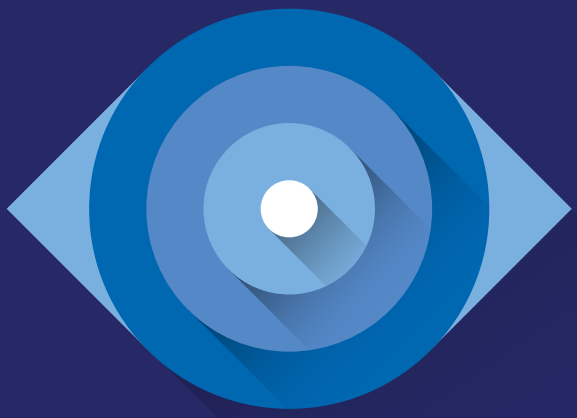
November, 2018

PandaLabs Annual Report 2018



panda

pandalabs

1. Introduction
2. PandaLabs: Threat Data in 2018
   - Pre-execution detections
   - Examples of cases investigated by the laboratory
   - Malware incidents escalated to PandaLabs
   - The “Threat Mitigation Funnel”
3. Cyber-news 2018
4. Data breaches
5. Cybersecurity predictions 2019

Introduction:
The State of Cybersecurity

Introduction: the State of Cybersecurity

2017 was the year when the word *ransomware* stopped being a term exclusive to cybersecurity experts and IT departments. The enormous media attention that attacks such as WannaCry and Petya/GoldenEye received turned this type of threat into one of the key trends for businesses last year. However, as professionals in the sector know, highly publicized events must never serve as a risk indicator, nor influence on any security related decision.

In this annual report, we at PandaLabs, Panda Security's anti-malware laboratory, have reviewed the threat data gathered in the laboratory from our sensor sources. We include here data from endpoint security solutions deployed on our clients' devices; the trends observed by our analysts whilst they were providing file classification and threat hunting services; as well as the most relevant cybersecurity incidents reported around the world.

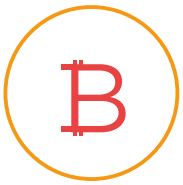
And the information compiled in 2018 continues to reflect the prevalence of malware attacks, with 9 million malicious URLs and 2.4 million attacks blocked per million endpoints per month. 20.7% of machines studied experienced at least one malware attack during the period analyzed.

PandaLabs can state that the threats of file-based malware is not a problem for Panda Security, with infections trending to zero. This is due to the adoption of the model of 100% classification of all executable processes on systems, which can block any program that is unknown to Panda Security from running until it has been classified. In return, cybercriminals are evolving towards more insidious attacks, abusing existing software tools once they manage to make their way onto the network. This leads us to believe that this kind of attack will increase in the future.

Most successful types of attacks against companies in 2018

Prevalence of malware attacks

Attacks utilizing RDP



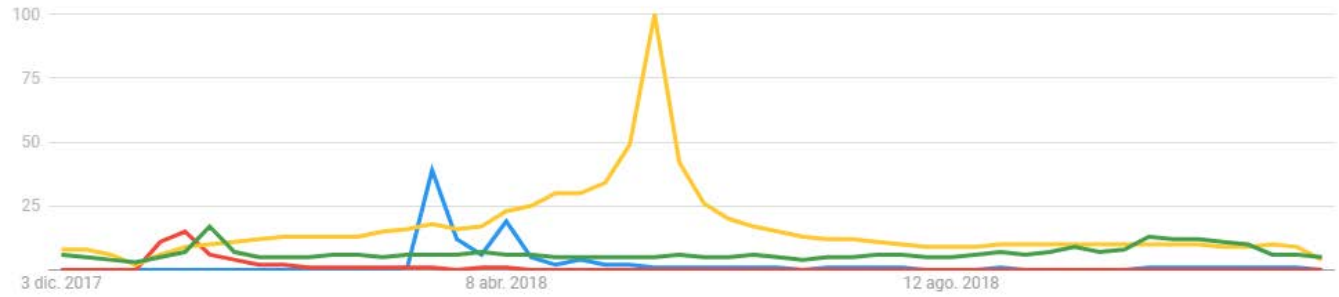
Boom of cryptojacking and Ransomware as a Service

While traditional techniques – phishing, ransomware, business email compromise – seem to be as fruitful as ever, the boom of attacks utilizing **RDP**, combined with other social engineering techniques, is consolidated as an entry vector for attackers. If we add to this the boom of **cryptojacking and Ransomware as a Service that we have seen this year, we have the three main attack types that have successfully undermined company networks in 2018**.

The main target for attackers is still the endpoint. This is where the most sensitive information is stored, and where they can abuse credentials that allow them to carrying out lateral movements and attacking other networks and systems. **However, the security budget for endpoint protection is approximately one third of that provided for network security.** -Source: Gartner-

It is no surprise, therefore, that given this budgetary limitation, most corporate endpoints are still protected by "traditional" technologies, which are not suitable for the cybersecurity challenges of today.

Neither is it surprising how successful many attackers are, given that on average it takes them much less time to compromise systems than it takes for them to be discovered. This lack of balance, along with a chronic lack of professionals in the sector, will, once again, continue to represent the main challenges for organizations when it comes to cybersecurity.



Google trends:

GDPR
Cambridge Analytica
Meltdown y Spectre

This chart confirms the fact that the GDPR has probably been the topic that has been of most interest in terms of search volume.

PandaLabs:

Threat Data in 2018

PandaLabs: Threat Data in 2018

However, most malware is stopped from running on the endpoint because phishing emails and URLs related to malware, the most common entry vectors, are stopped by Panda Security.

In this report, we will present the threat data corresponding to the most significant layers of protection, as reported by our installed base of endpoint-based corporate products, which are:

signatures (specific and generic), heuristics, behavior/context-based analysis, in-memory anti-exploit, and the 100% Attestation and Threat Hunting and Investigation services. These layers of protection are delivered both locally and from the cloud. Figure 1 represents the set of techniques used depending on the attack method

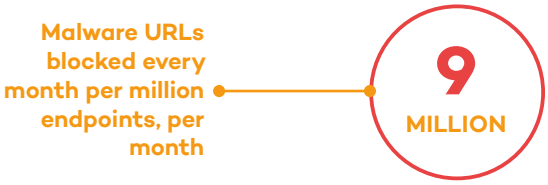
Figure 1. Protection technologies, attack methods and phases

Pre-execution detections

Most malware detected on protected endpoints in companies is identified using signatures and heuristics. However, most malware is stopped from running on the endpoint because phishing emails and URLs related to malware are blocked. While **the total amount of malware files that arrive at the endpoint is constantly growing (over 60% from the start to the end of the period), the risk that file-based threats pose for our clients has reduced dramatically**, to marginal levels. This is due to the efficiency of the integrated services, via products and services, and in particular due to the **"100% attestation" approach that Panda Security has taken, which, by default, prevents the execution of unknown executables until they are classified by PandaLabs.**

On average, **over 2.4 million malware files were detected and over 9 million malware-related URLs were blocked monthly per million endpoints.** Most of them were only seen once.

Analyzing the malware, the attack vectors and malicious codes on the rise in 2018, we can see that the prevalence of the malware categories detected in this stage hasn't changed much over the last year. **Trojans and ransomware represent most of these threats.** Relative to this, **the blocking of Malware-related URLs** (through direct web interactions or through embedded URLs in emails) happens at **over 3.7 times the rate** of malware file detections, **representing the biggest vector of entry for threats to the endpoint**, together with brute-force attacks against RDP, an attack vector predicted at the start of the year.



