November, 2017

PandaLabs Annual Report 2017

panda

Introduction.

Luis Corrons
Technical Director of PandaLabs

In the Heart of the Company.

In a cybersecurity company, the laboratory is the brain. It is from here that threat research activities and cyberdefense techniques are coordinated.

We carry the weight of our clients' security on our shoulders. If any of them happens to get infected, we have failed. The good news is that the **number of malware incidents that have escalated at PandaLabs trends to zero**.

One way of measuring whether we're truly doing our jobs is to have an independent firm analyze and compare our solutions. The most thorough test today is surely the Real World test by AV-Comparatives. This test awards the highest prize for threat detection, and they gave it to us:

What is the Secret?

In this report's conclusion, I go a little more into detail, but ultimately the secret is "forgetting about" malware. If we focus on fighting malware, the battle is lost before it has begun.

Using Machine Learning technology to protect our customers means that PandaLabs technicians are more comfortable when it comes time to investigate attacks.

That is very bad news for the attackers. Our Threat Hunting team analyzes and hunts down anomalous behavior patterns, no matter how innocent they may seem at first glance. And they have discovered numerous new attacks, some of which we describe in this report.

The combination of advanced technologies and managed services allows us to classify 100% of active processes and know what is happening while it is happening. Unlimited visibility and absolute control reduces the impact of any threat to zero.

Evolution of Attacks.

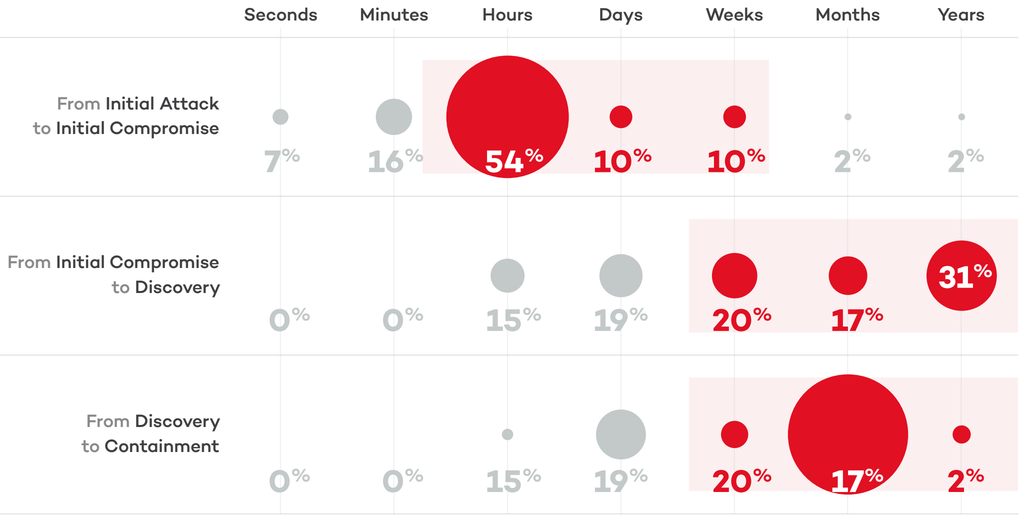
panda

There are **more heists at places of business and bank branches than ever before in history**, with the oddity that attackers can now be thousands of kilometers away, having never physically approached their victims.

In fact, it's not necessary for the attacked device to have access to the data or resources the cybercriminals are after, since it's only being used as a launching point.

They will use lateral movements through the corporate network until they hit upon the data that they're interested in, or the system they wish to sabotage.

And so, these new techniques for penetrating defenses and concealing malware are allowing threats to remain on corporate networks for long periods undetected.



Source: DBIR 2016

Now.

Cybercrime is an attractive and profitable business. Attackers are making use of more, and better, digital and economic resources than ever before, allowing them to develop attacks that are increasingly sophisticated.

Almost anyone can launch an advanced attack thanks to the democratization of technology, the black market, and open source tools. As a consequence, it must be assumed that all companies could become the target of an advanced attack to start working on effective security policies and actions. Having the mechanisms to detect, block and remedy any type of advanced threat can safeguard the coffers and the reputation of organizations.

Almost all of these crimes have an economic basis: it's all for money. Attackers are drawn to profitable victims. That is why we must take all possible measures to complicate and hinder their ability to reach their target, and thus cut into their productivity.

In most cases, when an attack becomes complex and the attackers fail to reach their final goal, they will choose to go to another victim who offers them a better return on their investment.

To give an idea of the complexity behind these attacks, hacking techniques have been used in 62% of security breaches taking place in companies. In fact, in **only 51% of cases did attackers use malware**. In the rest, they used other tools against which most companies are not protected.

In case of falling victim to a cyberattack, it is very important to have forensic information about it to know what you're up against and take the necessary measures.

It's also helpful to know where the attack came from, what techniques it used, what movements it made, what actions it took, how it evaded defenses, etc.

Other Motivating Factors.

While most attacks are financially motivated, there are plenty of outliers whose objective is quite different.

A clear case that we have seen this year was the **Petya/GoldenEye** attack targeting companies with offices in Ukraine. The motive was clearly political, and the Ukrainian government itself openly accused the Russian government of being behind it.

But this is not an isolated case. We are in the middle of an arms race in cyberspace, nations are creating cyber commands not only for offensives, but also as a key initiative for reinforcing defenses against external threats.

For example, President Obama's cybersecurity plan urged his successor to train 100,000 new computer security experts by 2020. In fact, the goal for 2018 is to reach **133 teams for Cyber Mission Force**.

All countries have included this priority in their militaries as another operative unit. Indeed, these units quite often have the largest budgets at their disposal.

Global Investment in Cyber-Forces

COUNTRY	ANNUAL BUDGET	NUMBER OF CYBER-TROOPS
🇺🇸	$7.000M	9.000
🇨🇳	$1.500M	20.000
🇬🇧	$450M	2.000
🇷🇺	$300M	1.000
🇩🇪	$250M	1.000
🇰🇵	$200M	4.000

Source: RBTH

Trends.

Knowing Your Enemy.

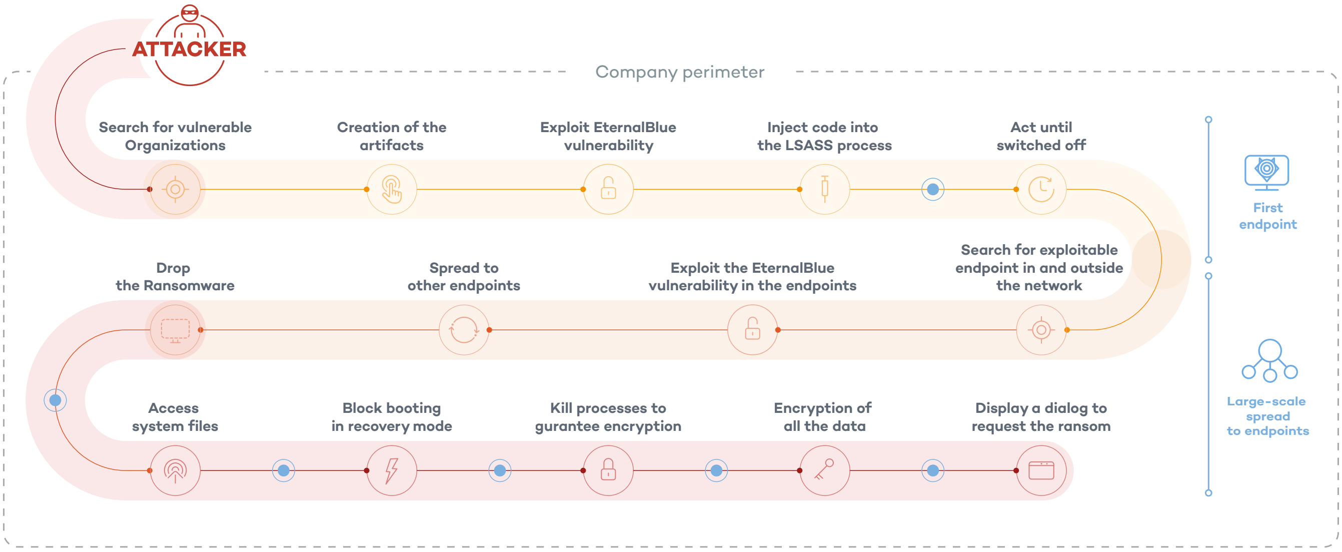
New attack vectors are helping to create increasingly complex offensives. Cyberattackers are creating new tools to take advantage of exploits. To complicate matters, they no longer rely on human interaction for the success of their attacks.

This implies a careful study of their victims, an armed reaction to exploit very specific security holes, and an automatic and exponential distribution of malware without having to resort to human intervention.

They interact in real time with the network and security solutions of the victim, adapting to their environment to achieve their goal.

It is crucial to know what we are up against.

At Panda Security, we have created this Cyber-Kill Chain to better visualize things from the attackers' perspective, revealing the different steps they take from the first stages to achieving the final objective:


ATTACKER
Company perimeter
Search for vulnerable Organizations
Creation of the artifacts
Exploit EternalBlue vulnerability
Inject code into the LSASS process
Act until switched off
First endpoint
Search for exploitable endpoint in and outside the network
Exploit the EternalBlue vulnerability in the endpoints
Spread to other endpoints
Drop the Ransomware
Large-scale spread to endpoints
Access system files
Block booting in recovery mode
Kill processes to gurantee encryption
Encryption of all the data
Display a dialog to request the ransom

● Points at which Adaptive Defense blocks the attack

This sequence is an excellent tool to understand how organizations can significantly increase their defense capabilities by detecting and blocking threats at each stage of the attack's life cycle.

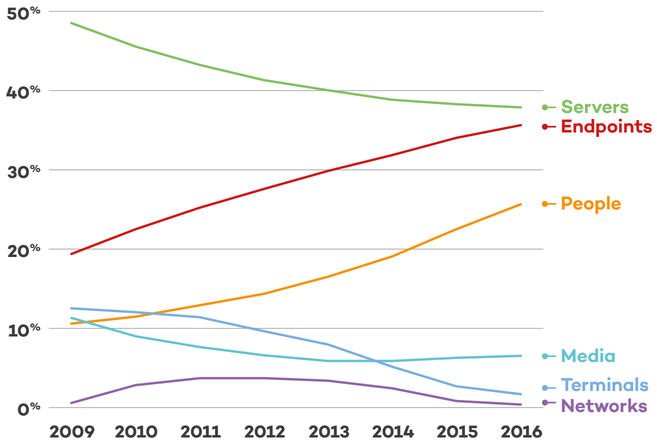
The Cyber-Kill Chain shows that while opponents must progress fully through all phases of the chain to succeed, all we need to do is to "simply" stop the chain at any step in the process to break the attack.

In this **document**, we provide a detailed explanation of each of the sections, and you can also see our **video**.

The Endpoint is the Target.

There is a critical point that is worth highlighting when we talk about the evolution of attacks. In many cases, security solution vendors themselves spend a lot of time talking about the perimeter, the Internet of Things, and other vectors that need protection, but the most important thing is often overlooked: the endpoint.

Why is it so important? If attackers are unable to reach the endpoint, they will be unable to access other targets, exfiltrate information, steal credentials, gather network data, or deploy new attacks. The trend is shown clearly by the following graph:



Source: Verizon Data Breach Investigations Report.

However, the majority of the security budget at companies is allocated to the protection of the perimeter, **neglecting the crucial part, the endpoint**.

