Eleven Paths

#CyberSecurityReport 18H2

innovationlab@11paths.com
elevenpaths.com

Telefonica CYBER SECURITY UNIT

Over 2018, many news related to cybersecurity have been published. From the entry into force of the GDPR, to the Cambridge Analytica's scandal, **privacy on the net is already a priority for users and governments.** Consequently, news on security breaches disclosing user data are currently in the general-interest journals and newspapers. Moreover, attacks performed by professional groups are no longer private issues. The alleged interferences in elections, espionage issues and sophisticated attacks are also public, for professionals of the field as well as for the general public.

Cybersecurity has such a presence that it is naturally mixed with general information, something that was unthinkable just some years ago. Indeed, **in 2018 the World Economic Forum placed cyberattacks among the first three global risks, and cybercrime is expected to have a cost of almost half a billion (1,000,000,000) euro per year.**

Nevertheless, it does not mean that this flood of information is correctly understood and analyzed, thus such information is not properly exploited to improve processes and be less vulnerable. Lack of information is as harmful as its excess. **To be updated and inform people is not enough, but it is also necessary to analyze and be able to prioritize, learn what is important and why.**

No matter if you are a cybersecurity professional or enthusiast, it is important that you can follow the rhythm of the relevant news on cybersecurity: What are the most relevant facts currently happening? What is the current outlook? How security problems, vulnerabilities and attacks are evolving? **It is necessary to summarize without losing depth.**

Given all the above, this report aims to summarize latest information on cybersecurity **(ranging from security on mobile phones to cyber risk, from the most relevant news to the most technical ones and the most common vulnerabilities),** while covering most aspects of the field, in order to help the readers to **understand the risks of the current outlook.**

In this way, the readers will be provided with a tool to understand the state of cybersecurity from different approaches, so they will be able find out its current state as well as to determine short-term trends.

The information here presented is mostly based on the collection and synthesis of internal data that have been contrasted with public information from sources considered to be of quality.

CONTENTS

THE MOST RELEVANT INCIDENTS OCCURRED OVER THE SECOND SEMESTER OF 2018

In the second semester of 2018, cybersecurity has been in the general-interest headlines, which constitutes a clear sign of the importance and influence of cybersecurity in all areas of society, ranging from political to economic and social aspects. In the following lines we will highlight the most relevant facts occurred over the second semester of 2018:

July

Magecart

Magecart, the name given to the virtual skimmer as well as to the cybercriminal group that created it, **attacked more than 800 e-commerce sites that had been previously compromised**. Magecart injected simple JavaScripts into the browser in order to steal credit card data and user identity while they were being used in a legitimate website. This performance culminated in the action against the British Airways' website some weeks later.

VPNFilter

The advanced malware targeting IoT devices that had been tied to the APT28 group, could have been **behind the attacks performed against the SCADA systems of a Ukrainian chlorine distillation station.**

Interference in the U.S. Congress elections

Microsoft declared that **the Russian Intelligence agency may have interfered in the U.S. Congress elections** held in 2018.

August

Coinhive

More than **200,000 MikroTik routers affected by a 0-day were compromised** and manipulated to inject the Coinhive Miner into user web traffic.

Malware in Taiwan

A malware impacted a number of Taiwanese companies working in chip manufacturing and **temporally prevented chipsets from being manufactured**, including those intended to be used in the most recent models of iPhone.

Apache Struts

The remote arbitrary code execution vulnerability in Apache Struts (CVE-2018-11776) **was massively exploited** to inject cryptominers **by using exploits derived from proof of concepts**.

September

Trinity

The FIN6 group attacked again with the malware called **'Trinity', designed to affect payment terminals**. Data from millions of credit cards were collected and transferred to be sold on the black market.

Xbash and Iron Curl

Palo Alto Network UNIT42 discovered the malware Xbash. It is a malware tied to the Iron Group with multiple capabilities: ransomware, cryptomining and botnets. Following that research, **at ElevenPaths we discovered a repository with all kind of resources belonging to the same group, in addition to a new creation: Iron Curl.**

Magecart

Magecart continued to cause troubles with new campaigns, one of them affected NewEgg, an online retailer with over 50 million visitors per month.

GreyEnergy

An ESET research allowed to discover GreyEnergy, a malware that caused **the first electrical blackout performed by a cyberweapon.** Known as GreyEnergy, this development of BlackEnergy has continued to target objectives, mainly located in Ukraine. According to ESET, its further developments are focused on increasing its capability to remain hidden.

Colourama

A malicious package was hosted in third-party libraries' repositories for the Python programming language (PyPI). This package, called 'Colourama' (leading to confusion with the actual package 'Colorama'), had a mechanism to keep track the clipboard and steal, when detected, user cryptocurrency data. By the end of October, there were already a dozen of packages detected that followed the same modus operandi.

CVE-2018-15454 exploitation

Cisco announced the detection of a massive campaign to exploit the vulnerability CVE-2018-15454, **impacting the SIP implementation within their firewalls.**

October

CVE-2018-8589 exploitation

In mid-November, the Russian firm Kaspersky announced **the detection of exploits that take advantage of the vulnerability CVE-2018-8589 (privilege escalation in Windows 7 and Windows Server 2008 via Win32k.sys)**. This exploit has been associated with the APT campaigns against Middle East entities.

MoneroOcean

Researchers from Juniper Networks announced that **misconfigured Docker services had been exploited** to install the cryptomining script MoneroOcean.

November

Marriot

Marriot security breach **has exposed data from 327 million of users** (passports, social security numbers… and in some cases also credit cards) that, in addition, had been exposed at least for 4 years, when Marriot acquired Starwood, that was already compromised.

Kubernetes

The first critical flaw for Kubernetes and other ones derived from it, such as OpenShift, was detected. The CVE-2018-1002105 vulnerability allows an attacker to gain admin privileges, and consequently to control any container cluster node. 1.0.x or 1.9.x versions were affected.

Facebook API

A flaw in the Facebook API, **that may have enabled an attacker to gain access to the photos of almost 7 million Facebook users**, was detected. Shortly after, it was discovered that Facebook may have been collaborating with the major technological companies and providing them user's private data.

December

MOBILES

In the hyperconnected world where we live, the number of terminals not only grows in quantity, but also in diversity. Mobiles and tablets have become an extension of our connection systems. Consequently, **your security is as relevant as any server or desktop computer's security.**

iOS and Android operating systems currently lead the market share. We analyze below **how security in iOS and Android has evolved over last months.**

Finding a method to avoid the lock screen has become a particular competition in each new iOS version. Two solutions were released for iOS 12: 12 and 12.1, published precisely to improve the first branch

Apple iOS

Remarkable news

In mid-September, it was released a proof of concept causing the reboot of those devices having an operating system earlier than iOS 12 (although it impacted the beta version) when visiting a web site purposely manipulated. The problem was in the Webkit engine used in Safari native browser when processing certain policies.