We believe **Internet-facing RDP connectivity represents a growing risk today** for many organizations, which are unaware of their exposure. Falling victim to this attack technique means continually being scanned by cybercriminals in search of easy opportunities to get onto the company's networks. The data recorded by PandaLabs corroborates the fact that approximately **40% of our mid to large clients are subject to this kind of RDP attack every month.**

As for the most common entry vectors and malicious codes this year, **email continues to be one of the most popular vectors for attack campaigns**, although many of them end up in the spam folder before they get to the endpoint. Users, particularly when using mobile devices, are more exposed to malicious URLs or infected websites.

In this regard, websites infected with Coinhive code are becoming a more pervasive threat, as a less aggressive form of cryptomining. Coinhive, initially designed to allow website owners to earn extra income without running advertisements, has emerged as a leading threat this year, with its code being installed on hacked sites without the knowledge of the owners. This unauthorized cryptomining service drains CPU cycles and power from devices for as long as the user visits the infected site. In fact, **cryptomining has grown 3.5 times more than during the same period last year**, whereas ransomware grew 2.5 times in the same period. In 2018, Monero miners represent almost 70% of the total number of cryptominers identified.

Pre-execution classifications.

Since new types of malware are created and published more quickly than detection capabilities are added, there is always a detection gap. This generates **inevitable infections of some "patient zero" users who don't have a more robust or complete protection.**

In order to close that gap and minimize infection risk for customers, in 2015, Panda Security introduced a "100% Attestation Service", which ensures that all Portable Executable (PE) files trying to execute on the endpoints must be classified as trusted by PandaLabs before being allowed to run. This security service acts as the last line of defense against file-based malware.

In the period January-November, a monthly average of approximately 5.8 million different executable files were observed per million endpoints. While most of the files are repeated from month to month, approximately 20% of them each month were unknown the first time they tried to run. 100% (99.98%) of these files were automatically classified, and an average of 1.3% were classified as malware.

Detection of attacks through behavioural and contextual analysis

The behavioral analysis module, which blocks actions based on their context of execution, can recognize hundreds of combinations of processes, process relationships, actions, etc., which are indicative of early stage attacks of various types (ransomware, miners, script-based attacks, among others). Paradoxically, due to the early prevention of the threat, it is impossible for us to determine the final nature of the threat, given that **attackers may also use a combination of techniques within the same attack**. The introduction of these prevention techniques represented a major success in the fight against dangerous threats for our customers, such as ransomware.

During the observed period, **the behavioral analysis module prevented over 15 thousand malicious actions** (e.g. a sequence of events indicative of an attack in its initial stages) **per million endpoints per month.** Abuse of PowerShell for fileless attacks is a foothold in the system, ranked as the top technique, representing almost 26% of these blockings.

The behavioural and contextual analysis module blocked

15
Thousand/month

Malicious actions

Per million endpoints

Detection of in-memory exploits

In-memory attacks, which exploit vulnerabilities in running applications, are detected using an integrated dynamic **anti-exploit module**. This module **detected an average of over 8,100 exploitation attempts during the period analyzed, per million endpoints per month. Internet Explorer and Outlook were the applications that suffered most attacks.**

PandaLabs Detected

8.100
exploit attempts per month

Per million endpoints

Threat Hunting

Attacks that seek to abuse legitimate tools already present in the environment, and which can be used with malicious intentions, such as administrative system management tools, represent one of the biggest threats today. The increased cyberoffensive capacity of groups or nation states using live hacking, malwareless techniques, and the difficulty (or rather, the impossibility) of detecting such infiltrations with conventional means all lead us to believe these attacks will become the top challenge for IT security departments.

This problem is compounded by the critical shortage in skilled security professionals. Some estimates calculate -Cybersecurity Jobs Report 2018-2021, from Cybersecurity Venture- that there will be a shortage of 3.5 million personnel by 2021. We believe that this is the most important challenge in cybersecurity today.

Panda Security's Threat Hunting and Investigation Service, as an integrated component of Panda Adaptive Defense solutions, **is aimed at identifying these attacks.** The service, provided by the PandaLabs team of experts, relies on proprietary tools to create and retrospectively test and validate hypotheses against all the activity being monitored across the installed bases, to investigate potential incidents and to help customers remediate confirmed ones.

In the period analyzed, approximately **90 incidents** were confirmed and investigated.

Examples of cases investigated by PandaLabs

Case #1. Large service company.

Suspicious outbound connections to China were detected in a system not protected by Panda, using telemetry from protected systems. Investigations led to the neutralization of a targeted Trojan designed to exfiltrate sensitive data. The Trojan "self-compiled" over 100 times, unsuccessfully trying to evade blockings by creating different variants of itself.

Case #2. Multiple customers.

A user received a targeted email with a Word document that was used to launch a script. This in turn invoked PowerShell to download a legitimate network connectivity tool (socat.exe) and Tor. The connectivity tool was being used to create a relay with Tor using local ports to hide it from network monitoring tools. This technique has been reported before in connection with Banking Trojans.

Case #3. Mid-Market customer.

The EternalBlue vulnerability was used to run a file directly in memory, including code to connect to a C&C server and to gather system information (OS version, security products installed, etc.), and steal user passwords. To avoid being detected, the targeted bot also tried to add its own location to the exclusions in Windows Defender, and included its own implementation of the Tor protocol. In one instance, the bot downloaded and installed a driver, a "Necurs" rootkit with functionality to disable numerous security products, and to look for the presence of process monitoring tools and stop its activity to avoid detection. In this case, the bot also downloaded and ran a modified XMRIG cryptominer as a service, without touching the disk.

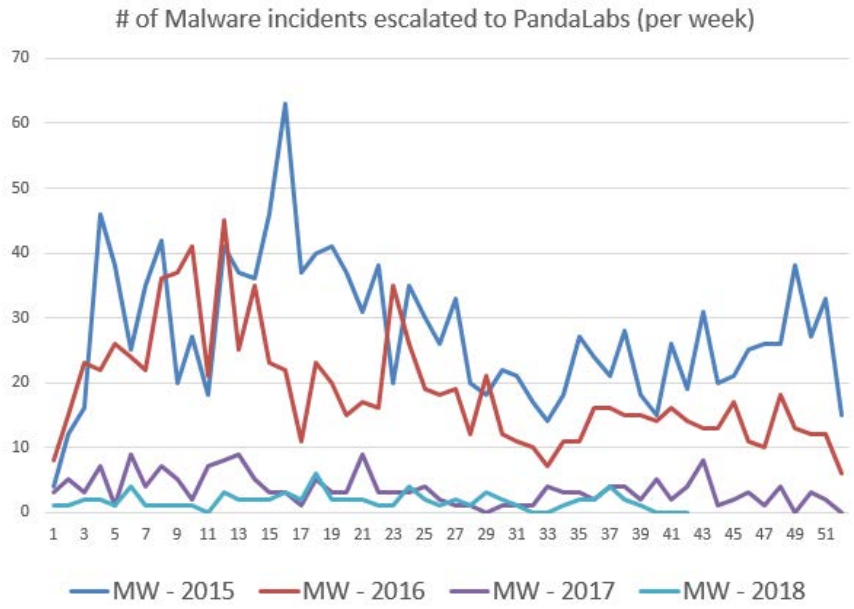
```
void __stdcall __noreturn threadWatchDog(LPVOID lpThreadParameter)
{
  OutputDebugStringA("MyWatchDogThread runned");
  while ( 1 )
  {
    if [redacted](L"taskmgr.exe") )
    {
      OutputDebugStringA("some monitoring stuff found! pausing..");
      [redacted](0);
      Sleep
      OutputDebugStringA("unpausing...");
      [redacted](1);
    }
    if [redacted](L"procexp.exe") )
    {
      OutputDebugStringA("some monitoring stuff found! pausing...");
      [redacted](0);
      Sleep(0x927C0u);
      OutputDebugStringA("unpausing...");
      [redacted](1);
    }
    if [redacted](L"procexp64.exe") )
    {
      OutputDebugStringA("some monitoring stuff found! pausing...");
      [redacted](0);
      Sleep(0x927C0u);
      OutputDebugStringA("unpausing...");
      [redacted](1);
    }
    if ( [redacted]"processhacker.exe") )
    {
      OutputDebugStringA("some monitoring stuff found! pausing...");
      [redacted](0);
      Sleep
      OutputDebugStringA("unpausing...");
      [redacted](1);
    }
    if [redacted](L"procmon.exe") )
    {
      OutputDebugStringA("some monitoring stuff found! pausing...");
      [redacted](0);
      Sleep(
      OutputDebugStringA("unpausing...");
      [redacted](1);
    }
    if [redacted](L"tcpview.exe") )
    {
      OutputDebugStringA("some monitoring stuff found! pausing...");
      [redacted](0);
      Sleep
      OutputDebugStringA("unpausing...");
```