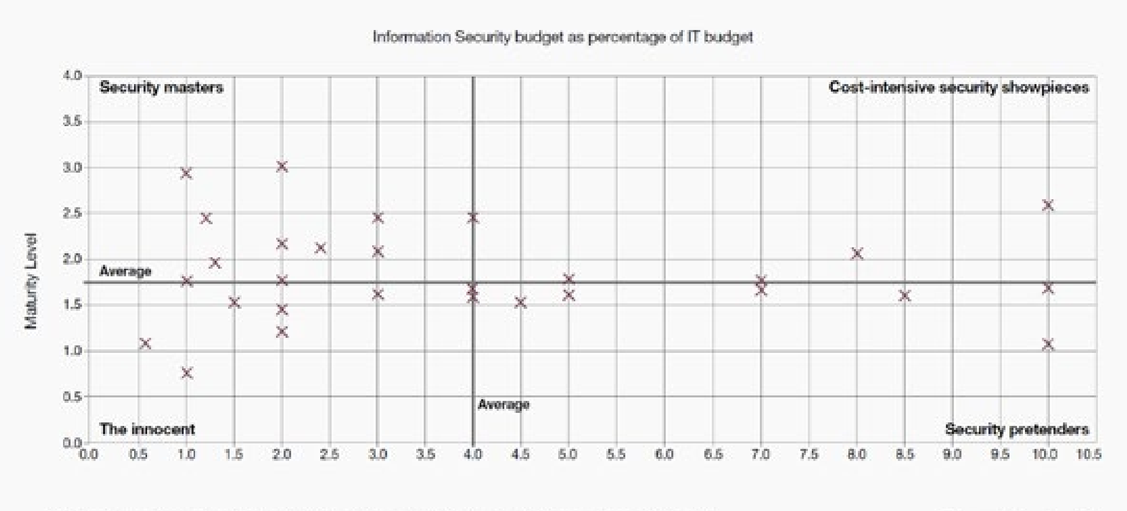
This does not happen out of ignorance or negligence. In the past, focusing on the perimeter made sense. Within the corporate network, endpoints were basically secure, so the priority was bulking up defenses against external attacks, which had to pass through the perimeter.

PRODUCTS		SERVICES	
Perimeter	$11,9B	Consulting	$21B
Identity	$4,6B	Integration	$20B
Endpoints	$3,8B	SOC:	$20B
Web	$2,6B	• Prevention • Detection • Response	
Others	$11,0B		

Today the situation is radically different: the perimeter has blurred, mobility is the norm at any company, and corporate networks are much more exposed.

Attackers level their sights on individual computers, knowing that if they manage to reach just one of them, the probability of being able to carry out further actions before being detected is very high.

Therefore, it's a question of establishing priorities, and not of investing more but rather of where it is necessary to invest. This was demonstrated in this Capgemini study, in which the level of investment in security is compared with the level of actual protection of corporate assets:



x = Participants overall security maturity level in relation to its Information Security budget as percentage of IT budget

© Capgemini Consulting 2016

Figures.

One of the most obvious consequences of the professionalization of attacks is that the number of malware samples has multiplied exponentially. According to Verizon, up to **50% more in ransomware attacks alone**.

This is not only due to the fact that the number of attacks has increased, although that is also true. Mainly, it can be chalked up to the techniques used by cybercriminal.

More than 10 years ago, we published an article where we discussed this trend. In a retrospective analysis we looked at how, in 2002, the 10 most prevalent malware samples caused 40% of all infections, and in 2006 it dropped to 10%.

What is the situation in 2017?

Since all our solutions communicate with our cloud, we can obtain data to analyze whether this tendency has become more acute.

To calculate the figures, we have taken all the malware (PE files) that we had never seen before January 1, 2017. Through September 20, we had received queries for **15,107,232 different malware files**. And these are only the ones we've never seen before. The total number of malware created is much greater, since you have to add all types of files (scripts, documents, etc.), as well as those that, although newly created, have not yet attempted to infect our clients. The actual figure would be a total of about **75 million samples – about 285,000 samples of malware per day**.

These are the 10 malware samples that were most consulted in our cloud:

POS.	SEEN	TYPE	NAME
1	15/8/17	Trj/HackCCleaner.A	HackCCleaner
2	5/1/17	Trj/CerberCrypto.A	Cerber
3	15/5/17	Trj/RansomCrypt.I	WannaCry
4	15/8/17	Trj/HackCCleaner.A	HackCCleaner
5	17/5/17	Trj/Agent.SM	Downloader
6	24/2/17	Trj/Genetic.gen	Bot
7	15/5/17	Trj/RansomCrypt.I	WannaCry
8	12/5/17	Trj/RansomCrypt.K	WannaCry
9	15/5/17	Trj/Agent.PS	Downloader
10	12/5/17	Trj/RansomCrypt.K	WannaCry

It makes sense that within this top 10 we find files related to the most serious cases occurring during this year, such as WannaCry (3rd, 7th, 9th and 10th position) and the backdoored version of CCleaner (1st and 4th position) . The rest are downloaders (Trojans that are used as an intermediary for installing all types of malware) and a bot.

And of all these 15,107,232 samples of malware, how many have been seen only one time? **99.10%, or 14,972,010 samples**.

If we look at the numbers from the other end, we see that indeed an insignificant part of all malware is truly widespread. We have only seen **989 malware files on more than 1,000 computers, 0.01%**.

This confirms what we already knew: with a few exceptions (like WannaCry or HackCCleaner), most malware changes with every new infection, so each sample has a very limited distribution.

By grouping it by families or types, it comes as no surprise that ransomware stands out from the crowd, as it is one of the most profitable attacks and therefore incredibly popular (and more so with every year that goes by).

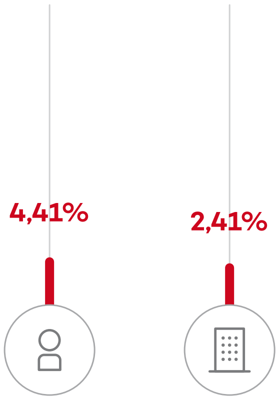
In any case, if we want to know what infection risks we are facing, the total number of new malware samples is not as relevant as the frequency with which we may be exposed to it. To calculate this figure, we measure only malware infection attempts not detected either by signatures or heuristics, including malware attacks, fileless attacks, or those that abuse legitimate system tools (something increasingly common in corporate environments, as we saw in the case of Goldeneye/Petya in June).

To measure this, we use data gathered by several of our own technologies, encompassing what we call "Contextual Intelligence", which allows us to reveal patterns of malicious behavior and to generate advanced cyber defense actions against known and unknown threats.

We then proceed to analyze the attack data we have obtained.

Not all of us have the same protection measures, since a home computer or a small company usually has more basic protections (putting them at greater risk), while medium and large companies have many more resources dedicated to data protection.

In this report, we will only account for attacks that make it past every layer of protection, are not detected, and are stopped at the last minute, just before compromising the computer. Entities which set aside more resources for security should receive fewer of these attacks, and indeed the figures show us just that. **While home users and small businesses make up for 4.41% of attacks, in medium and large companies the figure drops to 2.41%**.



Although this data can give companies peace of mind, we should not allow ourselves to be fooled: attackers do not need to attack all the computers in a corporate network to cause damage. In fact, they will attack the minimum number of possible computers to go unnoticed, and thus minimize the risk of detection and achieve their goal.

Geographical Distribution of Attacks.

We have calculated the percentage of machines attacked by country: the greater the percentage, the more likely it is to fall victim to new threats when using a computer in that country:

Iran	11,96%
Algeria	11,81%
India	10,96%
Egypt	7,89%
Bolivia	6,88%
Dominican Rep.	6,88%
Pakistan	6,43%
South Africa	6,30%
Malaysia	5,99%
Bangladesh	4,71%
Thailand	4,59%
Indonesia	4,48%
Morocco	4,28%
Moldavia	4,22%
Brazil	4,22%
Armenia	4,14%
El Salvador	3,98%
Paraguay	3,88%
Honduras	3,82%
Kazakhstan	3,70%
Ukraine	3,63%
Venezuela	3,55%
Uruguay	3,50%
China	3,42%
Tunisia	3,42%
Guatemala	3,32%
Filipinas	3,29%
Saudi Arabia	3,28%
Belorussia	3,25%
Arab Emirates	3,22%
Chile	2,98%
Colombia	2,89%
Russia	2,86%
Vietnam	2,82%
Ecuador	2,66%
Cyprus	2,56%
Mexico	2,39%
Georgia	2,34%
Macedonia	2,14%
Brunei	2,14%
Taiwan	2,08%
Peru	2,07%
Singapore	1,85%
Bosnia Herzegovina	1,82%
Costa Rica	1,82%
Bulgaria	1,81%
Turkey	1,79%
Italia	1,71%
Panama	1,68%
Argentina	1,63%
Portugal	1,58%
South Korea	1,53%
Serbia	1,51%
Puerto Rico	1,44%
Lithuania	1,42%
Latvia	1,39%
UK	1,33%
Croatia	1,30%
Ireland	1,26%
Slovakia	1,16%
Spain	1,14%
Estonia	1,09%
Germany	1,06%
Romania	1,03%
Austria	1,01%
Israel	0,99%
USA	0,99%
Norway	0,94%
Poland	0,94%
France	0,93%
Australia	0,91%
Czech Republic	0,88%
Hong Kong	0,86%
Hungary	0,82%
New Zealand	0,79%
Switzerland	0,78%
Malta	0,77%
Sweden	0,75%
Denmark	0,67%
Greece	0,64%
Japan	0,64%
Slovenia	0,62%
Canada	0,60%
Belgium	0,54%
Netherlands	0,53%
Finland	0,51%

2017 at a Glance.

Tracking the biggest attacks recorded throughout 2017 is a bit like riding a roller coaster: you can't quite see what's ahead, and you won't know how high the ups will be or how low the dips will be until you get to them. But in spite of all the not knowing, one thing is for sure: you've never seen anything like it, and you will not easily forget it.

Equifax, CCleaner, Sabre, WPA2, Vault7, CIA, KRACK, NSA, Election Hacking ... these are some of the key players analyzed below. They're the subjects of massive infections, data thefts, ransomware attacks, hacked applications, cyberwarfare, targeted attacks against large corporations, and vulnerabilities affecting billions of devices.

But there are two attacks that stand out for the impact and damage caused: WannaCry and GoldenEye/Petya.

WannaCry appeared in May, wreaking havoc on corporate networks and spreading around the world, proving to be one of the most serious attacks in history. Although by number of victims and speed of propagation we have seen attacks in the past much more powerful (like Blaster or SQLSlammer, to give just two examples), the fact is that the damage caused by previous attacks was collateral to their propagation. However, as a ransomware with network worm functionality, every computer WannaCry infected would have its data locked and encrypted.

Luis Corrons, Technical Director of PandaLabs, gave a webinar analyzing what happened in depth and considering the measures that must be taken to protect against other attacks of this type. You can listen to it here.

Goldeneye/NotPetya was the second most impactful attack this year, as a sort of **aftershock to the earthquake that was WannaCry**. Although its victims were initially limited to a specific geographical area (Ukraine), it ended up affecting businesses in more than 60 countries.

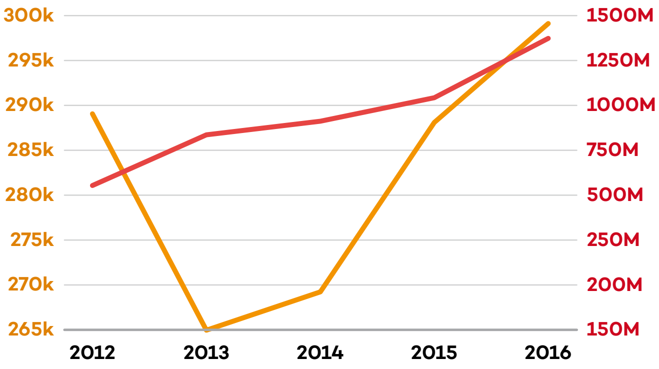
The carefully planned attack was carried out through an accounting application that is very popular among companies in Ukraine, M.E.Doc. The attackers compromised the update server of this software, so that all computers with M.E.Doc installed could be infected automatically and all at the same time.

