Charger", steals contacts and SMS messages before blocking the terminal, threatening to sell parts of your information on the black market every 30 minutes if the ransom is not paid. The requested ransom is 0.2 bitcoins.

Internet of Things (IoT)

For some time now, a majority of buildings have been equipped with smart meters to record the electrical consumption of homes and offices. Setting aside the potential effects these meters could have on the electricity bill (some consumer associations have already denounced possible fraudulent activity), the fact is that the widespread use of them carries some lesser known security risks.

As the researcher Netanel Rubin explained during the last edition of the Chaos Communications Congress held in Hamburg, Germany, smart meters pose a risk on several fronts. First, as all household and office consumption data is recorded and sent to the power company, an attacker with control of the device could view the information and use it for malicious purposes. For example, it would be extremely useful for a burglar to know at what times of the day a house or office is empty. They could even find out what valuable devices they will have at their fingertips before they break into the house, as every electronic device leaves a unique imprint on the power grid.

Another increasingly common device is the Smart TV. Some use versions of Android as an operating system, which has its advantages but also its drawbacks, as revealed by the American developer Darren Cauthon when he published on Twitter that the television of a family member had been the target of an attack. According to Cauthon, it all happened after the victim installed an application to watch movies on the internet, apparently from a third party site.

The TV was an LG model manufactured in 2014, which ran on Google TV, a version of Android specific to televisions. Once the device was infected, the malicious software demanded 500 dollars for code to unlock the screen, using a simulated notice from the US Department of Justice.

There are, however, far more dangerous attacks that hint at what awaits us in this area. In February, during the European Broadcasting Union Media Cyber Security Seminar, an exploit created by security consultant Rafael Scheel was demonstrated which allowed him to take control of a Smart TV without physical access to it, sending the attack through the DTT signal.

Robots and Personal Assistants

The “fourth industrial revolution” is just around the corner. A recent report from the World Economic Forum has put some numbers on the age-old debate: between now and 2020, 7.1 million jobs will disappear from advanced countries, and 2.1

million will be created. In other words, 5 million jobs will be lost permanently.

Another recent report, in this case coming from the Organization for the Cooperation of Economic Development (OCED) has singled out Spain, Austria, and Germany as the countries that will have the greatest impact on the robot revolution. Specifically, this phenomenon will make it so that 12% of workers in those three countries will be replaced by machines, compared with an average of 9 % in the rest of OCED member states.

Based on this data, the European Parliament has elaborated a set of regulations for the relation between robots, citizens, and businesses. This proposed legal framework is now being debated by the European Commission, who will have the final say on the extent of the implementation of robots in society. The goal is to minimize the negative impacts that could result from such an implementation.

In February, Google Homes all over the US were suddenly awakened by a Super Bowl ad for the company's virtual assistant when someone on the screen uttered the magic words, "OK, Google." It turns out that the Google Home's knack for tuning in on the fringes of conversations, patiently waiting for a voice command to summon it, makes it the perfect device for eavesdropping. This skill, paired with the virtual assistant's ability to store audio files, has even been used in the investigation of crimes. The police from a US town, for example, asked Amazon for access to the information of an Amazon Echo, as it could have stored information that would be useful to an ongoing investigation.

Cyberwarfare

More than ever before, cyberattacks and politics are becoming intertwined in a tight relationship. In the wake of last year's elections in the US, accusations against Russia with regard to cyberattacks began to pile up, and eventually led to sanctions. Before he left office, Obama accused the Russians of orchestrating cyberattacks to damage Hillary Clinton's campaign in favor of Donald Trump and announced the decision to expel 35 Russian diplomats and close two Russian-owned compounds.

All this finger pointing has had repercussions in other countries of the world as well. In France, for example, they have ruled out the use of electronic voting by their citizens residing abroad in the face of the "extremely high" risk of cyberattacks. In the Netherlands, they have gone even further, announcing that they would hand-check the votes on election