The driver detects the presence of security programs and process monitoring tools, in order to pause its activity.

Malware incidents escalated to PandaLabs

The mission of Panda Security is to keep its customers free from security threats. All the above information about threats, techniques, technologies, and services would be meaningless if, in the end, our customers could not protect their IT and information assets, and fell prey to the attackers. So, as a critical metric to measure our success in the fight against cyberattacks, we include the number of incidents escalated to PandaLabs by customers, and its evolution in the last 4 years. The figure below shows the weekly number of escalated tickets, for 2016, 2017 and 2018, for all corporate and consumer products.

As we can see, **in 2018, the number of incidents escalated because of malware trends to zero**. The classification of all executable files, the visibility of all running programs and their activity, the efficacy of behavioral analysis in real-time upon the execution of authorized applications, and the continuous threat hunting services provided by the lab have all contributed to the situation of infections among clients trending to zero.



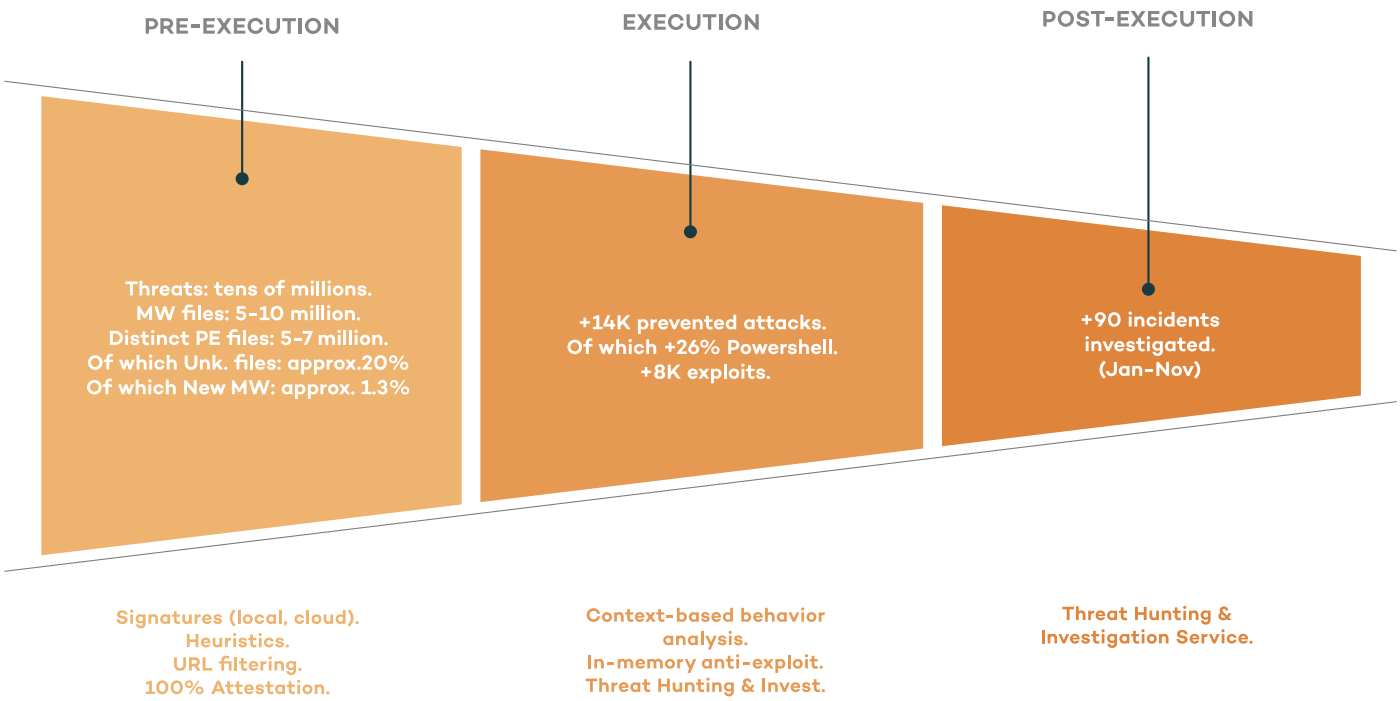
The "Threat Mitigation Funnel"

Threats targeting the endpoint can be characterized by their category or type (Ransomware, Cryptominer, Trojan, Fileless, etc., although many attacks use a combination of techniques), but also according to the level of sophistication or customization of the attack. **Protecting against highly sophisticated or customized attacks requires a higher maturity level of the endpoint protection capabilities.** Even though the single most effective mitigation measure an organization can take is patching, we don't expect significant changes in the average speed at which organizations deploy even the most critical patches. This is due to time or resource constraints, and also due to inconvenience and resistance from users. Nevertheless, **these days, threats can be greatly mitigated using next generation endpoint security defenses.**

Data shows that using a focus based on the classification of 100% of applications for unknown applications reaching the endpoint, together with a managed service that quickly resolves their classification, can bring the risk of file-based malware to marginal levels, with complete transparency and convenience for admins and users.

The graph below represents the mitigation of the threats observed on the set of endpoints analyzed, as the technology and service layers filter out the threats, characterized by their level of sophistication or customization.

«Threat Mitigation Funnel»



Cyber-news 2018:

Month by month

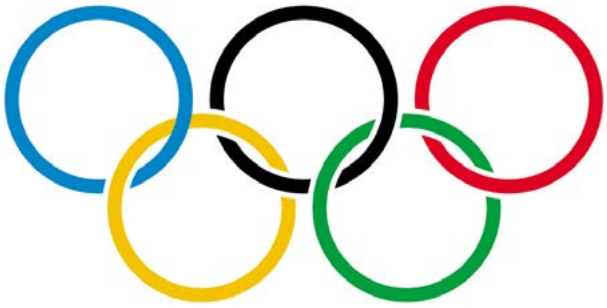
January

Meltdown and Spectre vulnerabilities

The year started with a big scare: the announcement of the "catastrophic" vulnerabilities Meltdown and Spectre (CVE-2017-5754), affecting the majority of modern day microprocessors. We won't go into too much technical detail here, since there is a lot of information available. We will simply note that we can breathe a sigh of relief since, so far, we haven't seen any real attacks, and its effects have been limited to a few performance problems, which you can consult here. There are some free tools for users to check if their systems are protected against the vulnerabilities.