In addition to encrypting the files, if the user who has the session started on the computer has administrator permissions, the malware goes to the MBR (Master Boot Record) of the hard disk. At first it seemed to be a ransomware in the style of WannaCry, but after analyzing it thoroughly it became clear that its authors really did not intend to allow any data to be recovered. Days later, the Ukrainian government openly accused Russia of being behind the attack.

Luis Corrons reveals the keys to this attack and its authors in a webinar that you can listen to it here.

Cybercrime.

According to the "2016 Internet Crime Report" published by the FBI Internet Crime Complaint Center (IC3), **losses caused by cybercrime increased by 24%, exceeding $1.3 billion**. It should be noted that this accounts for only the amount reported by US victims to the IC3, which estimates that this only accounts for 15% of incidents, so the real total figure (US only) could reach up **$9 billion of losses in 2016 alone**.



The most coveted exploits for launching attacks are known as "zero-day", as they are unknown to the manufacturer of the affected software and allow attackers to compromise users despite all their software being up to date.

In April, a zero-day vulnerability was discovered that affected several versions of Microsoft Word, and it has since become known that at least since January of this year it had been exploited by attackers. That same month, Microsoft released the corresponding update to protect its Office users.

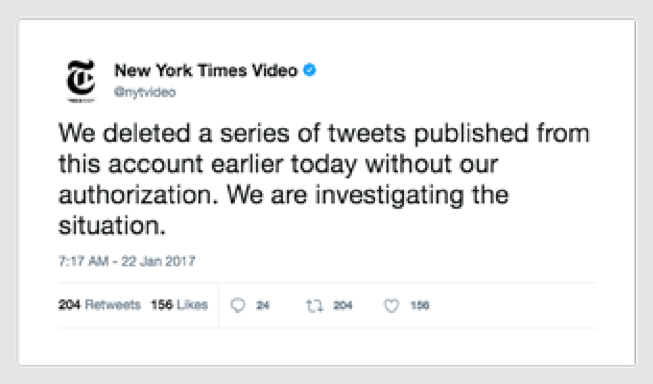
RDPPatcher showcases the increasing professionalization of cybercrime. This attack, discovered by PandaLabs, prepares its victim's computer to be rented out to the highest bidder on the black market.

Cybercriminals do their best to avoid being detected, and one of the most effective methods to achieve this is to not use malware. Because of this, malwareless attacks have become popular. In a case discovered by PandaLabs, attackers leave a backdoor open on the computer they've infiltrated, which they will later use to access the device without having to install malware, and using "**Sticky keys**".

In the second half of 2016 we saw several **DDoS attacks** that received a good deal of press, and in 2017 have seen more of the same, although this year they were not so brutal. For example, Lloyds customers had trouble accessing their accounts online as a result of a DDoS attack that saturated their servers.

Italian state police disbanded a cyberespionage ring, dubbed Eye Pyramid, created by two Italian siblings in January to manipulate institutions and public administrations, businesses, businessmen, and politicians.

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



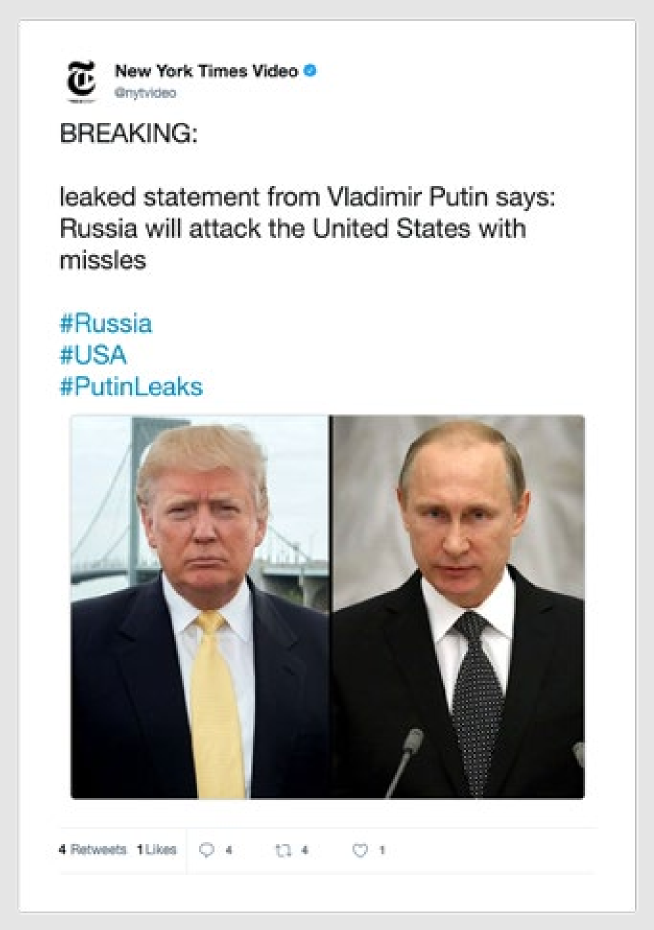
New York Times Video
@nytvideo

We deleted a series of tweets published from this account earlier today without our authorization. We are investigating the situation.

7:17 AM - 22 Jan 2017

204 Retweets 156 Likes 24 204 156

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



New York Times Video
@nytvideo

BREAKING:

leaked statement from Vladimir Putin says: Russia will attack the United States with missles

#Russia
#USA
#PutinLeaks

4 Retweets 1 Likes 4 4 1

The same group hacked other company accounts, such as those of Netflix and Marvel.

A group of cybercriminals known as the "**Turkish Crime Family**" blackmailed Apple, seeking a ransom under the threat of erasing data on iPhones, iPads and Macs belonging to 250 million users. Apple refused to give in to blackmail.

Corporate Data Thefts.

Data thefts have also made headlines throughout the year. Perhaps the most ironic story of the year: Cellebrite, an Israeli company that offers phone hacking services -specifically extracting data from mobiles- was hacked, and 900GB of their data was stolen, including customer data, databases, and technical information about the company's products.

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

Another type of security incident with no attackers directly involved are those in which, due to an error or negligence, data that should be protected is exposed to the general public. This happened in the USA, when marketing firms hired by the Republican Party left **data related to 198 million registered voters** accessible to the world, accounting for almost all of its registered voters.

Dow Jones accidentally allowed access to 2 million of its customers' data, via Amazon's cloud service, due to a configuration error. Among the compromised data could be found names, email addresses, and even credit card numbers.

22 people were arrested in China for trafficking in Apple customer data. All evidence pointed to an inside job, as some of the detainees worked for companies subcontracted by Apple and had access to the trafficked data.

HBO fell victim to several cyberattacks this year. In one of them, company servers were compromised and complete episodes of not-yet-released series were stolen, as well as internal corporate.

InterContinental Hotels Group (IHG) fell victim to an attack in which its clients' data was stolen. Although the company said in February that the attack had only affected about a dozen hotels, it has since become known that they had **infected POS terminals in more than 1,000 of their establishments**. Among the different hotel brands owned by the group are Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels, and Crowne Plaza.

Sabre Corporation is a North American company that manages reservations for 100,000 hotels and more than 70 airlines around the world. An attacker obtained credentials to access one of the company's reservation systems, accessing payment information and booking details.

This particular system manages the reservations of individuals and travel agencies for 35,000 hotels and accommodation establishments. **They were compromised from August 10, 2016 to March 9, 2017, 7 months**.

Among some of the hotel chains affected by the Sabre attack were Four Season Hotels & Resorts, Trump Hotels, Kimpton Hotels & Restaurants, Red Lion Hotels Corporation, Hard Rock Hotels and Loews Hotels.

Taringa, a popular social network in Latin America, suffered a security breach in which **information was extracted from more than 28 million users**, including usernames, emails and the MD5 hashes of passwords.

But the biggest security breach of the year — and the worst in history — would come a little later, when the credit reporting giant, **Equifax, was compromised**. Due to the nature of its services, the company possesses abundant amounts of highly confidential information on millions of people, including social security numbers.

The attack was carried out through a vulnerability in Apache Struts, present on one of the company's servers. The vulnerability was made public — along with the corresponding update that resolved it — on March 6. A few days later, the attackers hit the company's server, which was compromised until the end of July when the attack was discovered. **The data of about 200 million people was compromised**, 70% of them from the US and the rest from the UK and Canada. The list of affected countries was later extended to Argentina, Brazil, Uruguay, Peru, Paraguay, Ecuador and Chile.

To make matters worse, it was later revealed that three executives of the firm took advantage of the time between discovering the security breach and making it public to sell off their shares of the company for a value of $1.8 million. The security officer of the firm was fired, and just a month later Richard Smith, CEO of Equifax since 2005, announced that he was stepping down.

Trojan Horses.

After Goldeneye/Petya, the company **Netsarang** suffered an attack in which a file was introduced into versions of five of its programs (Xmanager Enterprise 5.0, Xmanager 5.0, Xshell 5.0, Xftp 5.0, and Xlpd 5.0) via a backdoor. The compromised file had a valid digital signature from the company, which means that the attackers had completely infiltrated their company at every level. Among the clients of this company are banks and energy companies.

The most notorious backdoored software case of the year was without a doubt that of **CCleaner**. Compromised versions were installed by more than 2 million users. The compromised software was waiting to receive orders, and apparently never got around to performing any malicious action. However, Cisco researchers discovered that the attackers had a list of the companies whose computers they wanted to compromise. These were 20 high-profile companies including Samsung, Cisco, Sony, Intel and Microsoft.

These three attacks indicate that a meticulous and extremely professional organization was behind them, leading one to believe that they were backed by governments. In fact, NATO itself declared that a state actor was behind the GoldenEye/Petya attack.

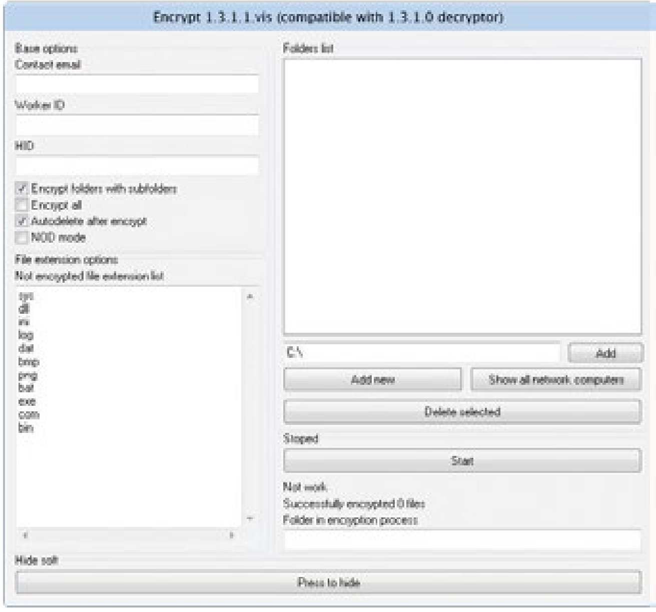
Global Impact of the Attacks

Ransomware.

Ransomware attacks are still on the rise, and this will continue to be the case as long as companies are willing to pay hefty ransoms for the return of their data.

In addition to the well-known families of ransomware (Locky, Cerberm etc.), there are special, more personalized versions for the kind of victims willing to pay.