Over the second semester of 2018 Apple released its iOS 12 version. Not long after its release, several users reported that **that some messages from the application iMessages were mistakenly being sent to the wrong users.**

Finding a method to avoid the lock screen has become a particular competition in each new iOS version. Some weeks after iOS 12 was released, the researcher José Rodríguez discovered **a method to avoid the lock screen,** so the company had to release a patch (12.0.1) in order to address the deficiencies.

By the end of October, the first version 12.1 was released. Again, the same researcher that had previously discovered the screen unlock published a method to **access the contact list.** By the start of December iOS 12.1.1 was released, and this version fixes the mentioned error as well as other security ones.

To end the year, on December 17th iOS 12.1.2. was released. It was an exclusive update for iPhone devices, so iPads stayed at the 12.1.1. version. Interestingly, apart from fixing some minor errors, **for Chinese users this update was also aimed at avoiding a functionality that breached a Qualcomm patent.**

iOS 12 is compatible with iPhone 5S and earlier in the case of mobile phones, and with iPad Mini 2 (although iOS 10, still supported, works in iPhone 5 terminals and 4th generation iPads). These models are respectively five and four years old.

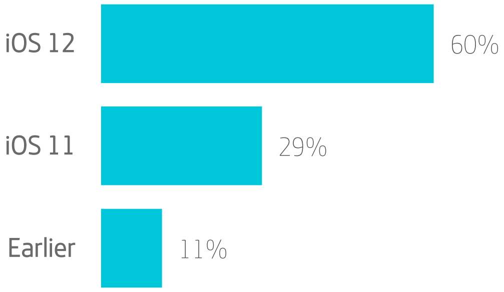
New security features[1]

Each new version of the operating system often comes with a number of developments regarding all the features, including security. In this regard, in the following lines you will find the new security features implemented with the 12 version:

- Safari **anti-tracking features** are enhanced.
- **Strong passwords** are automatically created.
- Passcodes received by SMS **will automatically appear** (one-time passcodes).
- **Passwords** are securely shared **between those devices associated** to the same identity.
- Integration of third-party **password managers** is improved.
- Identification of **previously-used passwords.**

iOS systems' fragmentation[2]

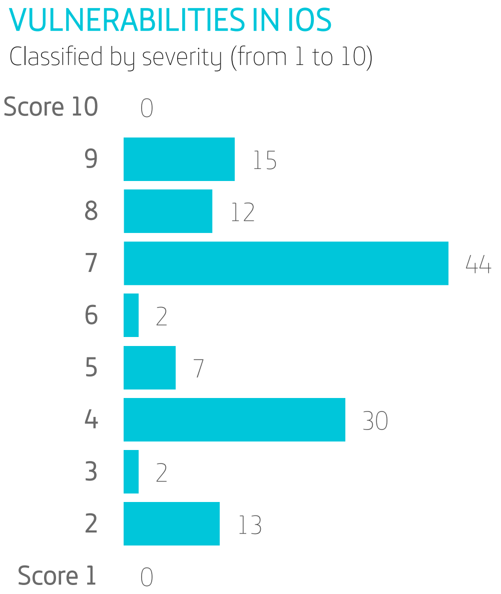
The data showed in the figure indicates that 60% of devices have integrated iOS12, 29% still work with iOS11, while 11% are classified as 'Earlier', i.e. devices working with operating systems earlier than iOS 11.



According to App Store, 29 th oct 2018.

Vulnerability evolution in iOS over the second quarter of 2018

A total of **125 vulnerabilities** of varying severity have been found, in the following graphic you can see their distribution by severity (ranging from 1 to 10):

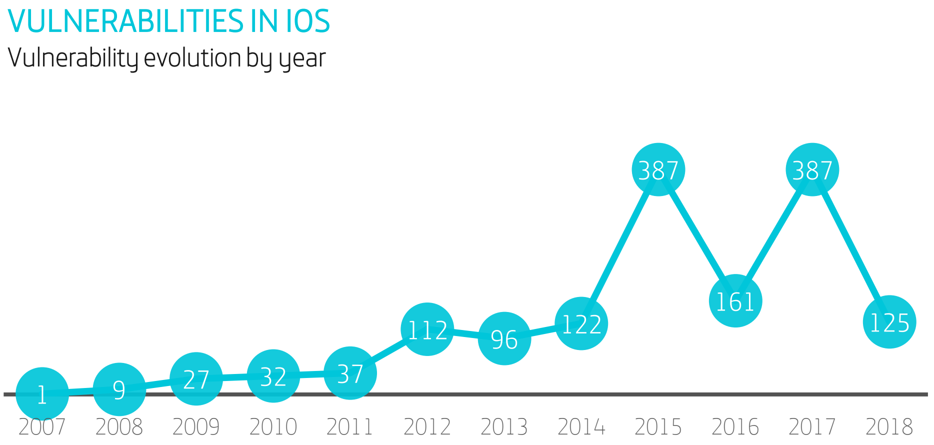


The new security features of the last iOS version are focused on improving the user experience regarding passwords, specifically their better management and use

[1] https://www.apple.com/ios/ios-12/features/
[2] https://developer.apple.com/support/app-store/

Vulnerability evolution by year in iOS

In this other graphic you can see a year-by-year evolution by cumulative number of vulnerabilities:



The number of vulnerabilities detected in iOS has grown significantly from 2012, with critical years such as 2015 and 2016

Android

On August 6th, Android released its ninth version: Android 9 or, as commonly referred by the codename, 'Pie'. As usual, **a great number of manufacturers have not still integrated this release in their latest updates.**

In mid-August, a new kind of attack affecting Android mobile terminals was reported: **'Man-in-the-Disk'. This attack could compromise legitimate applications, by manipulating the data they process on the external storage.** For a working example of the attack, the Android version installer of the so-called videogame 'Fortnite' was used. This error was discovered by Google researchers and made public after only seven days (instead of the 90-day timeline usually granted to complete the automatic update process). **Such initiative was not at all welcomed by the CEO of Epic Games, Tim Sweeney.** Some days before, Epic Games had announced that the game will be unavailable on Google Play Store.

By the end of October, 'The Verge' published details on a presumed contract by means of which Android device makers would be required to **roll out security updates for at least two years.** This way, they would be required to provide at least four security updates within one year of a terminal launch. Security updates would be mandated within the second year as well, although a minimum number of releases has not been specified.