Cyberattack on the Winter Olympics

During the opening ceremony of the Winter Olympics in South Korea, a cyberattack affected the Internet connection, the television service, and the website of the games. Although North Korea was initially blamed for the attack, the US intelligence services later attributed the attack to Russian agents.



February

"Infraud" cybercrime forum takedown

The US Department of Justice indicted 36 people and arrested 13 in conjunction with the takedown of the "Infraud" cybercrime forum. This group was responsible for more than $530 million in losses to consumers. Under the slogan, "In Fraud We Trust," the organization ran an illegal business forum for its 11,000 members, trading stolen identities, compromised debit and credit cards, personally identifiable information, financial and banking information, computer malware, and other contraband. You can find more information here.

March

"Cobalt" and "Carbanak" malware creators arrested in Spain

In March, of particular importance was the arrest of a Ukrainian citizen in Spain. According to reports, he is believed to be the brains behind the infamous Carbanak and Cobalt malware. According to the law enforcement agencies responsible for the arrest, the cybercriminal and his associates infected over 100 banks with the malware, which was used to remotely hack into ATM machines, stealing over $1 billion in less than a year.

Backdoors discovered in systems used by the UK government

In March, researchers discovered multiple backdoors in a UK Government contractor's systems, designed to steal government and military data. This attack has been linked to the group APT15, and it is suspected that the tool Mimikatz was used to gain system administrators' credentials.

April

Coinhive emerges as a top threat

Cryptojacking is the unauthorized use of a user's device to mine cryptocurrencies. Put simply, attackers use malware to take over these computers, tablets, or smartphones, and exploit part of their processing power to covertly mine cryptocurrencies. One of the most common techniques involves **appropriating the victim's CPU or GPU when they visit a website infected with cryptomining malware**, as recently seen on YouTube. In this case, the advertising platform **DoubleClick** was the victim of an attack that hid the Coinhive cryptojacking code in YouTube adverts. Indeed, Coinhive is the most commonly used script for this kind of attack. A study by the security researcher Troy Mursch has detected **50,000 websites infected with cryptojacking script**, with 80% of these using Coinhive.

May

VPNFilter – State-sponsored attack on SOHO routers

The FBI and the Justice Department in the US announced "actions" to disrupt the VPNFilter botnet, which affected hundreds of thousands of home routers from multiple manufacturers. The botnet is believed to be controlled by a group of state-sponsored actors. The malware was later found to have the capability to deliver exploits to endpoints via a man-in-the-middle capability. You can find more information here.

GDPR and some unintended consequences

In May, the much-anticipated General Data Protection Regulation (GDPR) came into force. Perhaps the most noticeable effect for users while the dust was settling was a deluge of consent messages asking for permission to keep their data on record, something that was leveraged by criminals by launching phishing campaigns.

Another unintended consequence of the new European regulation was the restriction of security research efforts for those using WHOIS, the system used to query the registration data of domain names and IP address ranges. The Internet Corporation for Assigned Names and Numbers (ICANN), the entity that oversees and manages the domain name system, proposed redacting some key information from public records in order to comply with the GDPR, thus limiting the investigation efforts of security researchers. In June, ICANN published a proposal to offer access to full WHOIS data for legitimate purposes, such as actions taken by law enforcement agencies, while also having adequate protection for personal data in line with GDPR. ICANN is now seeking feedback on the proposal.

Business Process Compromises in Mexico and Chile

Unnoticed by many security outposts, in May, several financial institutions in Mexico and Chile experienced cyberattacks. In Mexico, cybercriminals targeted applications and infrastructure used by several banks to connect to the *Sistema de Pagos Electrónicos Interbancario*, SPEI (the interbank electronic payment system). They were able to illicitly transfer over 400 million pesos (approximately €18 million). Days later, cybercriminals launched a two-pronged attack against Banco de Chile. The first one, believed to serve as a distraction, was a ransomware attack, which brought down thousands of PCs and ATMs, and had ripple effects over many third-party systems. The second one, which was the "true" attack, targeted the bank's SWIFT system. In this case, the attackers managed to transfer approx. $10 million from the bank's operating accounts to accounts in Hong Kong. No details have emerged about the techniques used by the attackers.

June

Products banned at European Union institutions

Following similar moves in the United States, United Kingdom and the Netherlands, on June 13, the European Parliament approved a resolution on cyber-defence which, among many other recommendations, called on the EU "...to perform a comprehensive review of software, IT and communications equipment and infrastructure used in the institutions in order to exclude potentially dangerous programs and devices, and to ban the ones that have been confirmed as malicious, such as Kaspersky Lab". Immediately after the news, Kaspersky suspended collaboration with Europol and the NoMoreRansom initiative.

This move by the European Union will bring even more attention to the geopolitical risks security organizations should consider when making purchasing decisions.

Cyberattack on satellites

In June, a cyberattack was discovered that, according to the researchers who spotted it, was launched from Chinese computers and targeted US and South East Asian satellites. These satellites belonged to defense companies and telecommunications operators. The objective of the attack was clear: espionage, specifically the interception of military and civilian communications. The researchers stated that the hackers were able to infect the computers that controlled the satellites, which means that, theoretically, they could have altered their locations.

July

Fake WhatsApp messages trigger mob killings in India

As a reporter explains, "Fake news is blamed for misleading voters and possibly influencing elections in the West. But in India, it's killing people". At least five people were beaten to death after fake rumors about child kidnapping were spread via WhatsApp. There were also reports of several other beatings across the country. The problem has forced the Indian police to launch an anti-fake news campaign, and the Indian government has demanded that the messaging app block these messages. The company will even introduce a new feature in the country to prevent users from forwarding messages to more than five people or groups at a time.

Russian spies indicted for DNC hack

On July 13, the US Department of Justice indicted 12 Russian spies for hacking crimes related to the 2016 presidential elections. The DOJ provided a detailed report about the tactics used and the operations carried out by the team of agents, who, according to the report, were members of the GRU, a Russian intelligence agency. Spear phishing was used to steal credentials of numerous individuals, robbing email content, hacking into their computers and planting hundreds of files of malicious code. To do this, the agency installed the malware X-Agent, which is capable of recording keystrokes, stealing files, and taking screenshots.

Sextortion

Spanish Police warned about renewed *sextortion* campaigns, with 6,000 reported victims since 2014. The campaigns use passwords collected in past data breaches, available on cybercrime forums, that may still be used by the victims. The victim is then led to believe that the hacker may have compromised their system and used the webcam to record a video while the victim was watching pornography, with the threat of releasing the videos if a ransom is not paid. According to Spanish police, the ransom demanded (in Bitcoins) may vary between €50 and €6,000.

Facebook fined for the Cambridge Analytica scandal

The Information Commissioner's Officer, the UK's privacy watchdog, fined Facebook £500,000, the maximum possible penalty, over two breaches of the UK Data Protection Act. Many consider this sanction to be just a slap in the wrist for the company, with revenue of over $40 billion in 2017. Under the new GDPR regulations, it is likely that the fine would have been much more substantial.

Maritime and shipping routes in danger

Many vulnerabilities have been revealed in the cybersecurity of the 50,000 ships currently at sea. It has been discovered that many of them are still using outdated systems – some of them even have Windows NT, from 1993, installed – together with exposed satellite communication terminals, user interfaces accessible via insecure protocols, and default login details that were never changed.

Security gaps in vessels can cause substantial damage, both to national industries and in the maritime environment, including ports, canals, and docks. The analysts suggested that by gaining access to ECDIS (the Electronic Chart Display and Information System, the electronic system used by these ships to navigate) it is also possible to gain access to the systems that warn the captain of possible collision scenarios. By controlling these collision alarms, attackers could bring routes as important as the English Channel to a standstill, endangering the imports and exports of a whole country.