One of them was discovered by PandaLabs, a ransomware with its own "user-friendly" interface, dubbed WYSIWYE, which allows the cybercriminal to configure the attack before it is launched:



Encrypt 1.3.1.1.vis (compatible with 1.3.1.0 decryptor)

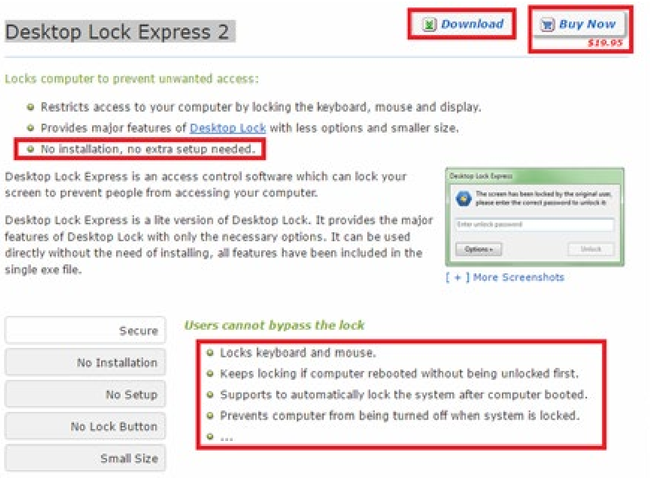
Base options
Contact email
Worker ID
HID
☑ Encrypt folders with subfolders
☐ Encrypt all
☑ Autodelete after encrypt
☐ NOD mode
File extension options
Not encypted file extension list
sys
dll
ini
log
dat
bmp
png
bat
exe
com
bin

Folders list
C:\
Stoped
Not work
Successfully encrypted 0 files
Folder in encryption process
Hide soft

One of the most popular — and relatively straightforward — methods of penetrating a corporate network is through brute-force attacks using the RDP (Remote Desktop Protocol) that comes with Windows. Attackers are scouring the Internet for computers that have it activated, and once they find a potential victim, they launch a brute-force attack until they find the correct credentials.

We have seen in the course of 2017 numerous attacks of this type, with attackers usually being of Russian origin, and all following a similar scheme: once they access the computer through the RDP, they install bitcoin mining software -as a sort of added benefit- 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 carry out the locking of the computer:



Locks computer to prevent unwanted access:

- Restricts access to your computer by locking the keyboard, mouse and display.
- Provides major features of Desktop Lock with less options and smaller size.
- No installation, no extra setup needed.

Desktop Lock Express is an access control software which can lock your screen to prevent people from accessing your computer.

Desktop Lock Express is a lite version of Desktop Lock. It provides the major features of Desktop Lock with only the necessary options. It can be used directly without the need of installing, all features have been included in the single exe file.

Users cannot bypass the lock

- Locks keyboard and mouse.
- Keeps locking if computer rebooted without being unlocked first.
- Supports to automatically lock the system after computer booted.
- Prevents computer from being turned off when system is locked.
- ...

The immediate consequences of a ransomware attack are clear: you lose access to your files. However, digital “kidnapping” cases can go far beyond this, something a hotel in Austria can attest to, which found its guests locked out of their rooms after cyberattackers disabled the keycard programming software.

Ransomware encrypted the data of 153 Linux servers belonging to the web hosting company Nayana, of South Korea. **The attackers demanded a ransom of $1.62 million**. The company negotiated with the criminals and lowered the figure to 1 million dollars, to be made in three payments.

Internet Of Things (IoT).

For years now there have been many warnings about the dangers regarding devices on the Internet of Things (IoT), largely because many such devices do not take security into account when designed.

Also, because they are simply devices without an Internet connection that do not pose a risk, but then become Internet enabled and as such are vulnerable to attacks.

It seems that these warnings are gradually being heeded and in the US a group of Democrat and Republican senators have come together to create legislation that partially addresses this situation. The idea is to require the manufacturers of products with an Internet connection to make them updatable (to fix security flaws), to stop them from having fixed passwords, and to prevent the sale of products with known security holes, among other measures.

Intelligent buildings.

Over the years many buildings have undergone changes such as the installation of ‘smart meters’ to monitor energy consumption in homes and offices. In addition to the possible negative effects on energy bills reported by consumer associations, there are other less known security concerns regarding the widespread use of such devices.

As the researcher Netanel Rubin explained during the recent Chaos Communications Congress in Hamburg, Germany, these meters represent a threat on various levels. Firstly, as they record all the data regarding consumption of energy in homes and offices in order to send them to the utilities, an attacker who took control of the device could see this information and exploit it maliciously.

They could, for example, see when the premises are empty in order to rob the place. Given that all electrical appliances leave a trace on the grid, they could even use the information to detect any valuable items that could be stolen once they have broken in.

Smart TV.

Another increasingly common device is the Smart TV. Some of these run Android operating systems, which has its pros and cons, as Darren Cauthon, an IT developer in the US noted on Twitter after the TV of a relative had been attacked. As Cauthon explained, it all happened after the victim installed an application to watch films on the Internet through a third-party site.

The TV was an LG model manufactured in 2014, which runs with Google TV, a version of Android specifically for televisions. Once the device had been infected, **the malicious software demanded a $500 ransom to unlock the screen** which simulated a notice from the US Department of Justice.

Similarly, many more dangerous attacks are also taking place, which would seem to indicate the shape of things to come in this area. In February, during the European Broadcasting Union Media Cyber Security Seminar, the exploit created by security consultant Rafael Scheel was revealed. This could allow an attacker to take control of a Smart TV without physical access to it, simply by launching the attack through the TDT signal.

Smart Cities.

In Australia, **55 traffic cameras** installed at traffic lights and speedtraps were compromised after a subcontractor connected an infected computer to the network to which they were connected.

On April 7, in Dallas, Texas, 156 emergency sirens went off in unison at 11:40 at night. Officials managed to switch them off some 40 minutes later, but only after bringing down the entire emergency system. It is still not known who was responsible for the attack.

The Car Industry.

There have been reports of a new vulnerability affecting cars, specifically Mazdas in this case. Yet unlike previous occasions, in order to compromise the car's IT system, an attacker would have to insert a USB drive while the engine is running in a specific mode.

While it's not surprising that cars and other vehicles can have an Internet connection and can consequently be attacked, there are other targets in this sector that would never occur to most of us. This is the case with carwashes. At the Black Hat conference in Las Vegas, researchers Billy Rios and Jonathan Butts revealed how they managed to hack automatic carwashes that are connected to the Internet, hijacking the system in such a way that they could physically attack the vehicle and its occupants.

Still in the automotive sector, Segways can also be hacked remotely, and completely controlled by an attacker. IOActive researcher Thomas Kilbride demonstrated different vulnerabilities and security issues. One of the most concerning is that Segways do not check the updates applied, so anyone could, at any given time, update the device with a malicious firmware that did whatever the attacker wanted.

Critical Infrastructure.

Dutch researcher Willem Westerhof has been analyzing the transformers used in solar panels to transform direct current into alternating current and to be able to supply it to the grid of one of the leading companies in this sector, SMA Solar Technologies.

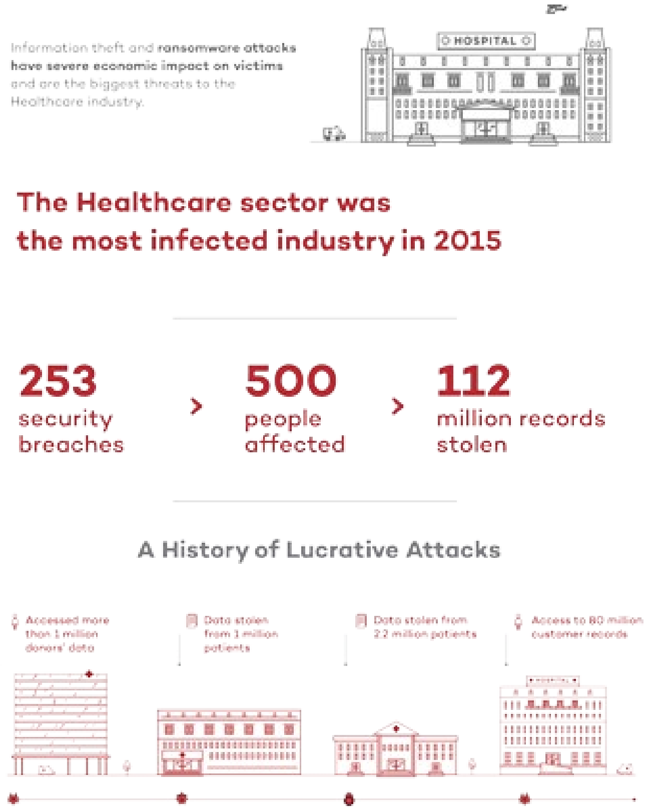
In total he uncovered 21 vulnerabilities that could allow an attacker, say, to control the amount of electricity supplied to the grid. These vulnerabilities can be exploited remotely over the Internet.

A malicious attacker who compromised these installations could cause incalculable damage. More details are available **here**.

The Health Sector.

The hacking of the electrical grid is, of course, an extremely serious crime that could affect the lives of countless people, yet it is nowhere near the potential danger of an attacker controlling a pacemaker or hospital equipment which, in the worst case scenario, could enable people to be killed remotely, as shown in our **report**.

The FDA (Food and Drug Administration) warned almost half a million patients to see their doctor to update the firmware of different models of Abbott pacemakers.


Information theft and ransomware attacks have severe economic impact on victims and are the biggest threats to the Healthcare industry.
HOSPITAL
The Healthcare sector was the most infected industry in 2015
253 security breaches
500 people affected
112 million records stolen
A History of Lucrative Attacks
Accessed more than 1 million donors' data
Data stolen from 1 million patients
Data stolen from 2.2 million patients
Access to 80 million customer records

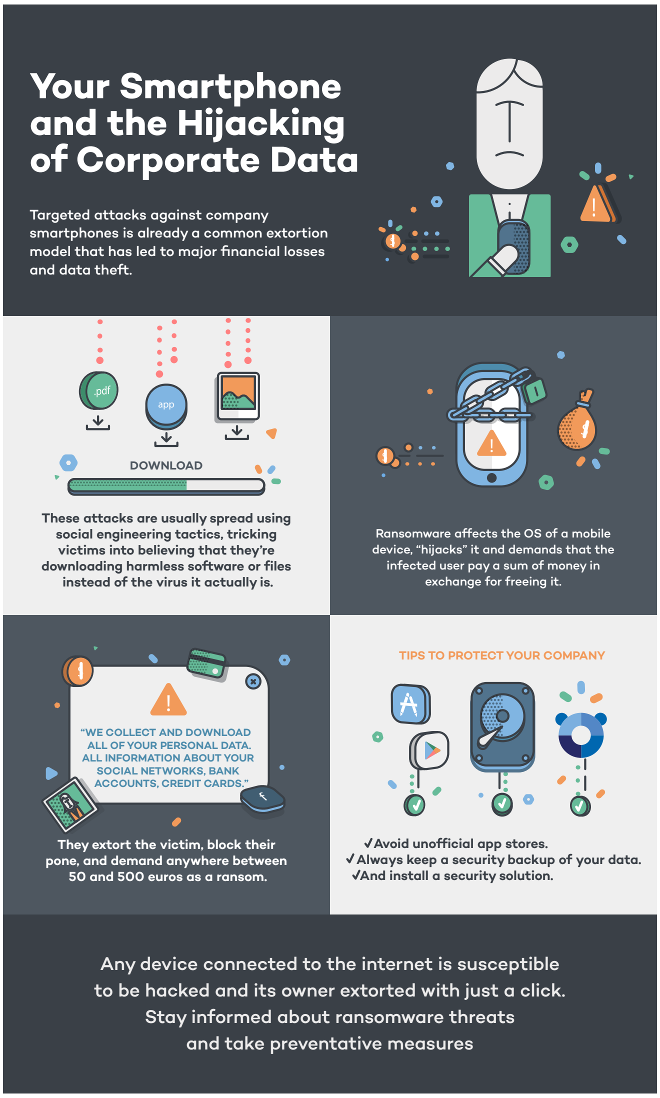
Mobile Devices.