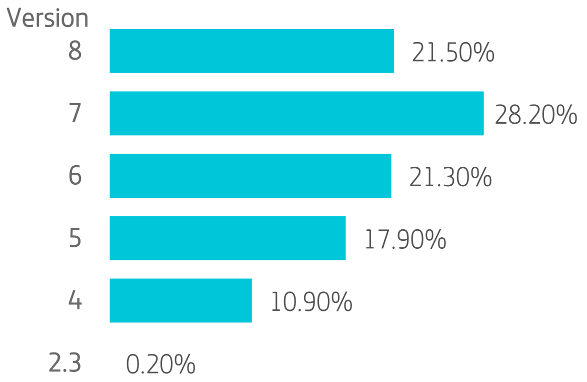
New security features[3]

Android 9 came with the following new security features:

- New **APK signature scheme,** which supports APK key rotation.
- Biometric support through the **BiometricPrompt API.**
- New antiexploit tools and countermeasures such as Control Flow Integrity, that detects dynamic changes from the control flow graph of a compiled binary.
- The file-based encryption is updated **(at a more granular level of disk encryption)** to work with adoptable storage.
- Update to Keymaster 4 and encryption improvements.
- Support for **metadata encryption** (where hardware support is present).
- Improvements regarding **SELinux** use and support.

Android systems' fragmentation

Fragmentation has been traditionally the greatest complaint of Android applications' developers, without forgetting security patches' reduced time of support. The state of fragmentation of Google's mobile operating system, Android, is as follows:[4]



These percentages represent the absolute number of versions (i.e., for ease of reading 4.x versions have been joined together, for instance).

These figures show a significant fragmentation**. A great number of Android operating systems are more than 2 years old.**

This means that **those versions earlier than Android 'Nougat' 7 don't have update support.**

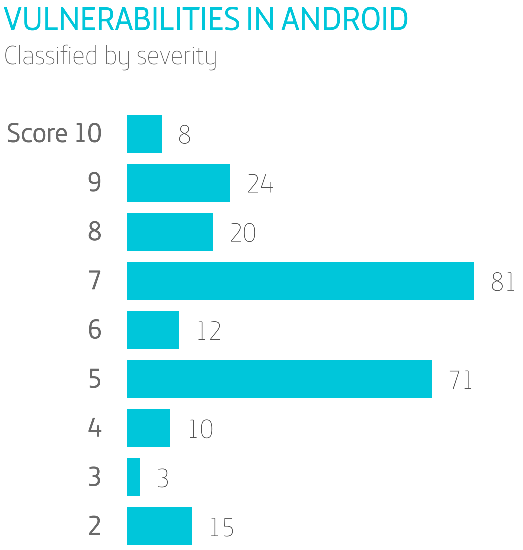
Last Android version security developments are based on a stronger and more granular encryption, as well as on the introduction of antiexploit security improvements

[3] https://source.android.com/setup/start/p-release-notes#security_features

[4] https://developer.android.com/about/dashboards/

Vulnerability evolution in Android over the second quarter of 2018

A total of **173 vulnerabilities** of varying severity have been found:



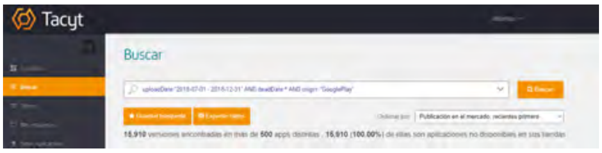
Average removing time of malicious applications from Google Play

We have examined **the time that Google Play (the official app store of Android applications) takes to remove malicious applications (or, as called by Google, 'Potentially Unwanted Application').** That is, the time that a given application is available to the public from it is uploaded by its author(s) until such application is removed from Google Play. The common reasons that lead to remove them from the official store are:

- The owner decides to remove it.
- The app violates the Google Play Terms of Service regarding an aspect not related to the malware (copyright infringement, for example).
- It is an aggressive malware/adware (or Potentially Unwanted Application, as named by Google) that violates the Google Play Terms of Service as well.

In this report we wished to analyze **Google's response capacity when facing the last circumstance mentioned: an aggressive malware/adware.** For this purpose, not only the fact that the app has been removed is taken into account, but **the app must also have been detected as a malware by several antivirus engines** in order to calculate its lifetime.

Our analysis covers the period between July 1st, 2018 and December 31st, 2018. The selected group of applications includes 15,910 applications removed at any moment within the period considered:

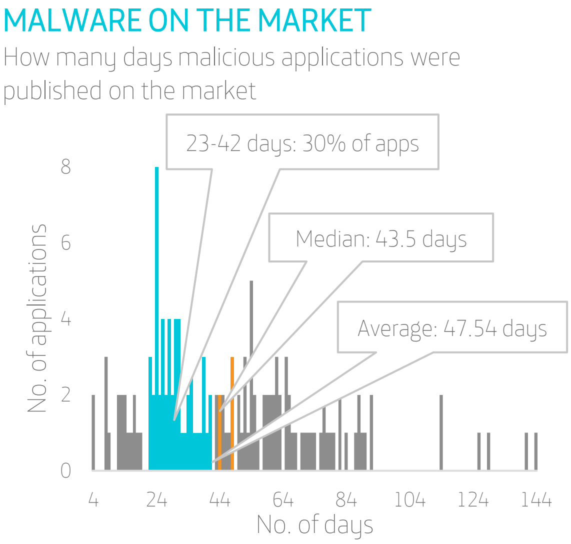


uploadDate:"2018-07-01 - 2018-12-31" AND deadDate:* AND origin:"GooglePlay"

Publicación en el mercado, recientes primero

15,910 versiones encontradas en más de 500 apps distintas . 15,910 (100.00%) de ellas son aplicaciones no disponibles en sus tiendas

We have analyzed a subgroup of more than 2,000 applications selected on an arbitrary basis, and we have got 142 malicious applications. In the following graphic you can observe the number of days until they were removed from the market:



It is interesting to highlight that it is possible that any application was not malicious or detected from the first moment it was uploaded, **but it has been updated with a more aggressive code in the subsequent updates.** In this case and for this analysis we have just considered those applications that were malicious from their first upload to the market.

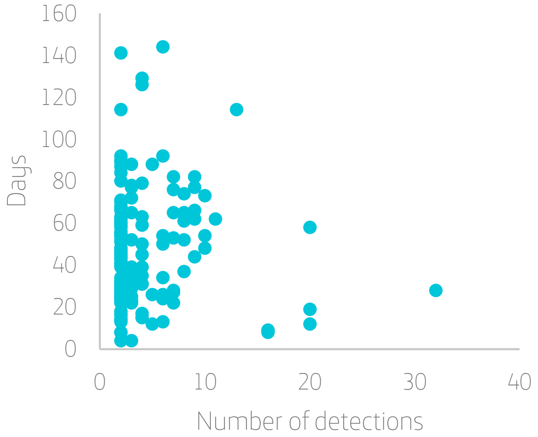
On average, the applications detected by any antivirus engine were more than 47 days on Google Play before being removed

Correlation between the number of detections (by engines) and the time such applications were on the market

This graphic means that, out of the three applications detected by 20 engines, two were removed earlier than 20 days and only one by day 60 regarding their date of publication.