August

Coordinated Inauthentic Behavior – Opinion manipulation

Acting on a tip from cybersecurity company FireEye, on August 21, Facebook announced the removal from Facebook and Instagram of 652 pages, groups and accounts (some originating in Iran and Russia) that had been engaging in "coordinated inauthentic behavior". These pages were being used to mislead others about who they were and what they did.

The same day, Microsoft announced that it had thwarted plans to attack the US mid-term elections in November. According to the tech company, hackers from the group Fancy Bear had created six web domains that were designed to look like International Republican Institute websites, and which were to be used in spear phishing campaigns.

September

Spyware reaches 45 countries

On September 18, it was revealed that a dangerous spyware called Pegasus had spread to 45 countries – 6 of which had in the past used spyware to abuse human rights. Developed by the **Israeli company NSO Group**, the spyware targets iPhones and Android devices, gaining access to them using phishing in order to launch a series of zero-day attacks and thus avoid security mechanisms. It is used to read text messages, track calls, gather passwords, trace location and compile data.

WannaCry charge

In September, the US Ministry of Justice took an unusual step: it officially charged a North Korean hacker for carrying out the WannaCry attacks, as well as for being implicated in the hacking of Sony Pictures in 2014, and the robbery of the Bangladesh Central Bank in 2016.

October

Cyberattack in the Netherlands

On October 4 the Dutch government reported that Dutch and British officials had interrupted a cyberattack against the Organisation for the Prohibition of Chemical Weapons in The Hague. It is believed that this organization was targeted because of its ongoing investigation into Russia's use of chemical weapons in Syria and the United Kingdom. In this case, four Russian agents have been accused, who are apparently members of the cyberwarfare team of the GRU. They allegedly travelled to the Netherlands with diplomatic passports. Their intention was to hack into the Organisation's network using equipment hidden in a car parked close to the HQ, and disrupt the office's computers.

Google Plus

On October 8, Google announced that it was to close its social network, Google Plus, due to a security flaw that had exposed the personal data of at least 500,000 users. The company assured its users that no hackers had been able to access this data.

November

New version of Stuxnet

The worm Stuxnet was first discovered in Iran in 2010. It is believed that it was developed specifically to attack Iranian nuclear power plants. On November 2, Gholamreza Jalali, Iran's Civil Defense chief, said that they had uncovered what is believed to be a new version of this attack. It was discovered trying to gain entry to the country's strategic networks and critical infrastructures

Amazon Black Friday data leak

With just hours to go before Black Friday, and with Cyber Monday just around the corner, Amazon informed some of its customers of a "technical error" in its website that had exposed the name and email address associated with their accounts. The e-commerce giant confirmed that the suspicious looking email sent to these users was in fact real, explained that the problem had been fixed, and that those customers affected had been notified. Unlike this leak, the one Amazon suffered the previous month was caused by an employee who was caught selling client data, and who was subsequently fired. In spite of Amazon's reassurances to the contrary, it is always a good idea to change your password after a security incident.

Data breaches.

The Year of the GDPR

May 25 was D Day, the day that the **GDPR**, the new General Data Protection Regulation, came into force across the whole of the European Union. Although companies had two years in which to adapt, in the end, the majority of cases saw a last-minute scramble to implement the new regulation.

Many companies were noticeably nervous and apprehensive, something that is understandable if we consider that the consequences of breaching the GDPR are severe, with **fines of 10 million Euros** or 2% of annual turnover (Level 1), or 20 million Euros or 4% of annual turnover (Level 2).

One of the most immediate consequence was the last-minute rush to comply with the new regulation. Inboxes were flooded with emails from companies asking for users' permission to keep their data on file, drawing consumers' attention to this eleventh-hour dash. However, many experts noted that these emails were unnecessary, since the companies already had these users' permission. This meant that many companies lost a large chunk of their contacts.

Despite having had a significant timeframe in which to get ready, many organizations seem to have been caught off guard; this was made clear by the fact that, one month after the implementation of the GDPR, several data protection bodies reported a significant increase in the amount of complaints and data breach notifications.

And it didn't take long for the consequences to appear. The first economic sanction given within the framework of the new regulation came at the end of October, when the Hospital do Barreiro in Portugal was fined €400,000 for two breaches of the rules.

Fines LEVEL 1

10.000.000 €

2% of annual global turnover

Fines LEVEL2

20.000.000 €

4% of annual global turnover

Social Networks: Facebook

This year, the most widely used social network in the world has faced several problems related to data protection and user privacy.

The first of these issues, uncovered in March, was the **Cambridge Analytica scandal**. Several newspapers published details of how personal data (PPI) of at least 87 million users was exploited without permission in order to try to influence the presidential elections in the United States. As a result, Mark Zuckerberg was obliged to appear before the US Senate's Commerce and Judiciary committees.

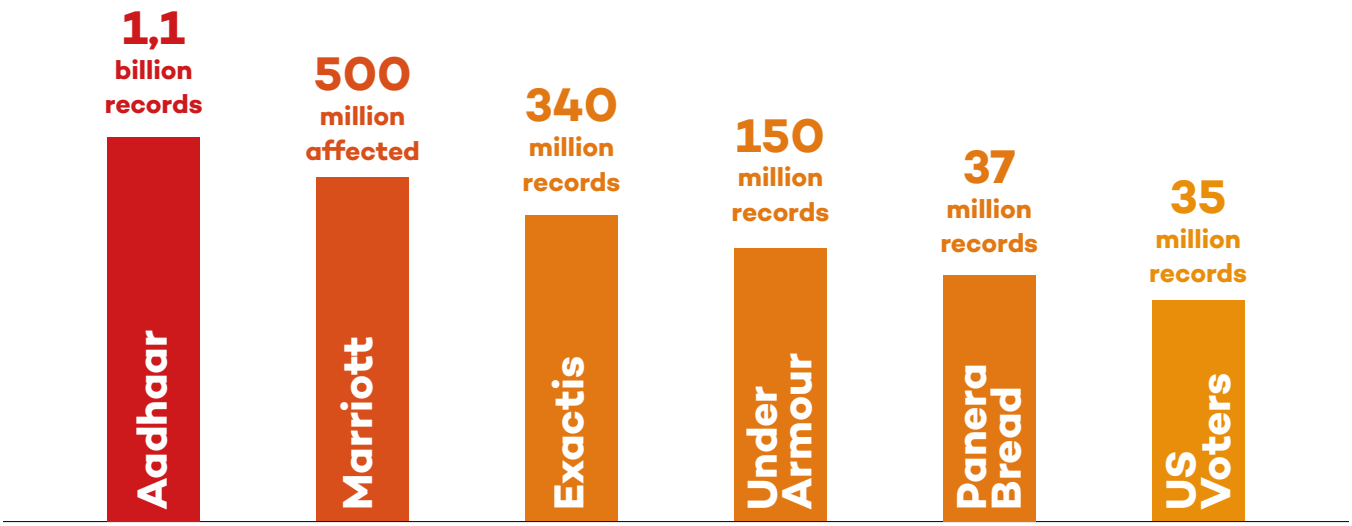
The Information Commissioner's Office (ICO) in the United Kingdom reacted by imposing a £500,000 fine, the maximum sanction possible under the data protection laws in place prior to the GDPR.

Then in September, nearly 50 million accounts were exposed in a cyberattack on the social network. The attackers made use of a vulnerability that allowed them to steal users' access tokens. In this case, the notification process and the consequences have been markedly different.