Malware designed specifically for mobile devices is still inferior to the malware found on PCs, but the basic steps it takes is the same.

The popularity of ransomware, which is giving great results to cybercriminals, and it's migration to these devices is clear evidence of this.

Malware for Mobile Devices.

Charger, the new Android-oriented malware, is a good example of how mobile malware is progressing. **Charger steals contact information** and SMS messages before blocking the terminal, demanding a ransom under the threat of selling part of your information on the black market every 30 minutes. The ransom amounted to 0.2 bitcoins.



Your Smartphone and the Hijacking of Corporate Data

Targeted attacks against company smartphones is already a common extortion model that has led to major financial losses and data theft.

These attacks are usually spread using social engineering tactics, tricking victims into believing that they're downloading harmless software or files instead of the virus it actually is.

Ransomware affects the OS of a mobile device, "hijacks" it and demands that the infected user pay a sum of money in exchange for freeing it.

"WE COLLECT AND DOWNLOAD ALL OF YOUR PERSONAL DATA. ALL INFORMATION ABOUT YOUR SOCIAL NETWORKS, BANK ACCOUNTS, CREDIT CARDS."

They extort the victim, block their pone, and demand anywhere between 50 and 500 euros as a ransom.

TIPS TO PROTECT YOUR COMPANY

✓Avoid unofficial app stores.
✓Always keep a security backup of your data.
✓And install a security solution.

Any device connected to the internet is susceptible to be hacked and its owner extorted with just a click. Stay informed about ransomware threats and take preventative measures

Big companies are worried, something that is reflected in initiatives such as Google's Project Zero Contest, which is increasing the rewards for anyone who finds the most serious zero-day vulnerabilities (none have been discovered in recent years). The first place prize has increased from $50,000 to $200,000, and the second from $30,000 to $150,000.

Vulnerabilities.

A vulnerability (CVE-2017-6975) in the firmware of Broadcom Wi-Fi HardMAC SoC chips made it necessary for Apple to urgently launch an iOS update (10.3.1). This vulnerability, occurring when a Wi-Fi connection is renegotiated, didn't only affect Apple products, but also mobile devices from other manufacturers such as Samsung or Google, who issued their updates in April in response to the problem.

But if there is one vulnerability that wins the day, it would have to be KRACK, which affects the WPA2 protocol. It is not exclusive to mobile devices, as it affects all types of devices that implement WPA (personal computers, routers, etc.), but it is worth noting that it mainly affect users of Android mobile phones.

The problem was discovered in 2016 by Belgian researchers Mathy Vanhoef and Frank Piessens, but it wasn't made public until October 2017. One of the implementations of the free-code protocol, "wpa_supplicant", used by both Linux and Android, is especially vulnerable to this attack.

While Google will release the corresponding security patch for its operating system, there are many device manufacturers that have yet to implement their version of the updates, and there are many devices (hundreds of millions) in use that are no longer supported by their manufacturers and will therefore never receive the necessary updates, a recurrent problem in this ecosystem.

Cyberwarfare.

The two major attacks of the year (WannaCry and **GoldenEye/Petya**) are suspected of having been perpetrated by governments (North Korea in the case of WannaCry, and Russia in GoldenEye/Petya), but these are only a couple of cases within a larger cyberwar that is taking place in the shadows.

The main protagonists are consistently the same: the United States, Russia, North Korea, China, and Iran, although in most cases it is impossible to be sure who is behind any given attack, as in most cases the attackers do a good job of covering their tracks, and sometimes even plant red herrings that would point to another perpetrator.

More than ever, cyberattacks and politics have become intertwined. Following the hangover of last year's US elections, and before leaving office, Obama announced sanctions against Russia, accusing it of having orchestrated cyberattacks to damage Democrat Hillary Clinton's campaign in favor of Donald Trump. Thirty-five Russian diplomats were expelled, and two Russia-owned centers closed.

The repercussions can be felt around the world. France has ruled out the use of electronic voting for 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 possible cyberattack.

In February, the Netherlands also called for the creation of an international cyber defense alliance, through NATO, which would have defense capabilities, control, and response measures against the growing threat of cyberattacks.

German Chancellor Angela Merkel said in March that protecting their nation's infrastructures from potential cyberattacks would become one of Germany's top priorities.

Shortly thereafter, they announced that the **German army will form its own cybercommand** to reinforce its online defenses. It is slated to have 260 employees, a number which will increase to 14,500 by 2021.

None other than the CIA itself came into spotlight for one of the year's most newsworthy events in cyberespionage.

On March 7, **WikiLeaks began publishing a series of documents under the title "Vault 7"** containing details of techniques and software tools used to break into smartphones, computers, and even Smart TVs. WikiLeaks is publishing the documents and has dedicated a section of its **website** to the leaks.

The good news is that you can use this now-public knowledge to better protect yourself against such threats; the bad thing is that other actors can learn to implement similar tactics to violate the privacy of citizens.

The United States is clearly concerned about the attacks targeting US institutions. The Congressional Intelligence Committee held a hearing to discuss **the impact of Russia's hacking of the 2016 presidential elections** in which former DHS Secretary under the Obama administration, Jeh Johnson, reiterated that Russian President Vladimir Putin had ordered the attack with the intention of influencing the result of the US presidential elections. He also said that they had failed to manipulate votes in these attacks.

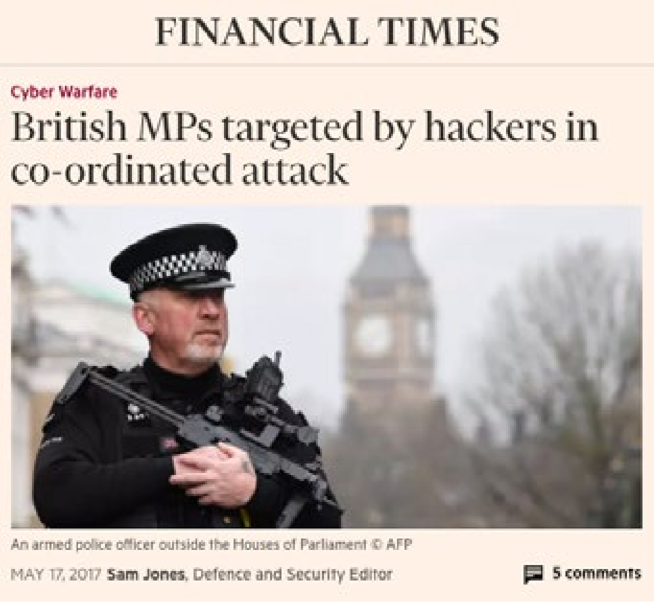
In June the US government issued an alert blaming the North Korean government for **a series of cyberattacks occurring since 2009**, and warning that they are likely to commit even more.

The warning, which came from the DHS and FBI, referred to a group of attackers, "Hidden Cobra", who have attacked the media, aerospace and financial sectors, as well as critical infrastructures in both the US and others countries. **There is evidence linking WannaCry's recent attack with the same group**, "Hidden Cobra", more recently known as "Lazarus Group".

One possible explanation for the number of attacks attributed to North Korea is the increased sanctions levied against them by the UN, pushing them to seek alternative financing.

During the Gartner Security and Risk Management Summit held in Washington in June, former CIA director John Brennan spoke on the alleged **alliance between the Russian government and cybercriminals** to carry out the theft of Yahoo accounts. According to Brennan, this was just the tip of the iceberg. He warned that future cyberattacks by governments will follow this formula and will increase in frequency.

Members of the British Parliament had their accounts hacked, according to the Financial Times, in what was believed to be a foreign-sponsored attack.



FINANCIAL TIMES

Cyber Warfare

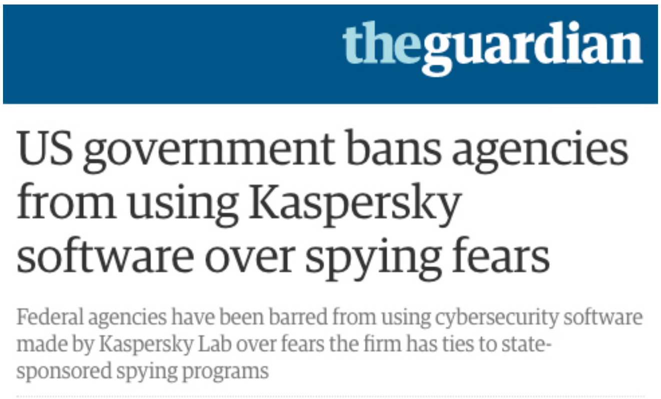
British MPs targeted by hackers in co-ordinated attack

An armed police officer outside the Houses of Parliament © AFP

MAY 17, 2017 **Sam Jones**, Defence and Security Editor

5 comments

This whirlwind of politically motivated cyberattacks is also affecting technology companies. The Russian FSB is demanding that companies like CISCO, SAP, and IBM hand over 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.



theguardian

US government bans agencies from using Kaspersky software over spying fears

Federal agencies have been barred from using cybersecurity software made by Kaspersky Lab over fears the firm has ties to state-sponsored spying programs

Altough there has not yet been any tangible evidence to attest to malicious activity on the part of Kaspersky, it is understandable that in the current climate of tension between the two powers the US government would be concerned. But rather for the mere fact that it is a company based in Russia, a country whose government is verging on the authoritarian. They are anticipating that the **Russian government could at any given moment mandate Kaspersky to use its software to launch an attack** or steal information in the hypothetical case of an escalating conflict.

About Threat Hunting Systems.

Iñaki Urzay

Chief Security Strategist of Panda Security

The number of cyber-security experts around the world is growing exponentially. An increase driven primarily by governments that need to take an active role (either on their own initiative or reactively) in a virtual conflict in which no one can remain on the sidelines. Governments around the globe have, for some time now, been creating specialist cyber-defense agencies, including the newly created German division with **more than 13,000 cyber soldiers, the more than 100,000 agents anticipated by the U.S. Government by 2020, the 6,000 that North Korea appears to have**, along with those in the armies of Russia, China, UK, France, Spain, Israel, Iran, etc.

In addition, there are the specialists working with security solution providers and contractors around the world. All these firms have experts in cybersecurity, in all countries. And finally, there are the cybercriminals who, as a result of this boom in the number of security experts and global interest in cybersecurity, are able to find trained resources much more easily.

This increase in highly-qualified human capability has created an environment in which it is possible to discover vulnerabilities in software systematically. It also favors the development of professional attack tools and the sustainability and scalability of malwareless attacks that are carried out directly by the perpetrators and are able to adapt to the targeted environment with the utmost stealth.

As we can see with Panda Adaptive Defense, **malware-based attacks can be perfectly contained** with solutions based on the 'strict positive' model created by Panda Security.

When all applications that attempt to run on a computer are classified and only those that are genuinely safe are allowed to run, **the 'detection gap' characterized by the traditional antivirus model disappears**. Malware can no longer hide in unknown files that a traditional security solution would have to ignore.

The capability that this security model has to prevent attacks is something that the market can no longer afford to ignore and the growth of market share of the model is easy to predict.