VULNERABILITIES IN ANDROID

Correlation: Days on the market / positive No. of engines



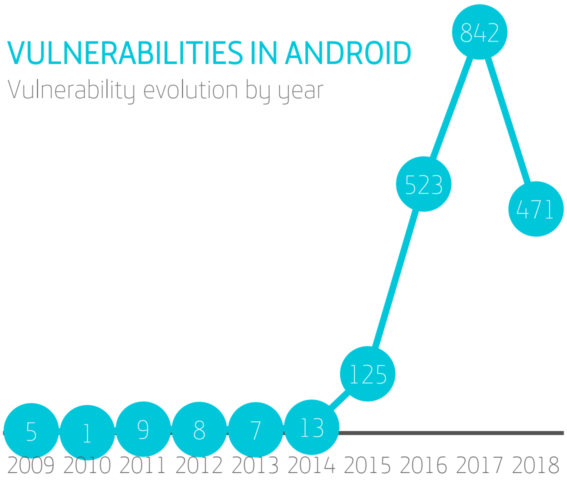
Annual evolution by cumulative number of vulnerabilities

As it can be observed, the trend or investment in Google's mobile system vulnerabilities has soared in the last three years.

Apps detected by less than 5 engines stay longer on the market, some being available up to 100 days. The more detected an app is, the shorter time it is on the market. However, there are some exceptions, for instance an app detected by 20 engines has been 60 days available to be downloaded

VULNERABILITIES IN ANDROID

Vulnerability evolution by year



VULNERABILITIES

Vulnerabilities are in many respects the cornerstone of cybersecurity. They are responsible for a lot of attacks and some **have such relevance that can alter the established ecosystem, alerting both attackers and defenders** and coordinating both managers and manufacturers. It is important to watch for those vulnerabilities that may alter the balance on the network. In order to apprehend the nature of the most common errors in the network-supporting programs, it is worth knowing how many weaknesses are appearing and which weaknesses are the most common ones.

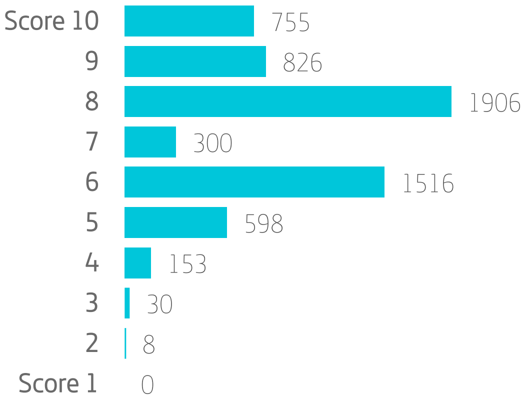
In this section we will discuss **some of the most remarkable vulnerabilities** over the second semester of 2018.

CVE ID	Target	Description	Scoring (CVSS v3.0)
CVE-2018-1002105	Kubernetes (open-source container-orchestration system)	Unauthenticated remote privilege escalation.	9.8
CVE-2018-17456	Git (version control system)	Arbitrary code execution via the recursively cloning of sub-modules.	8.8
CVE-2018-11776	Apache Struts 2 (web application framework for Java)	Remote arbitrary code execution.	8.1
CVE-2018-8453	Microsoft Windows from 7 to 10 and Windows Server from 2008 to 2016	Elevation of privileges using win32k.	7.8
CVE-2018-14665	Xorg (X11 graphical server used on UNIX)	Privilege escalation to root.	N/A
CVE-2018-10933	libssh (library written in C implementing the SSH protocol)	Authentication bypass.	9.1

Vulnerabilities in figures

In the following graphic you can observe the precise figures representing the vulnerabilities discovered (with CVE and severity assigned). The distribution of CVEs by level of severity (scored according to CVSSv3) is as follows:

VULNERABILITIES
Distribution of vulnerabilities by risk



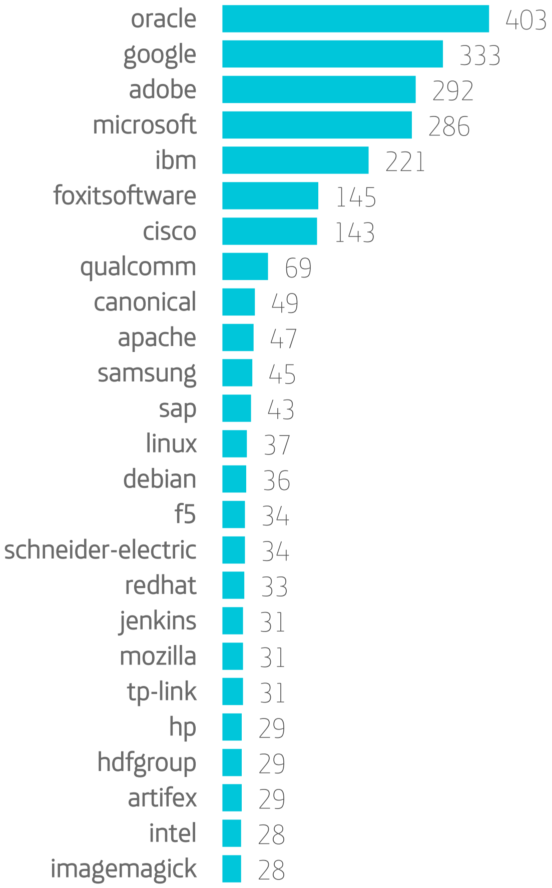
The reward programs implemented by technological companies **partly encourage researchers to focus on the most critical findings** (thereby the highest-rewarded) instead of on those that don't opt for the reward or are lower-rewarded.

A proof of the success of the reward programs is that from 2019 Europe will fund Big Bounties for 14 widely-used open-code projects

Top 25 companies with the highest number of CVEs gathered

It is worth stressing that these figures must not be interpreted as absolute figures, since some manufacturers have a number of products that could get a CVE. For instance, it is remarkable the difference between Oracle and the remaining companies. It may be due to **the immense Oracle's on-premise portfolio of products.** In contrast, Google's cloud applications don't get CVEs, since their vulnerabilities are internally fixed.