Following the rules set out by GDPR, Facebook notified the Data Protection Commission (DPC) in Ireland, where the company's European headquarters are located. However, it is yet to be seen whether there will be a fine —a fine that in this case could reach **$1.63 billion (€1.4 billion)**.

And just when it seemed as though nothing else could go wrong, in November a website was discovered selling the private messages of at least 81,000 compromised accounts. According to the owners of the website, they had the details of a total of 120 million accounts, which they were aiming to sell. Facebook, however, was quick to defend itself, stating that its security had not been compromised, and that the attackers had most likely used malicious browser extensions to access these accounts.

Unfortunately data breaches continue to make headlines on a regular basis. Here we provide a **ranking of the six most serious cases** between January and November according to the amount of records affected (or potentially affected).



1. Aadhaar (India).

Potentially 1.1 billion records.

Aadhaar, India's national ID database, contains records of 1.1 billion Indian citizens, including their biometric identification data. In January, journalists from a national newspaper reported that they were able to obtain any record of any registered individual in Aadhaar for 500 rupees (almost 6 Euros), from a WhatsApp group. They also obtained Aadhaar's printing software for an additional 300 rupees. The Unique Identification Authority of India (UIDAI), the agency managing the system, has strongly denied the claims of the breach. Then, several months later, in June, a security researcher reported that a data leak on a vulnerable system allowed anyone to download private information on all Aadhaar holders, exposing their names, their unique 12-digit identity numbers, and information about services they are connected to, such as their bank details and other private information. The UIDAI has also denied the claim and stated the database remained "safe and secure".

2. Hotel chain Marriott.

500 million customers affected.

On November 30, the hotel chain Marriott International revealed that the booking system of many of its hotel chains had been hacked, exposing the personal and private data of up to 500 million customers, in one of the largest data leaks in history. The potential value of the information exposed is so great that it has led to speculation that it was part of a state-sponsored attack, aimed at spying on the movements of diplomats, spies, military authorities and executives. Unauthorized access to the booking system of Starwood Hotels, which includes chains such as St. Regis, Westin, Sheraton, Aloft, Le Méridien, Four Points, and W Hotels, began in 2014.

3. Exactis (US).

Approx 340 million records.

In June, security researcher Vinny Troia discovered that Exactis, a US data broker, had exposed the records of approximately 340 million individuals on a publicly accessible server. According to Troia, each record contained up to 150 fields of information describing a person, including names, home addresses, and phone numbers. What's more, around half of the records contained email addresses.

A lot of the compromised records also contained data such as the number of children in a house, the ages of the children, the type of payment card used by that person, an estimation of the value of their house, if they have shares, their hobbies, their mortgage company, their ethnic group, their religion, along with many more fields. While the records did not contain social security numbers or bank details, they would be very useful for carrying out fraud or phishing attacks.

In this case, and for many of the other most important cases of the year, we are yet to see a definitive outcome. In Fact, Giovanni Buttarelli, the European Data Protection Supervisor, recently commented that the first fines will most likely be seen by the end of the year.

4. Under Armour (US).

Approximately 150 million records.

In March, Under Armour was the protagonist of one of the largest breaches of personal data in history. The company announced that the data of 150 million users of its popular food and nutrition application, MyFitnessPal, had been leaked when the app and the website were compromised. The company discovered that in February an unauthorized party had accessed usernames, email addresses, and hashed passwords of the users of the app.

5. Panera Bread (US).

Up to 37 million records (or more).

In April, after being contacted by security researcher Dylan Houlihan, Brian Krebs reported that the website of the casual restaurant chain Panera Bread had left millions of customer records exposed— including names, email and physical addresses, birthdays and the last four digits of the customer's credit card number. According to the researcher, the data had been exposed for 8 months, despite repeated notifications to the company after the leak was first discovered.

6. Voters in the United States.

Up to 35 million records.

In October, just a few weeks before the November 6 mid-term elections in the United States, up to 35 million voter records were discovered for sale on a popular hacking website. It was feared that these records could be used to influence the elections – including manipulation of voter lists at polling stations to stop people from voting. 19 states were affected by this leak.

Other relevant data breaches of 2018 were:

British Airways.

In September, the British airline revealed that between August 21 and September 5, cybercriminals had been able to steal the personal and financial data of over 380,000 customers. A group named MageCart was behind the attack, infecting the BA website with a malicious code that allowed them to gather British Airways customers' personal information. The latest figures on the incident, published at the end of October, suggest that 185,000 users were affected.

Orbitz

In March, the travel booking website Orbitz announced that **information pertaining to up to 880,000 payment cards** had been leaked, and that there was a possibility that the attacker also had access to more personal data and sensitive information of those affected.

Ticketmaster

In June, the ticket sales website Ticketmaster reported a data breach that affected up to 40,000 clients in the United Kingdom and other countries. The stolen information included payment card details, home addresses, and phone numbers. According to Ticketmaster, malware inserted into one of their customer support products was the cause of this breach.

Adidas

In June, the sportswear brand, Adidas, announced that clients of its US website may have been affected by a data breach. Although the company didn't reveal many technical details, this incident potentially affected millions of people.

T-Mobile

In August, the telecoms company T-Mobile was the victim of a cyberattack in which the personal data of around two million people was stolen. This data included names, phone numbers, account numbers, and ZIP codes.

SingHealth, Singapore

In July, Singapore suffered the "most serious" data breach in the country's history, when the **personal data of 1.5 million patients of SingHealth**, the largest healthcare group in the country, was stolen. **The personal information of the country's Prime Minister, Lee Hsien Loong, was among the data stolen**. According to the Singapore government, the attack was "not the work of casual hackers or criminal gangs." The attackers "specifically and repeatedly" targeted Mr. Lee's personal data.

Timehop

In July, the application Timehop announced that it had experienced a data breach affecting **21 million of its users**. Phone numbers, names, and email addresses were stolen, and the attackers may even have been able to gain access to the accounts of those affected. According to Timehop, the breach was possible due to a lack of security measures on their cloud account.