As this approach replaces traditional antivirus models, attackers will adapt their techniques in order to circumvent them. And in this case, it is conceivable that attacks not based on malware will become more prevalent.

Malwareless attacks are characterized by the use of tools usually used by legitimate network administrators, such as applications for installing software remotely or for backing up data, etc.

In this type of action, **attackers assume the identity of the administrator**, after having managed to obtain their network credentials, and in the eyes of any external observer would appear to be the network administrator going about their business.

As no malware is used, security systems have to be able to identify these types of attacks based on the behavior of network users. The technologies that are capable of performing such tasks fall within the concept of **Threat Hunting**.

Threat Hunting platforms ought to be capable, among other things, of monitoring the behavior of computers, the applications running on them and, in particular, their users.

For each of these components, typical behavior profiles have to be defined dynamically and then, in real time, cross-checked against the data of what is really happening, in order to root out any behavior that could indicate that someone has stolen an identity.

Technically speaking, the Threat Hunting process is based on an immense pool of data regarding all the behavior of the monitored components and updated in real time as new events occur. In this context, **the platform used must be able to explore this vast store of information in order to develop new attack hypotheses**, backtest them on partial groups of data before activating them on the main data stream in real time, and generate models based on the search for behavioral profile anomalies. At that point, **machine learning systems will prioritize potential incidents** which, once triggered, need to be analyzed in detail using remote forensic analysis tools integrated in the platform.

Such tools will allow analysts to run personalized scans on affected computers so that they can situate themselves at any point in time in the event history of each computer or user and reconstruct their steps in order to confirm the attack.

In the immediate future, **traditional malware in the form of evidently malicious specific programs, will be superseded by malwareless operations**, in which attackers usurp the identity of network users and carry out actions under the guise of seemingly legitimate users.

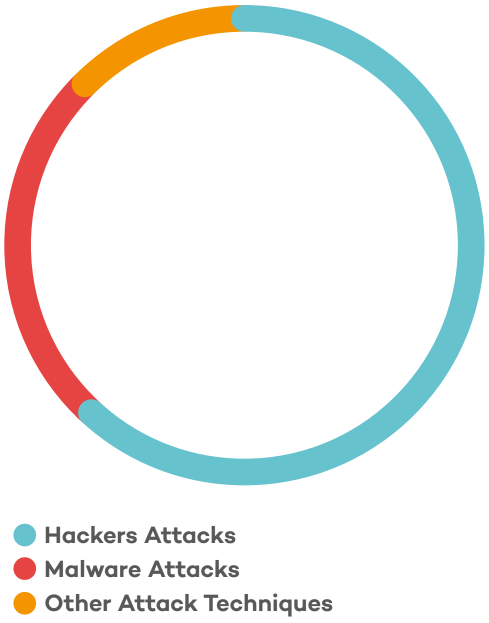
In this context, it will be imperative that security solutions, in addition to offering the ability to implement strictly managed positive models, provide scalable threat hunting services and platforms.

Panda Adaptive Defense is the first solution on the market to simultaneously offer both capabilities, an automated Threat Hunting service and tools in the form of APIs and consoles that allow customers to perform scanning and reconnaissance of their networks in search of hidden attackers behind the identities of corporate users.

Compromised Situations.

Attacks have evolved. The targets have changed. The techniques have become more sophisticated, the attack vectors multiplied, and the tools refined.

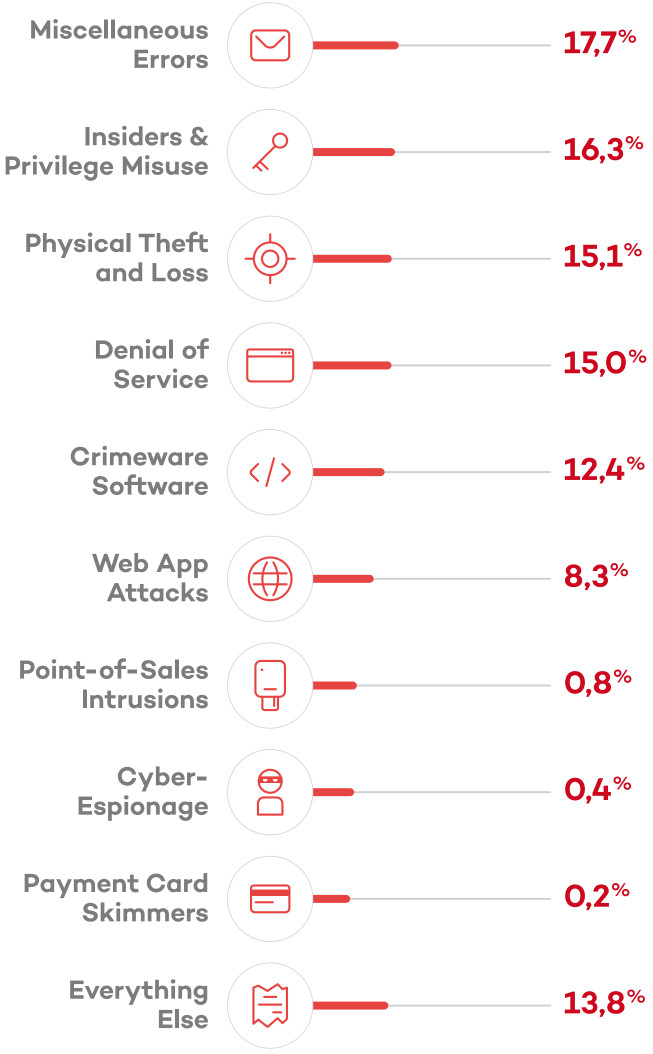
Attackers are studying their victims meticulously in order to better adapt their attack strategy to have the greatest possible impact. **Behind 62% of threats are hackers** that carry out analysis activities and adapt their attacks accordingly and with great care.



Their efficiency, effectiveness, and profitability are proven time and again, with up to 100,000 new breaches and security incidents in corporate environments this year alone.

Throughout this report, we have seen how they do it and what they have achieved. With all this, it would seem that it is now more likely than ever to fall victim to a cyberattack. This is partially true, but it isn't the whole story: prevention, detection, response and remediation systems are increasingly effective. They combine, as in the case of Panda Adaptive Defense, solutions and services to **optimize protection, reduce the surface of attack, and minimize the impact of threats**.

Thanks to this evolution of techniques, we are able to offer you a series of cases in which Panda Security aborted an attack in time. Our forensic investigations played a decisive role here. These attacks showcase the fulfilment of these new tendencies and attack techniques, confirming Verizon's study which concluded that **95% of security gaps can be reduced to nine action patterns**.



In this way, we have also helped to improve the protocols and defense structures of companies, even in workstations and systems that did not have the direct protection of Panda Adaptive Defense.

Lateral Movements.

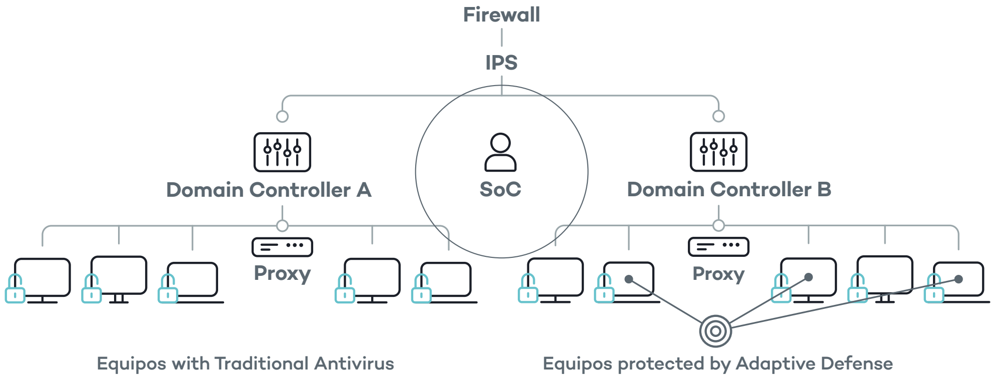
As a sample of both types of evolution, we'll begin by presenting a hidden attack with adaptive lateral movements, a type of attack that is becoming all too common. This time the company had a complete battery of detection and protection systems (firewall, IPS, SoC, domain controllers, proxies, traditional protection, etc.)

But no one noticed the lateral movement that could have led to the perfect attack against the client's assets.

However, the criminals were not counting on the fact that this company had Adaptive Defense, which did discover their intentions and aborted their plan of attack:

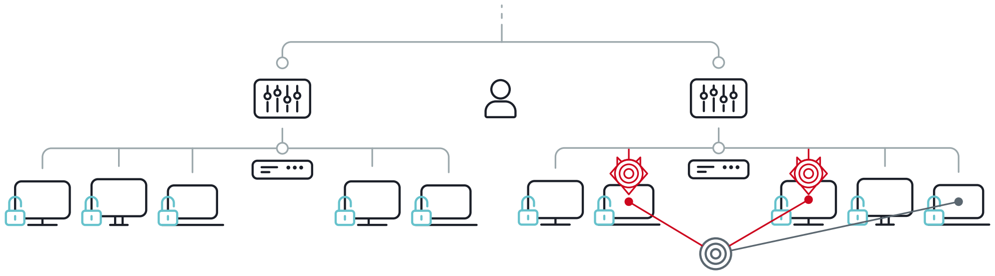
1 An apparently protected network

Key Account environment of thousands of endpoints in two domains, a few domain controllers, Firewall, IPS, antivirus and a SoC. Adaptive Defense deployment starts to a few endpoints at Domain "B".


Firewall
IPS
Domain Controller A
SoC
Domain Controller B
Proxy
Proxy
Equipos with Traditional Antivirus
Equipos protected by Adaptive Defense

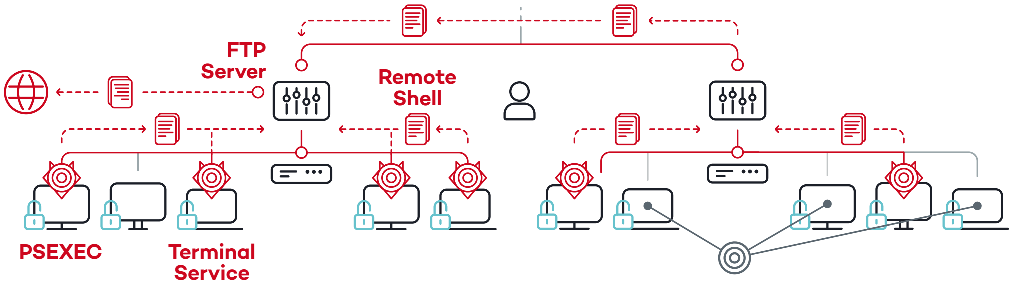
2 Adaptive Defense Security Model

Blocks untrusted programs and sends protected endpoint telemetry that is immediately processed in the cloud.



3 Threat Hunting and Investigation

Threat Hunters link retrospective to discover an apparently protected network domain "A" was in fact compromised, using administrative tools to gather and send endpoint profiling data to Malaysia.



☆ Attack discovered by the Threat Hunting team

The attacker's lateral movements to gain control of domain "B", were discovered and remediated by Adaptive Defense before being compromised.

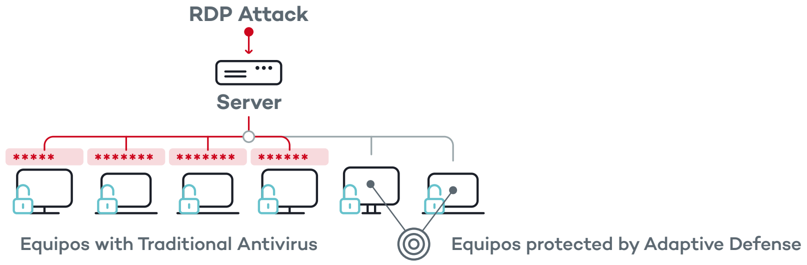
RDP: Malwareless Attack.