VULNERABILITIES
Top 25 manufacturers by CVEs gathered



As it can be observed, there is a higher number of vulnerabilities detected in certain types of software: **Adobe and Foxit's PDF readers,** or ImageMagick's library and utilities (whose code has attracted researchers' attention over the last periods).

Debian seems to have a low number regarding the quantity of patches they release for distribution. **However, only organization's own products are taken into consideration, so excluding those products they keep as third-party packages.**

Adobe deserves a particular attention: **almost all the CVEs correspond to their software Acrobat Reader, with 239 CVEs assigned.** A few years ago, Flash and Acrobat Reader were both malware vectors when they were executed in the context of the browser, as plug-ins. However, the inclusion of readers directly implemented on JavaScript and the virtual discontinuation of the Flash technology (replaced by web technology developments) have made this kind of products to be used out of the browser's context.

Nevertheless, opening a PDF email attachment by means of a viewer which has been set up to use one of these products, for example, would imply a potential infection if the reader remained vulnerable. For this reason, it would still be a relevant vector to be considered.

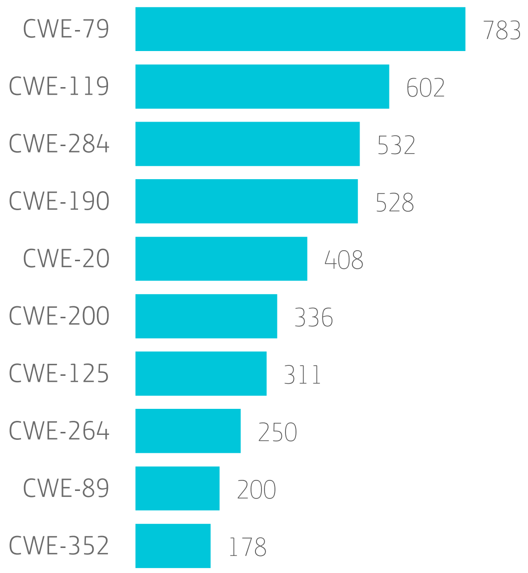
Top 10 the most significant CWEs

CWE (Common Weakness Enumeration) is a list of common security weaknesses identified in software products. Similar to the CVE effort for categorizing the specific vulnerabilities found per product, CWE is focused on abstractly defining the security weakness types. This allows the performance of a direct mapping between CVE and CWE.

This list includes **the 10 most-assigned CWEs by number of CVE,** allowing us to observe the most frequent category of weaknesses over the period analyzed.

VULNERABILITIES

Top 10 the most significant CWEs



The following table includes a description of each CWE presented in the previous graphic:

CWE	Name	Description	Number
CWE-79	Improper Neutralization of Input During Web Page Generation	It basically includes the three well-known types of vectors used to perform a Cross-site scripting: Reflected, stored and DOM based.	783
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	It generally includes programming errors where the bounds of a memory buffer are not being controlled, both in read or write operations.	602
CWE-284	Improper Access control	The application does not correctly restrict access to resources. It is a generic category where you can find those flaws related to the lack of an appropriate control or prohibition when third-parties can access resources even if they do not have the appropriate permissions.	532
CWE-190	Integer overflow or Wraparound	It occurs when an integer value is incremented to a value that is too large to be stored. In such a case, the value may wrap to become a very small or negative number.	528
CWE-20	Improper Input Validation	Generic category that includes errors consisting of an inappropriate or non-existent user data input.	408
CWE-200	Information Exposure	It generally includes compromising sensitive information due to a lack or flaw of controls that could prevent an information leakage from happening.	336
CWE-125	Out-of-bounds Read	Highly related to CWE-119, it includes read memory operations exceeding the control bounds of an intended buffer.	311
CWE-264	Permissions, Privileges and Access Controls	It is a generic category including all the flaws related to the permissions and privileges granted to users and processes, as well as to resource access control (in this sense, it is related to CWE-284).	250
CWE-89	Improper Neutralization of Special Elements used in a SQL Command	Related to CWE-20 but specialized in SQL code. The application is unable to correctly filter data streams coming from the user, so causing uncontrolled access to the database.	200
CWE-352	Cross-site Request Forgery (CSRF)	Lack or flaw of mechanisms allowing to discern if a web request has been intentionally submitted by the authenticated user or if such action has been, conversely, launched by a third-party in the context of a user's ongoing session.	178

The most common errors can be generally classified into three types:

- **Lack of appropriate controls** to monitor a correct authentication, authorization and tracking of the use of privileges: the so-called AAA Protocol (Authentication, Authorization and Accountability).
- **Lack of secure user data filtering.**
- Errors in the **management of the dynamic memory.**

There has been no significant movement towards one general type or another. The classified errors remain at similar figures when they are classified into the three mentioned categories. For example, the first three CWEs from the classification have similar figures and shape accurately the mentioned division.

The lack of appropriate controls regarding the AAA Protocol falls under every range of applications, although, of course, it is more common in those applications having a user hierarchy, with their respective permissions and privileges, namely operating systems and web applications.

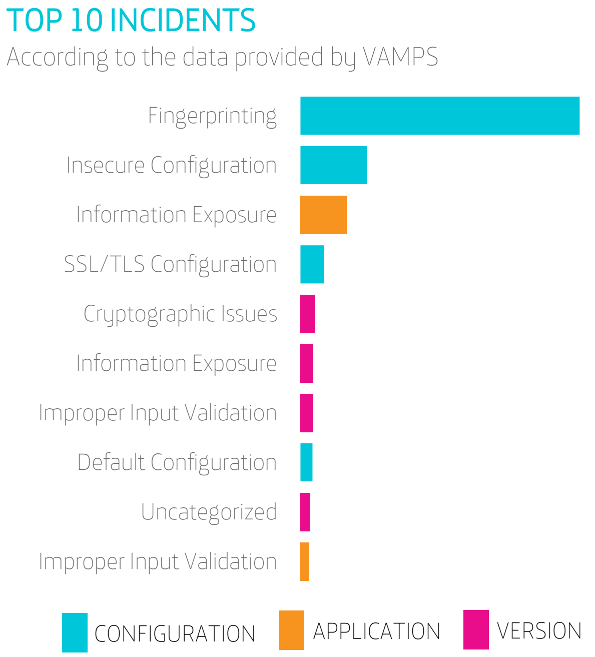
The second category is closely related to web applications where user access may cause various harmful effects if it is not controlled: cross-site scripting, SQL injections, injections resulting in command execution, local or remote files inclusion, etc.

The third category rules out almost completely web applications, since memory management is related to operating systems and native code.

According our monitoring systems for clients, the most frequent security problems are far and away those related to applications and services' configuration, followed by problems derived from previous versions.