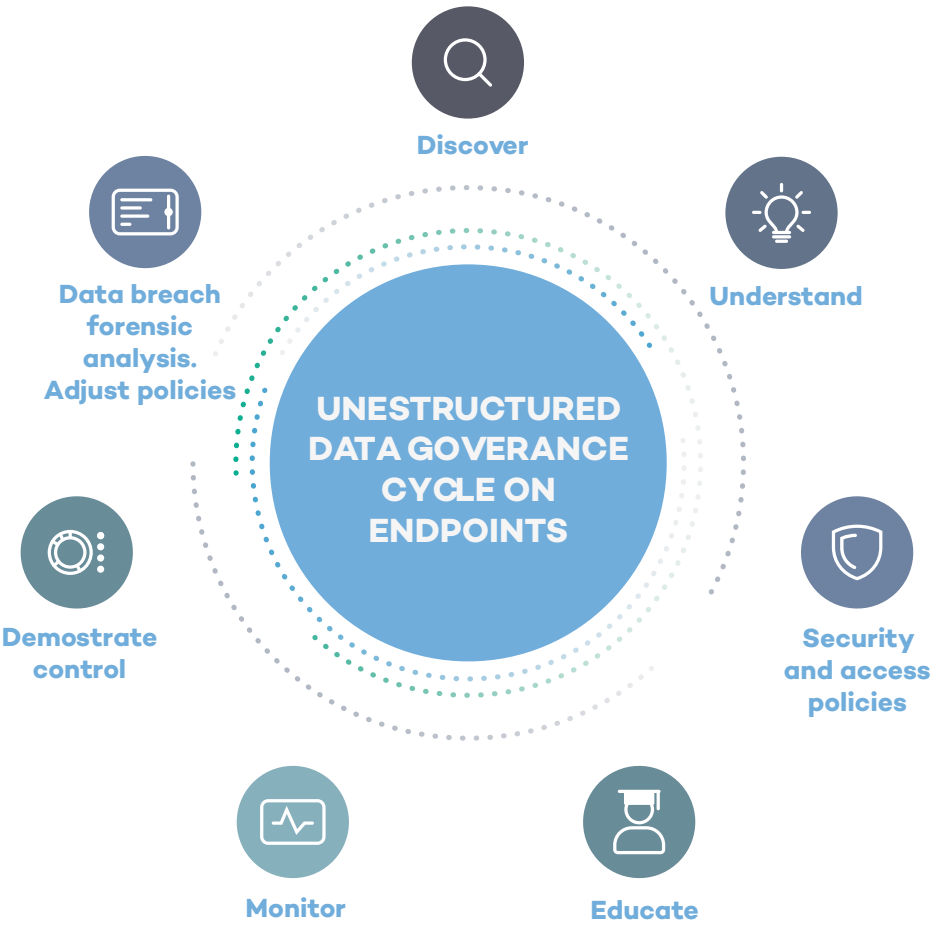
Don't be the next victim

Nobody wants their company to appear in the news as the latest victim of a security breach, with its ramifications for the company's reputation, its users, or its business. This is now more than ever the case, since GDPR came into effect. The main objective of this regulation is to protect the data of European citizens and to control how organizations process, store, and use this data, guaranteeing that it is secure, traceable, and correctly managed. This also includes the right to be forgotten. Malpractice in any of these processes now carries with it a series of extra consequences, such as **fines of up to €20 million or 4% of a company's annual global turnover.**

In order to avoid this outcome, the first step is to be aware of the importance of implementing effective security measures and policies. For organizations that handle data, prevention is a key aspect of the regulation. It is important to work with perspective and foresight as a competitive advantage in your business strategy.

Solutions like **Panda Data Control** are able to discover, audit and monitor unstructured personal and sensitive data on endpoints: from data at rest, to data in use and data in motion. This way, it is possible to avoid unwanted access to your company's sensitive data, guaranteeing that all personal data is registered and traced, and that you comply with regulations such as GDPR and PCI-DSS.

The control of personal data offered by **Panda Data Control** is vital in order to demonstrate to managers, DPOs and the authorities that your company has strict control over the PII found on your endpoints and servers. The definitive tool to justify any action you need to perform on this data: modification, confirmation, or cancellation.



Cybersecurity predictions 2019.

1. Live hacking.

Although "traditional" types of malware, such as Trojans or worms, are still being used frequently by attackers, new malwareless attack techniques will grow at a faster rate. This can be put down to an increased difficulty in detecting them on the one hand, and on the other hand, to the increased cyberoffensive capacity in the world, both of states, and of criminal gangs – both state sponsored and unaffiliated.

2. In 2019, the concept of digital sovereignty will also extend to security.

In 2018, geopolitics has played a more significant role in the digital realm, as a consequence of the more protectionist positions in the western world (The United States and the United Kingdom), the reactions of other powers (mainly Russia and China), and the increasing climate of mutual distrust among them. Countries such as France are taking measures to protect their digital sovereignty. **We believe that this trend will only increase in 2019, especially in Europe (which will move towards a European digital sovereignty)**, which will take shape as a fourth bloc against the American bloc (USA), China, and Russia. This will have an important effect in terms of cybersecurity strategies and policies, as well as purchasing decisions for products in this area.

3. Increase in supply chain attacks.

This type of attack is possibly one of the most dangerous; supply chain attacks involve infiltrating the development process of companies or legitimate software projects, into which attackers embed malicious code. This code is then distributed to the users along with the updates of this software. A case of this kind was recently detected in an open source project on GitHub, just one of many discovered throughout the year. In 2019, more cases like this are likely to be seen, given their effectiveness, the large impact they can have – since they can be spread rapidly to millions of systems – and given that the attack relies on the trustworthiness of a piece of legitimate software, which makes it more difficult to prevent.

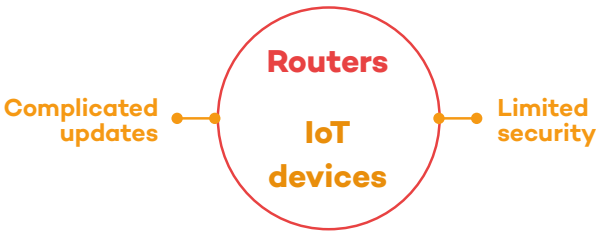
4. Artificial intelligence will become more widely used by attackers.

The same tools and knowledge that are used to analyze large volumes of data and to produce intelligent algorithms will become more widely used by attackers with malicious intent. This can be explained by the democratization of these tools, and their availability, as well as the availability of information about security products, all of which will allow algorithms to be designed that would automatically discover new ways to attack.

5. New catastrophic vulnerabilities will be discovered, similar to those discovered almost a year ago (Meltdown and Spectre). In the middle of November, and with little impact, a team of researchers discovered seven new attacks on processors. Two of these were variations of the Meltdown attack, and the other five variations of Spectre. We believe that the greater level of attention that these vulnerabilities received from researchers, given their impact, and the comparatively little research carried out so far compared to vulnerabilities in applications (which means there is a lot still to discover) will mean that we are likely to have more news about this, along with the consequent risk that functional exploits will be developed that will then end up in the hands of cybercriminals.

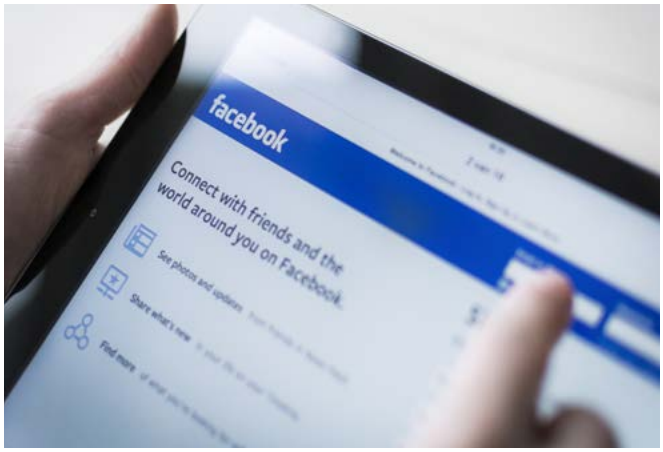
6. More attacks on routers and IoT devices:

Related to the previous point, and continuing the trend indicated by attacks such as VPNFilter – which affected an estimated half a million routers from a large number of manufacturers – in 2019 we are likely to see an increase in attacks not just on routers, but on IoT devices in general. **There are two main reasons for this: on the one hand, these devices' default security leaves much to be desired**, with default passwords or simply no passwords at all. On the other hand, **these devices are more difficult to update**, and many users don't even know how to do so. As such, their level of protection is far lower than other devices (PCs, laptops). This means that they can become easy targets for attackers, both to carry out DDoS attacks, and to distribute software such as cryptominers, with low costs and low risks for the attacker, especially now that the value of cryptocurrencies has fallen dramatically and legal mining operations have become less profitable.