The malwareless attack has become one of cybercriminals' favorite threats. In fact, o**nly 51% of the security breaches registered this year used some kind of malware** as an attack maneuver. They prefer to remain invisible to traditional protections and not rely on human interaction on the victim's part, and, as in this example, to be able to double profitability by optimizing the effect of the attack.

Once its victims were located, it deployed an **RDP attack** to monetize the offensive in two different ways: 1) generating online traffic that was sold to third-party websites, or 2) selling access to the compromised machines to the highest bidder. We have seen these cases with some frequency. They can be summarized in this infographic:

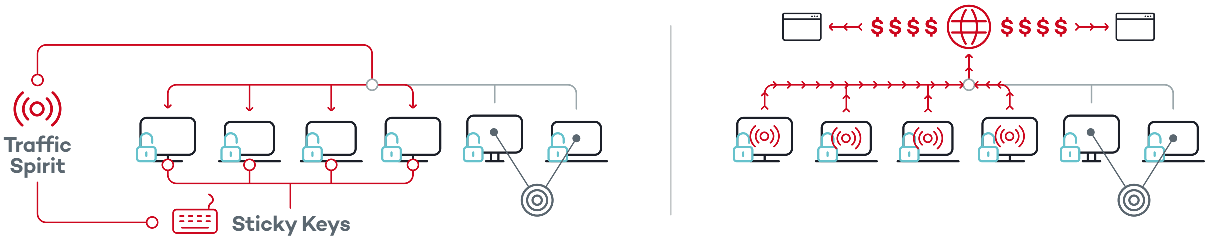
1 Gaining access and persistence

Attacker scans the Internet looking for potential victims with Remote Desktop enabled.
When found, he uses a brute-force attack to login into the system. Once in the system, he gets persistence by modifying the Sticky Keys feature registry entry. When Sticky Keys is activated (e.g. pressing CAPS 5 times) it will open a backdoor to the victim's computer that allows the attacker to access it even if Remote Desktop credentials are changed.


RDP Attack
Server
*****
****
****
******
Equipos with Traditional Antivirus
Equipos protected by Adaptive Defense

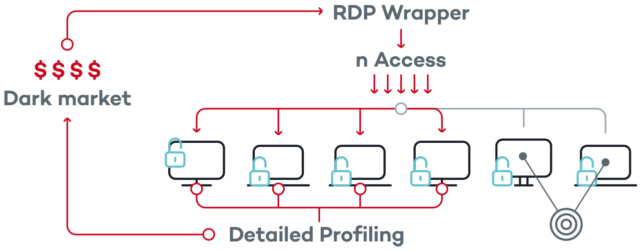
2.1 Monetization of the compromised endpoints: Generating online traffic

The hacker downloads "Traffic Spirit", a "legal" traffic generator application which is used to make extra money off of the compromised computers. There is no malicious program in this attack.



2.2 Monetization of the compromised endpoints: Selling the access to the machines

Once the attackers get the access, they carry out a detailed profiling of all the computers. They then offer access to these machines on the black market for different purposes (extortion, data leak, make them zombies, bots, etc.).



Attack discovered by Threat Hunting team

The attack is discovered thanks to continuous monitoring and visibility of all activities at the endpoint. That data shown to Panda Threat Hunters indicated an abnormal behavior at endpoints that were compromised with a brute-force attack (hundreds of login tries in a short period of time).

An Ex-employee's Extortion.

One of the most widespread motives for launching an attack on a company is resentment and wishing to exact revenge.

And this year, we have seen several cases of ex-employees who tried to extort their old companies, to the point that **attacks initiated by internal actors already account for 25% of global threats**.

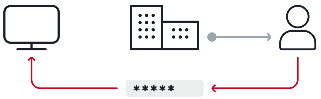
The common denominator of these cases is the laxity of protection policies and the attacker's having access to corporate resources.

81% of illicit accesses occurred because of insecure passwords, or the direct theft of passwords.

In spite of this, once inside, employees use strategies of expansion and control worthy of the best hackers to evade the rest of security systems and to do damage to the company's reputation and its finances:

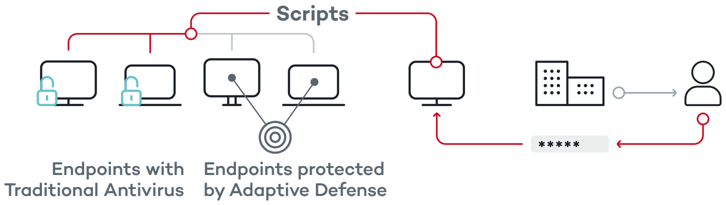
1 The employee is fired

But his credentials were not revoked, so he still can remotely access his computer.



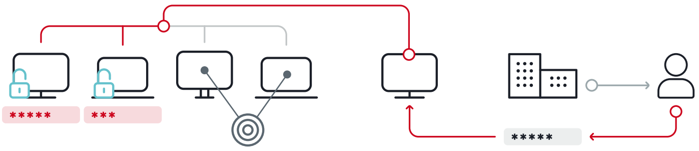
2 Detailed profiling

Thanks to several OS tools, the employee gets the list of endpoints connected to the network. He launches a script with a MS command to find out the users of the domain.


Scripts
*****
Endpoints with Traditional Antivirus
Endpoints protected by Adaptive Defense

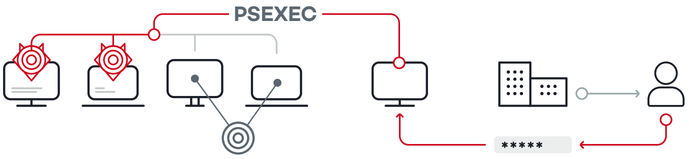
3 Brute-force attacks

Within the following days, he deployed brute-force attacks and finally got access to several endpoints.



4 Ransomware attack

He creates a ransomware, which is compiled the day before it is deployed. From his former computer, and by executing PSEXEC, he launches a script to remove all the existing backups and then copies and executes the ransomware.



Attack discovered by the Threat Hunting team

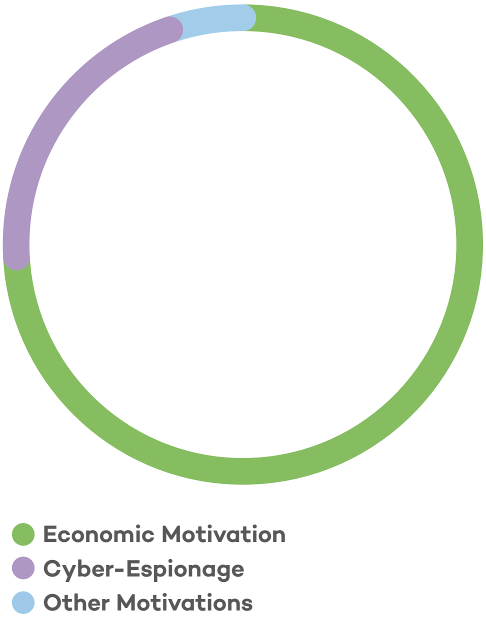
Adaptive Defense blocked the attack in all the machines where it was installed. After the first attack attempt on an endpoint protected by Adaptive Defense, the Threat Hunting team investigated all the processes and behaviors, which revealed all the details of the attack and the identity of the attacker.

Coincidences.

Despite some of their differences, these cases have a few similarities:

- A **preparatory study** of the company's weaknesses prior to the attack.
- The **adaptation of the offensive** to those weaknesses, stealth access that doesn't arouse suspicion or trip alert systems in traditional security solutions.
- Carefully planned and mapped out **internal movements** to reach their goals.

The common goal of these attacks is usually, as ever, money. According to Verizon, **a financial goal is shared by 73% of attacks**, while 21% of motives are related to espionage.



The other common denominator that these cases have is that they were all detected and aborted by the Threat Hunting team and the advanced solutions of Panda Security.

The Price of Attacks.

We've seen how the democratization of cyberattacks was facilitated by variables such as the professionalization of attackers, the evolution of technology, or the ease of access to data.

Although this is something that certainly helped to popularize these kinds of threats, these actions are driven by profitability.

Inexpensive cyberarms, with which the attacker can reap a handsome reward.

		From	To
Attack Tools	Malware	$50	$200
	Ransomware	$1	$400
	Software	$100	$700
	Payments & Log-ins	$1	$25
Data	Personal Information	$3	$150
	Data Base Records	$25	
Services	Hacking	$100	$300
	Users	$20	$150
	Malware	$1	$25
	Spam	$20	$400
	Fake Documents	$15	$25

Source: Recorded Future.

GDPR, the Regulation of Opportunity.

The new General Data Protection Regulation (GDPR) was developed in response to the undeniable increase in cyberattacks and seeks to counter it through the collaboration of public and private entities.

Although it is already in effect, **the GDPR will begin to be fully enforced in May 2018**. Companies are now racing against the clock to adjust their practices to the new legislation.

Current national laws and the GDPR will part ways in May 2018 when the latter is imposed throughout the European Union. The new law calls on companies to adapt their policies to much more restrictive and punitive requirements. For example, it will obligate companies to report any personal data breaches to the Data Protection Agency under **penalty of sanctions that can reach up to 4% of annual turnover**.

Organizations will also be compelled to incorporate encryption and dual-factor authentication systems across all layers of data. Cutting any corners of the legislation will be costly. One of the more salient changes introduced by the legislation will be the mandated appointment of a Data Protection Officer (DPO). The person charged with this role will have expertise in both the legislation and the necessary technological infrastructures for adhering to it.

However, the full scope of the DPO's duties has yet to be defined, nor is it decided whether the role could be delegated to the CISO in certain companies.

The GDPR at a Glance:

- Establishes in greater detail how to handle data of EU residents, including for countries outside the EU.
- Requires the express consent of the residents in relation to the data to be collected and clarity regarding the use that can be made of them.
- Defines the scope of what personal data is to include social media data, photos, email addresses, and even IP addresses.
- Addresses data transfers through open and popular file formats.
- Takes into account the "right to be forgotten", which allows individuals to permanently delete or rectify the data of a person on request.
- Establishes that organizations of all sizes should designate data protection officers, who will answer to data protection authorities.
- Requires that processes and workflows integrate privacy into design.
- Requires any potential data breach to be reported within a few days of being detected.
- It includes large fines of up to 20 million euros or, up to 4% of the overall turnover, whichever is higher.

It will affect companies that handle the personal data of EU citizens

Obligation to send notification of data incidents within 72 hours

Up to 20,000,000€ in fines for failure to comply with the regulation

The DPO will be in charge of consulting and supervising on GDPR compliance

Case in Point.

In most US states, there are laws requiring that any security breach of customer data be immediately reported. It's no surprise, then, that the vast majority of data breaches covered in the media involve American companies.

Before the GDPR, many countries of the European Union had no such provision in place.

A recent and particularly vicious example is the Equifax breach, considered to be the most serious breach of sensitive personal data in history. Had it occurred in Europe under current, pre-GDPR legislation, the breach would probably have gone unreported. Neither affected customers nor regulators would have been any the wiser.

If it had happened in Europe, and with the new regulation in force, Equifax would face a lawsuit with the EU and all affected users. With a net annual turnover of $500 million, **Equifax would be facing fines imposed by the EU of $20 million**; and that's not even counting the damages that would be awarded to those affected by the breach.

This will all change with the new legislation, and the result will probably be that we'll see a sharp spike in cases of data theft in the EU. Such breaches were already taking place.