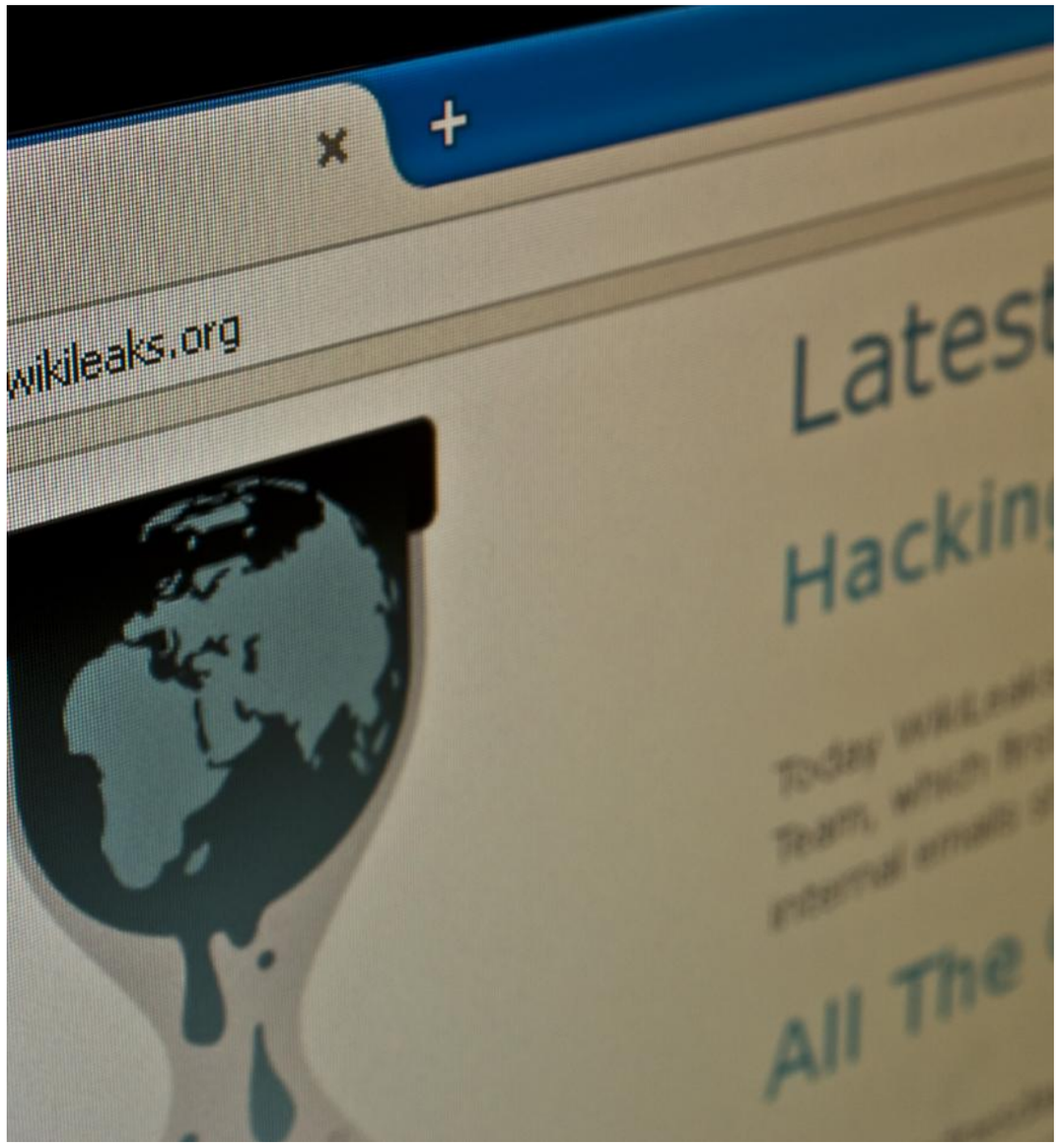
night and report the results by phone to avoid the risk of a possible cyberattack. The announcement followed a security expert's warning that the software used at polling stations was vulnerable.

In February, the Netherlands submitted a proposal to NATO to forge an international cyberdefense alliance to deal with the growing threat of cyberattacks, which would have capabilities in defense, enforcement, and measured responses to attacks.

In March, Chancellor Angela Merkel stated that protecting German infrastructures from cyberattacks was one of her country's top priorities in security. Shortly thereafter, it became known that the German army was forming its own cyber-command center to reinforce its online defenses. The new center will start out with 260 employees, a number that will in theory grow to become 14,500 in the year 2021.

But if there's been one event in the world of cyberwarfare and cyberespionage that should be singled out for the year so far, it would be the CIA/Wikileaks case. On March 7, Wikileaks began publishing a series of documents under the title "Vault 7", containing technical details and tools used by the CIA to break into smartphones, computers, and even Smart TVs.

Wikileaks is still publishing the documents on a section of its website. The sheer quantity of tools and techniques is astonishing. The documents leave little room for doubt that the CIA has at its disposal a vast cyber-arsenal of espionage tools and can spy on whomever it likes. Also true is that the agency has now lost its complete control of said tools. The good news is that the knowledge can be used to bolster your own defenses and better protect yourself against these kinds of attacks. The bad news: any other threat actor can now take advantage of what's been published to use it for his or her own malicious purposes, learning the same tactics developed by the CIA to violate the privacy of ordinary citizens.



4. CONCLUSION

4 Conclusion

Wikileaks will continue to publish information in Vault 7, and we can be sure to analyze new findings in our next report.

We should stay alert to the evolution of the Internet of Things, which from a security standpoint leaves a lot to be desired.

Ransomware attacks will remain in the lead in terms of attack numbers, and as long as there remains a percentage of victims willing to pay the ransom and security forces are unable to track the money through bitcoin, this trend will not change.

We'll keep a close eye on corporate attacks, and on the increasingly frequent use (and abuse) of legitimate, non-malicious software tools that attackers are using to infiltrate corporate networks and steal information, all the while attempting to slip under the radar of detection systems.

Working closely with PandaLabs, we'll be sure to keep you informed about any news from the world of cybersecurity through our Media Center, and we'll see you in three months to analyze the events of the second quarter of 2017.

5. ABOUT PANDALABS

5 About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory, and malware treatment center where:

- PandaLabs creates real and uninterrupted time 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.

panda

pandalabs