7. Abuse of data, and fake news.

In March 2018, the Cambridge Analytica scandal came to light. It is estimated that it led to the data of approximately 87 million Facebook users being used for political ends without their permission. The massive analysis of data through readily available Big Data tools allows for the extraction of detailed profiles of personal preferences and trends in many areas, not just in politics. Just as fake news seeks to influence people's opinions and political behavior, personal information spread over different social networks (Facebook, Twitter, LinkedIn, etc.), correctly analyzed and correlated, can allow highly sophisticated and personalized social engineering attacks with malicious intentions to be developed. For example, using information extracted in this way, it is possible to impersonate someone – or a company – more effectively, and thus trick the victim into carrying out actions, or behaving an in undesirable way (such as making transfers to the attacker's bank account). These kinds of attacks (phishing, business email compromise), which have increased in 2018, will grow even more in 2019, given their effectiveness (it is estimated that on average 4% of recipients of emails that aim to deceive click on them), and the increased difficulty in detecting them.



In point of fact, the security needed to protect against these predicted trends for 2019, and against any other kind of illegitimate actions, lies in the concept of Panda Adaptive Defense's model: it is able to monitor, classify, and categorize absolutely every active process (100%) on all workstations on the corporate network. This includes those tools that are apparently legitimate, but which develop suspicious behaviors or become entry vectors for the network, such as RDP.

Panda Adaptive Defense is not a product; rather, it is a cybersecurity suite that combines Endpoint Protection and Endpoint Detection & Response (EDR) solutions with 100% Attestation, and Threat Hunting & Investigation services. This is the perfect combination of solutions and services to provide a detailed visibility of all activity on all endpoints, control of all processes running on the network, and reduction of the attack surface.

Panda Adaptive Defense automatically classifies 99.985% of processes, but behind that remaining 0.015% there is a human touch. Qualified PandaLabs analysts who, thanks to the 100% Attestation service, put a stop to the detection gap, ensuring the trustworthiness of all running processes. All of this allows them to react in terms of prevention, detection and response against both known and unknown malware. They can also react to attacks that don't follow traditional patterns, such as fileless or in-memory attacks. Moreover, the Threat Hunting and Investigation service also serves to perfect our Machine learning system, providing alerts about anomalous activities and behaviors from users, applications, and devices.

Prevention, detection and response for attacks with and without malware, in a single agent

Real time and historical visibility of all activity on all endpoints on the corporate network

Classification of 100% of processes: 99.98% via machine learning, and the other 0.02% by Panda analysts

Threat Hunting and Forensic Analysis: from the Panda experts and from our MSSPs investigate attacks in depth

Bibliography.

2. PandaLabs: Threat Data in 2018

https://www.pandasecurity.com/mediacenter/malware/no-kidnapping-no-ransom/

https://www.pandasecurity.com/mediacenter/security/evolution-cyberattacks-2017/

https://www.pandasecurity.com/mediacenter/security/what-is-cryptojacking/

https://www.pandasecurity.com/mediacenter/security/boom-fileless-malware-attacks/

3. Cyber-news 2018: Month by month

https://www.pandasecurity.com/mediacenter/security/meltdown-and-spectre-security-hole/

https://arstechnica.com/gadgets/2018/01/heres-how-and-why-the-spectre-and-meltdown-patches-will-hurt-performance/

https://www.grc.com/inspectre.htm

https://www.pandasecurity.com/mediacenter/pandalabs/cyber-sabotage-winter-olympics/

https://www.theverge.com/2018/2/25/17050868/winter-olympics-2018-russia-north-korea-cyberattack-opening-ceremonies

https://en.wikipedia.org/wiki/Infraud_Organization

https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

https://threatpost.com/china-linked-apt15-used-myriad-of-new-tools-to-hack-uk-government-contractor/130376/

https://thenextweb.com/hardfork/2018/03/07/wordpress-cryptocurrency-mining-malware/

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://www.pandasecurity.com/mediacenter/panda-security/1980-2018-gdpr/

https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/

https://www.pandasecurity.com/mediacenter/security/whois-protocol-gdpr/

https://www.pandasecurity.com/mediacenter/security/the-european-parliament-calls-for-reinforced-cyberdefense-in-europe/

https://www.roalddahl.com/shop/books/my-year-exclusive-museum-edition

https://www.npr.org/2018/07/18/629731693/fake-news-turns-deadly-in-india?t=1536657722588

https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

https://www.bleepingcomputer.com/news/government/us-charges-12-russian-intelligence-officers-for-hacking-dnc-running-dcleaks/

https://www.pandasecurity.com/mediacenter/security/gdrp-facebook-fine/

https://www.pandasecurity.com/mediacenter/security/danger-shipping-industry/

https://www.zdnet.com/article/microsoft-weve-just-messed-up-russian-plans-to-attack-us-2018-midterm-elections/

https://threatpost.com/dangerous-pegasus-spyware-has-spread-to-45-countries/137506/

https://www.pandasecurity.com/mediacenter/news/korean-hacker-charged-wannacry/

https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body

https://www.pandasecurity.com/mediacenter/news/cyber-security-glitch-google-plus/

https://www.infosecurity-magazine.com/news/stuxnet-returns-striking-iran-with/

https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-black-friday-2018-data-breach-a8645306.html

4. Data breaches

https://www.pandasecurity.com/mediacenter/security/gdpr-is-here-what-now/

https://www.pandasecurity.com/mediacenter/adaptive-defense/gdpr/

https://www.theguardian.com/technology/2018/jun/26/european-regulators-report-harp-rise-in-complaints-after-gdpr

https://www.itpro.co.uk/data-protection/28029/latest-gdpr-news-uk

https://www.pandasecurity.com/mediacenter/security/gdrp-facebook-fine/

https://www.pandasecurity.com/mediacenter/news/facebook-minimize-risks-vulnerabilities/

https://www.bbc.com/news/technology-46065796

https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

https://www.wired.com/story/exactis-database-leak-340-million-records

https://www.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUSKCN1MJ2AY

https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html

https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/

https://threatpost.com/up-to-35-million-2018-voter-records-for-sale-on-hacking-forum/138295/

https://www.pandasecurity.com/mediacenter/news/british-airways-hacked/

https://www.cnet.com/news/possible-orbitz-data-security-breach-affects-880000-payment-cards/

5. Cybersecurity predictions 2019

https://thehackernews.com/2018/06/ticketmaster-data-breach.html

https://www.bloomberg.com/news/articles/2018-06-28/adidas-says-millions-of-u-s-customers-being-alerted-of-breach

https://www.theverge.com/2018/8/24/17776836/tmobile-hack-data-breach-personal-information-two-million-customers

https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/

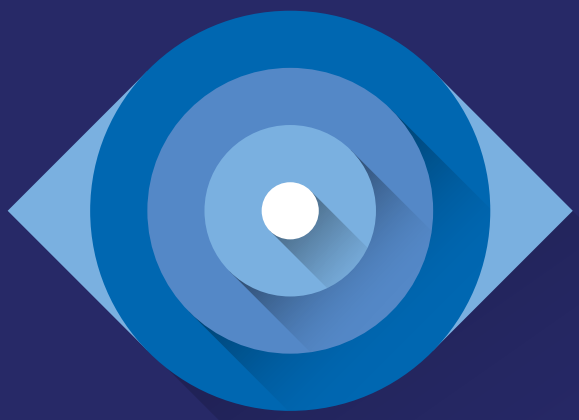
https://www.businessinsider.es/timehop-breach-21-million-users-2018-7?r=US&IR=T

https://www.wired.co.uk/article/google-france-silicon-valley

https://boingboing.net/2018/11/26/candy-from-strangers.html

https://www.zdnet.com/article/researchers-discover-seven-new-meltdown-and-spectre-attacks/

https://en.wikipedia.org/wiki/VPNFilter



panda

pandalabs