The difference now is that we will know about them.

Cybersecurity Predictions.

From the above analysis, it would appear that problems of cybersecurity are increasingly pressing, especially for businesses and large corporations, most of which suffer from data breaches at one time or another. The interval between a data leak and its detection is increasing, and the usual method of preventing data loss is becoming less effective.

These are just some of the pressing issues in computer security today, but **what are the threats waiting for us in 2018?**

In this section, we will discuss our predictions about what we think the world of cybersecurity has in store for next year.

Cyberwarfare and its Consequences.

Cyberwarfare is a reality that we are already living through. In the place of an open war where the divisions are clearly demarcated, cyberwars take place in the shadows and involve isolated guerilla-style attacks whose authors are never known for certain.

Freelancers in the service of the highest bidder.

The major world powers already have entire legions of cyber soldiers, tens of thousands of trained "combatants" with offensive capabilities in cyberspace. Over time, some of them will become freelancers, offering their expertise and capabilities to the highest bidder. Bands of professional cybercriminals will be able to find a pool of well-prepared professionals with access to (cyber) weapons and valuable knowledge for launching attacks. As a consequence, w**e will see how the number of advanced and complex attacks grows**.

False flag operations.

One of the most attractive features that cyberattacks offer to nations in conflict is the anonymity provided by the Internet. Of course, there will always be suspicion surrounding the perpetrators of a particular attack, analyzing for example the victim and drawing conclusions about who could benefit from their suffering.

Another method is to look at the tracks that attackers may left behind: characteristics in the malicious code used, servers the attack connected to for carrying out its communications, etc.

Regardless, anonymity is yet another weapon in these attacks: **it is very simple to carry out an attack by making it go through an unrelated third-party**. This type of false flag operation will become increasingly common, and figuring out who is really behind a government-backed cyberattack will become ever more difficult.

Collateral victims.

WannaCry showed that there are attacks that can infiltrate corporate networks and indiscriminately attack any and all vulnerable victims.

But there are also surgical attacks, where the target is very well defined. This was the case of Petya/GoldenEye, which clearly targeted public and private enterprises in Ukraine. However, the reality is that on the Internet there are no borders, and companies from dozens of countries around the world were affected by this attack, turning them into collateral victims of a conflict with which they had no relationship.

The Enemy in our Midst.

One of the biggest nightmares we can imagine is being attacked in a protected environment in which we feel safe, such as in our own home. It is a situation that we are not adequately prepared to face, since, a) we trust the people we've invited into our homes, and b) even if a knife can be used as a weapon, we all have one as a cooking utensil. This analogy serves to illustrate the type of attacks that we are going to have to face:

Malwareless hacking attacks.

One of the tendencies that we are going to see throughout 2018 is how the number of malwareless attacks and attacks that abuse non-malicious tools will increase.

In 2017, we have seen that **hacking techniques had been used in 62% of corporate security breaches**, and in half (49%) of these incidents there was no malware involved at all, according to the Verizon's 2017 Data Breach Investigations Report).

Compromised applications.

We have seen this in the Petya/GoldenEye attack, where versions of the accounting software M.E.Doc were compromised. Another case of special note is CCleaner, modified by unknown attackers in what appears to be an attack targeting specific victims of large technology companies.

Mobile Devices.

To what extent should we care about threats in the mobile environment? The answer is: within reason. Keep in mind that there are more smartphones than computers in the world, and yet the number of attacks targeting them is a small fraction of what PCs have to face.

This does not mean that we should be nonchalant about the security of our mobile devices. Attacks will continue to take place, but it seems that Google has taken note of the main issues and is slowly taking steps to secure its operating system (**Android, which has the largest market share in the world in the mobile sector**) and to close the gaps (without yet making it to Apple's iOS).

But the fact remains that there are millions of threats that target Android, so it is of course necessary for any data that we access on our mobile phones to be properly protected.

The Internet of Things.

The number of devices connected to the Internet continues to grow. What effect can this have on security? There are already botnets composed of thousands of IoT devices, from IP cameras to printers, giving cybercriminals the ability to launch massive attacks.

In general, IoT devices are not the primary target of cybercriminals. However, these devices increase the surface of attack, so it will become more and more frequent to see them being used as an entry vector for attacks on corporate networks.

All for the Money.

Ransomware.

There is little doubt that the main objective of cybercriminal organizations is to turn a profit. Ransomware attacks will continue to be prevalent in 2018, since the potential return on their investment is very high, while the risk remains low.

More Advanced Attacks.

attacks will be professionalized, especially in cases where the potential gains are higher. When new methods of cybercrime are shown to be successful, they will be immediately replicated by masses of imitators. This is one of the primary reasons for which the number of advanced attacks will increase significantly in 2018.

Following the trend of recent years, **in 2018 there will be a 50% increase over attacks** suffered in the course of this year.

2018, the Year of Attacks on Companies.

It may be true that we've lived through some major attacks in the past, with astronomical amounts of stolen data. Everyone remembers, for instance, the Yahoo breach and the theft of hundreds of millions of credentials.

And this year, of course, we've had Sabre and Equifax. So why do we think that 2018 will be worthy of the title, "the year of attacks on companies"? This question can be answered with a four-letter abbreviation: GDPR.

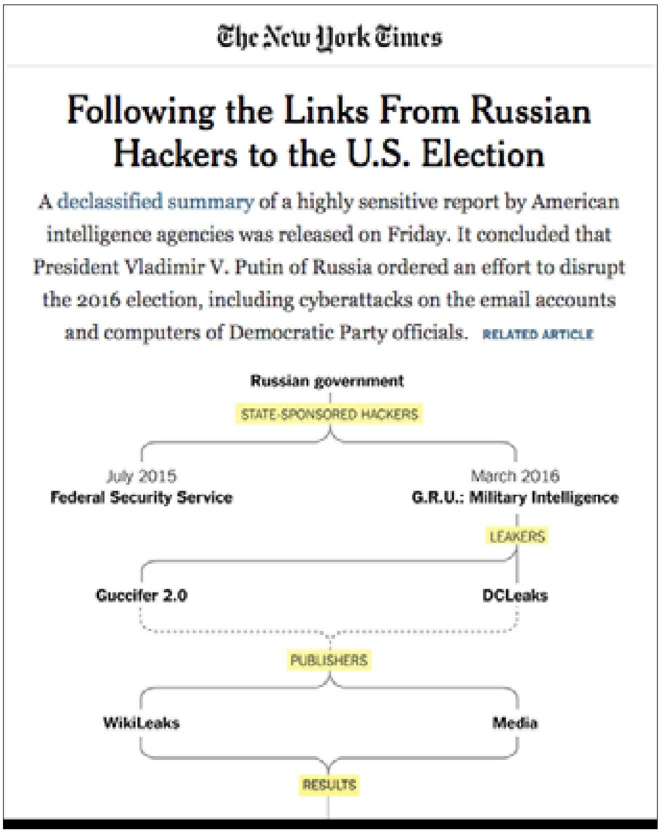
This doesn't necessarily mean that in 2018, companies will come under attack more than in other years.

Rather, for the first time ever, the public will be made aware of each and every data breach, including those that, pre-GDPR, may otherwise have been swept under the proverbial rug.

Social Media and Propaganda.

Never before in history have human beings had access to so much information. Ironically, it has never been so difficult to find factual information as it is now.

Simply put, social networks are tools where we can exchange information, and when used by billions of people, they become a clear target for anyone wishing to influence public opinion. In a way, their role has become comparable to that of the press. We have heard that **President Obama personally cautioned Facebook founder** and CEO Mark Zuckerberg to take the threat of fake news in the US presidential election very seriously.



The New York Times

Following the Links From Russian Hackers to the U.S. Election

A declassified summary of a highly sensitive report by American intelligence agencies was released on Friday. It concluded that President Vladimir V. Putin of Russia ordered an effort to disrupt the 2016 election, including cyberattacks on the email accounts and computers of Democratic Party officials. RELATED ARTICLE

Facebook, the world's largest social network, is already taking action on the issue. If it is discovered that a Facebook page repeatedly distributes fake news, Facebook will prohibit it from being advertised anywhere on the network. They have also posted announcements on their network and in the media giving advice to readers so they can identify fake news. They are now in the process of changing their policy for elections-related advertising to make it as transparent as possible.

Cryptocurrency.

Bitcoin and other cryptocurrencies are increasingly being used as a means of digital payment. While there is a lot of speculation on the future of this, there are more and more merchants that accept payment in these currencies. Another reason for the success of these currencies is their usefulness to cybercrime, as it allows for large amounts of money to move around quickly and anonymously.

Ransomware is the best example of this, since almost all of these attacks seek a ransom in the form of bitcoin.

Cryptocurrencies will continue to gain in value and usability, and so will the cybercrime that has grown alongside them:

- Infecting computers and servers with cryptocoin mining software.
- Infecting web pages to turn all visitors of the page into miners.
- Stealing coins from cryptocurrency exchanges.
- Stealing crypto wallets.

Conclusions.

After seeing global attacks that have hit companies and institutions around the world, it is important to know how we can safeguard our privacy and security on the Internet.

Security update protocols should be a priority at all companies. Cases such as WannaCry or Equifax reaffirm this, as every day that passes without patching a vulnerable system puts the company at risk, as well as the integrity of its data, including that of customers and suppliers. Production can be endangered and incur millions in losses. One example: the AP Moller-Maersk group was one of the victims of the GoldenEye/NotPetya attack, and calculates that the losses suffered are between 200 and 300 million dollars.

Countries are investing more and more in defensive and offensive capabilities, with a focus on critical infrastructures. The ability to remotely launch a blackout-causing attack is not just a theory: it has already happened in Ukraine and could be repeated in any country in the world. Groups with limited funding may nevertheless have access to the knowledge and tools required to launch crippling attacks on infrastructure; such attacks are no longer the sole domain of state actors. And it is known that terrorist groups, such as ISIS, are willing to use all the cyber means at their disposal to further their spread of terror.

2018 augurs a more dangerous situation. For many professionals, **a change of mentality (and strategy) will be necessary to achieve the highest levels of security** and protect the assets of their companies' networks. Countering malware is only the beginning. We are entering an era in which the best security strategy entails trusting nothing. Any new process that wants to run on any device connected to the network must be previously approved, and those that we trust will have to be closely monitored in order to detect any anomalous behavior in the shortest possible time.

Both in business and at home, **training and awareness are key**. It follows that cybersecurity, often forgotten by management, will require a greater investment.

Having in-depth knowledge of attacks and what they consist of should be the basis for a good defensive strategy. **Security based on detection and response in real time**, with forensic reporting and details of how the attack occurred, is essential to avoiding future intrusions. Gartner Peer Insights endorses Panda Adaptive Defense, the leading EDR solution with the largest number of analyses on the entire market.

Signature files no longer work and the figures speak for themselves: more than 99% of all malware never appears again anywhere else. Compiling signatures is already an insufficient and inefficient way of approaching detection. Most security companies add them just in case a testing laboratory later decides to carry out a malware detection test by signatures (something which is becoming less and less common), or for those who believe that such results translate into a product can detect a threat or not.

There is a problem of focus: **solutions that remain focused on fighting against malware (the majority of those available on the market) are doomed to become extinct** if they do not change their strategy. The number of malwareless attacks, in which no malware is used, continues to grow. And in the face of this reality both security solutions and their clients are completely lost and defenseless.

And of course, we can't forget **international cooperation and the creation of common legislative frameworks** such as the GDPR. Having political and economic support and a plan of action will make it possible to benefit from the latest technological advances in the safest manner.

After all, it is all about **reinventing cybersecurity**.