Top 10 most common errors and their consequences (by VAMPS)

A list of the 10 most common errors (per number of incidents) reported from our clients thanks to VAMPS Is given below:



In contrast to the information provided in previous sections, **these data show the everyday life of the working systems, and are periodically audited.** The most common errors are still those derived from a mistake or those due to an improper deployment. Most of the entries show the need to apply security policies including the appropriate instructions to perform a secure deployment as well as the controls allowing to detect and fix flaws or security policy failures, for instance: forgotten but accessible files (both configuration and documentary files) from which sensitive information can be extracted. Within insecure configuration, we can also include non-updated TLS or the lack of headers preventing other type of attacks from happening.

APT OPERATIONS, ORGANIZED GROUPS AND ASSOCIATED MALWARE

In this section we will go over the activity of those groups that are supposed to have performed APT operations or noteworthy campaigns. However, as it has been shown on many occasions, **the authorship of this kind of operations, their structure as well as the origin and ideology of the organized groups is highly complex, so it must not be, by definition, entirely reliable.** The actors may use (and so they do) the means to manipulate the information in order to hide their actual origin and purposes. As is the current practice, in certain cases some groups adopt other groups' modus operandi, so that they can divert attention and undermine them.

APT operations detected over the second semester of 2018

Campaign	Publication	Group	Malware	Targets	Notes
GOLDFIN	Accenture (August 2018, but it is supposed to be working from February 2017)	CANDLEFISH (Patchwork, Dropping Elephant, Chinastrats)	SOCKSBOT	Financial institutions in the Commonwealth of Independent States (CIS)	• Use of spear-phishing • Infrastructure overlap and shared use of a PowerShell obfuscation technique with FIN7
GlanceLove	Check Point Research (July 2018, but it is supposed to be working from November 2017)	Israeli security agencies argued that the campaign would have been organized by Hamas	Several Android applications from Google Play, the official app store of Google	The Israeli military	• Phishing by an infected 2018 FIFA World Cup schedule and results checker • Steal users' credentials from browsers and email managers, images, contacts, etc. • Modular-code malware with specialized components
LeafMiner	Symantec (July 2018)	LeafMiner		Middle East companies	• Use and modification of public exploits (Fuzzbunch framework, Eternal Blue…) • Use of techniques such as Watering Hole
Operation DOOS (summer 2017)	Area 1	OilRig (IRN2)	Helminth	Oil and gas companies from the Middle East	• Use of PowerShell and VBScript • Use of Phishing • Use of Excel documents with malicious macros
Operation Red Signature (July 2018)	TrendLabs (August 2018)	Unknown	9002 RAT	South Korean Organizations	• CVE-2017-7269 is exploited • Database credential dumper
Operation Red Signature (July 2018)	FireEye (July 2018)	TEMP.Periscope (China)	EVILTECH, DADBOB	Cambodian government and entities (as well as other regions such as the U.S., Europe and the Middle East)	

New organized groups identified over the second semester of 2018

Group	Origin	Publication	Targets	Notes
DARKHYDRUS		PaloAlto Networks -UNIT42 (July 2018)	Government agencies in the Middle East	• Use of spear-phishing • Use of domains such as micrrosoft[.]net, cisc0[.]net, 0utl00k[.]net, allexa[.]net and other similar ones
Gordon Group	It might be Pakistan	PaloAlto Networks -UNIT42 (August 2018)	Undefined. Performances have been detected in the UK, Spain, Russia and the US, among others	• Use of URL shortening services to download payloads • Use of multiple malicious office documents, with macros and use of PowerShell

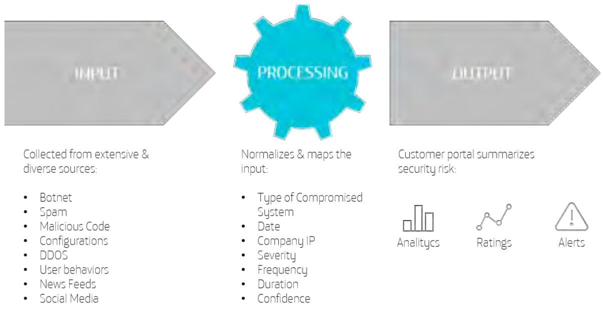
Malware associated to ongoing APT operations or detected over the second semester of 2018

Malware	Group	Origin	Targets	Publication	Notes
QUADAGENT	OilRig (APT34, Helix Kitten)	It is likely to be the Middle East	Mainly the Middle East, and other targets as well.	PaloAlto Networks - UNIT42 (July 2018)	• Vector: malicious macro embedded within an office document • Use of .Net and PowerShell • Use of spear-phishing strategies • Use of public code: https://github.com/danielbohannon/Invoke-Obfuscation
BISKVIT	Unidentified	Unknown	It is likely to be the Russian military staff	Fortinet (August 2018)	• Malware coded in .Net • Use of phishing (Russian e-mail on military issues) • CVE-2017-0199 is exploited (linked to previous operations)
Final1stspy	APT37, Group123, Reaper	North Korea	They are likely to be the Middle East and South-East Asia	INTEZER (October 2018)	• It shares code and infrastructure with malwares such as ROKRAT, NOKKI and KONN, among others

Spear-phishing and malicious office documents (mainly through macros) are the most common infection methods used by the analyzed groups, both by new and repeated groups,regardless their origin

CYBER RISK RATING ON A SECTORAL BASIS

We have used the BitSight cyber-risk-measurement technology and its Security Rating Platform to set out a security comparison between industries.



Collected from extensive & diverse sources:

- Botnet
- Spam
- Malicious Code
- Configurations
- DDOS
- User behaviors
- News Feeds
- Social Media

Normalizes & maps the input:

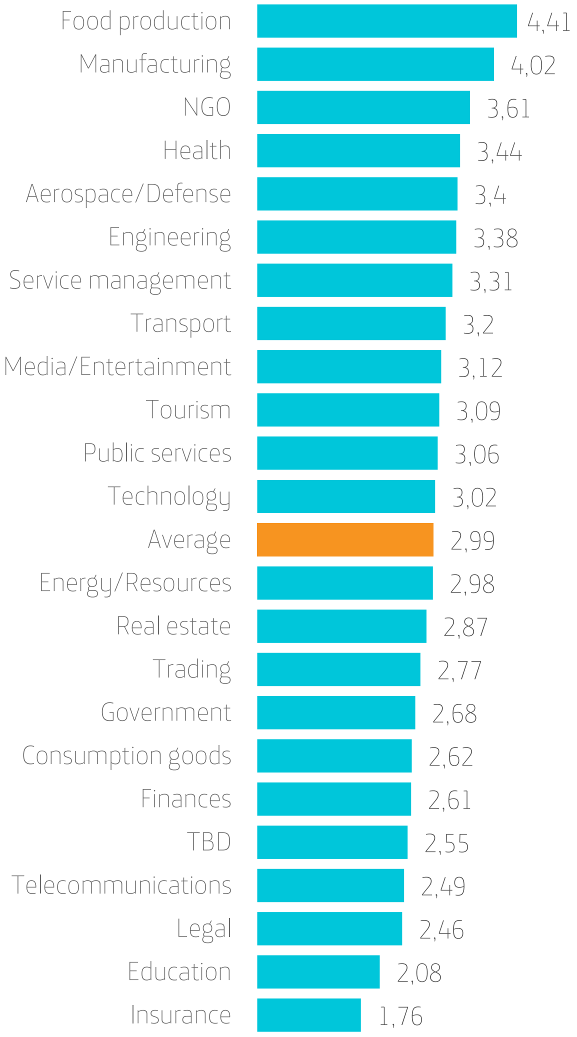
- Type of Compromised System
- Date
- Company IP
- Severity
- Frequency
- Duration
- Confidence

Customer portal summarizes security risk:

BitSight generates objective and quantitative measures of a company's security performance on a daily basis. Policies, rules or good practices are not monitored, nor network analysis are performed. **Incidents, external evidences are included (for instance, command and control connections from a company's IP, leaks in social networks...), as well as other data that, thanks to BitSight algorithms, provide an approximate idea of security in a given company,** even including its technological providers. This implies one of the most accurate ratings on cybersecurity risk. The ratings are based on four classes of data: compromised systems, diligence, user behavior, and public disclosures.

With this technology, we have been able **to distil relevant information on the security practices undertaken by the European industrial sector,** and also compared to Spain, as you can observe in the following example:

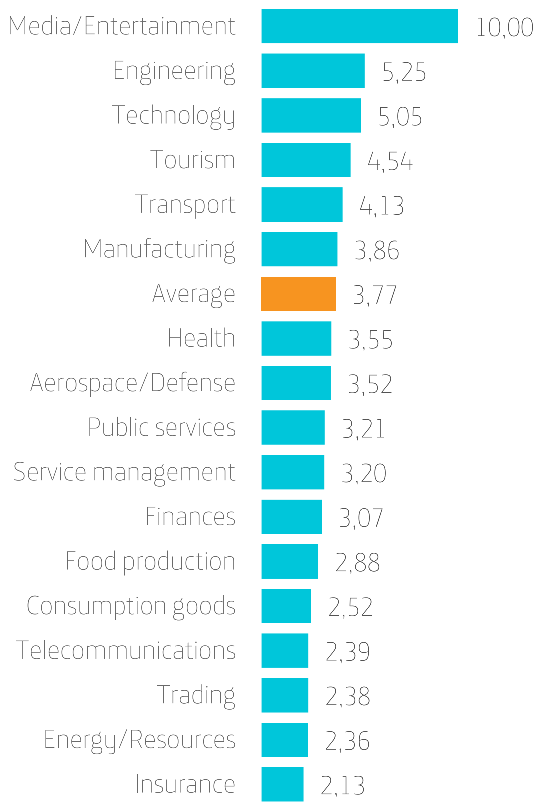
Average number of effective days needed by a European company to fix a malware threat (grouped by sector)



European food production companies need an average of 4.41 days to fix their malware problems, while insurance companies solve them in less than 48 hours.

By focusing on Spain, the average is as follows:

Spanish average from threat detection to neutralization, grouped by sector

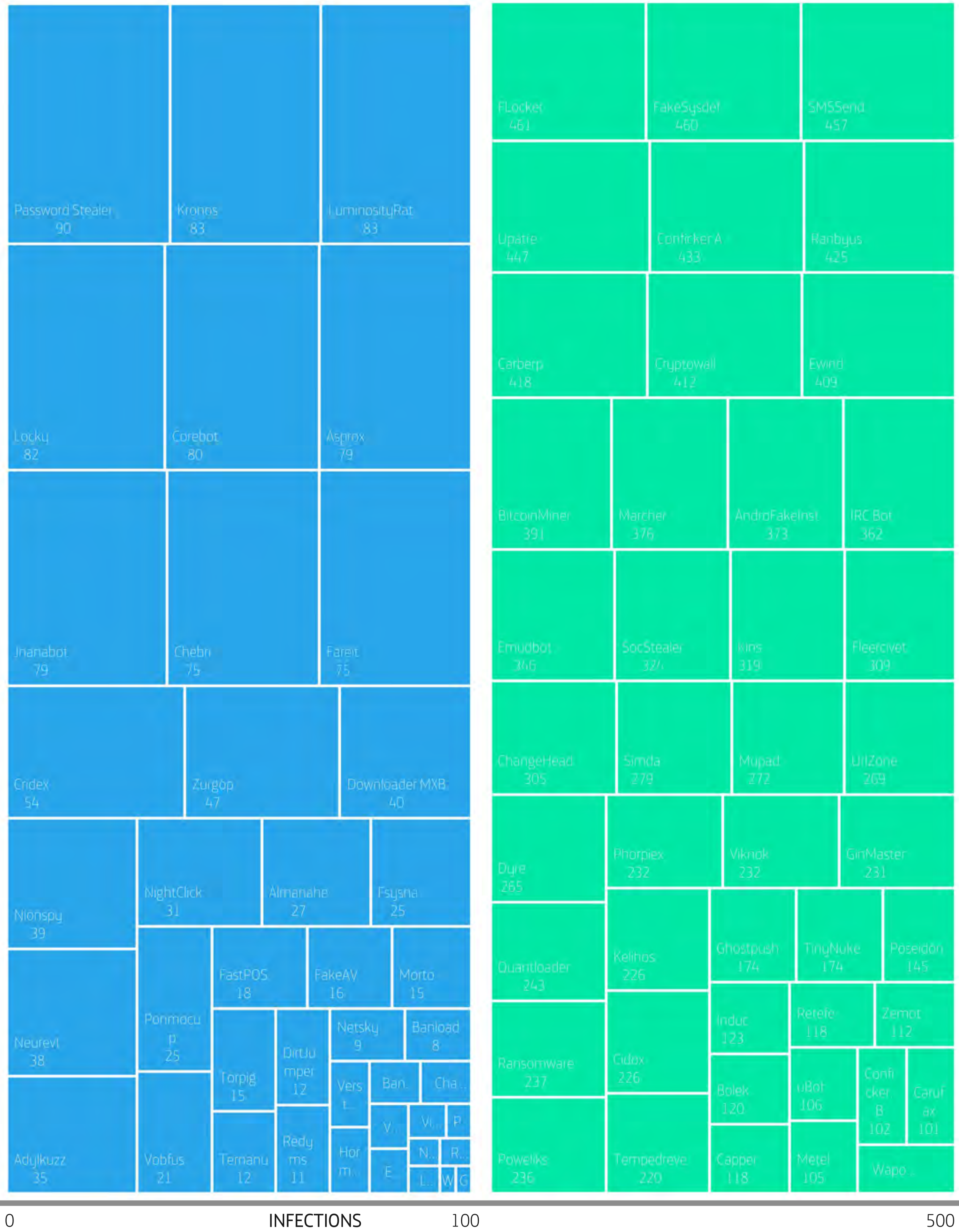


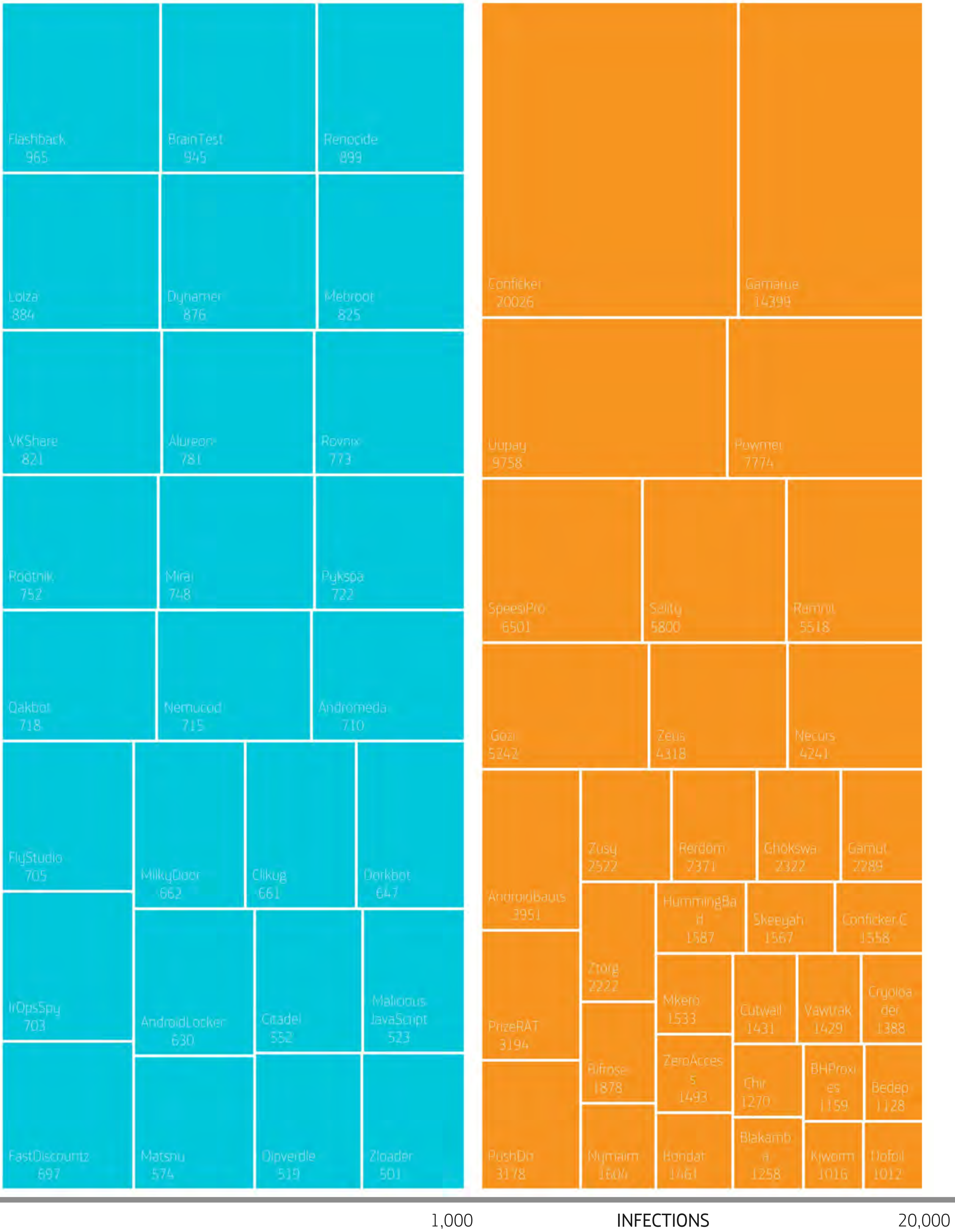
As it can be observed, **the Spanish average (3.77 days) is higher than the European average.**

Thanks to the BitSight technology, **we can find out as well what have been the most detected malware and infection families in Europe and Spain.**

Bitsight technology provides an innovative vision on companies' cyber risk. It is based on compromised systems, diligence, user behavior, and public disclosures. In the metrics here presented, grouped by sectors in Europe, we have analyzed the celerity to fix incidents and the most common malware within their infrastructures.

The following graphics include the name of the detected sample's family and the number of infections or prevalence over the last months.


Password Stealer 90
Kronos 83
LuminosityRat 83
Locky 82
Corebot 80
Asprox 79
Jnanabot 79
Chebri 75
Fareit 75
Cridex 54
Zurgop 47
Downloader MXB 40
Nionspy 39
NightClick 31
Almanahe 27
Fsysna 25
Neurevt 38
Ponmocup 25
FastPOS 18
FakeAV 16
Morto 15
Torpig 15
DirtJumper 12
Netsky 9
Banload 8
Vers t...
Ban.
Cha...
V...
Vi...
P
Hor m...
E
N...
R...
L...
W
G
Adylkuzz 35
Vobfus 21
Ternanu 12
Redyms 11
FLocker 461
FakeSysdef 460
SMSSend 457
Upatre 447
Conficker A 433
Ranbyus 425
Carberp 418
Cryptowall 412
Ewind 409
BitcoinMiner 391
Marcher 376
AndroFakeInst 373
IRC Bot 362
Emudbot 366
SocStealer 324
Kins 319
Fleercivet 309
ChangeHead 305
Simda 279
Mupad 272
UrlZone 269
Dyre 265
Phorpiex 232
Viknok 232
GinMaster 231
Quantloader 243
Kelihos 226
Ghostpush 174
TinyNuke 174
Poseidón 145
Induc 123
Retefe 118
Zemot 112
Ransomware 237
Cidox 226
Bolek 120
uBot 106
Conficker B 102
Carufax 101
Poweliks 236
Tempedreve 220
Capper 118
Metel 105
Wapo...
0
INFECTIONS
100
500


Flashback
965
BrainTest
945
Renocide
899
Loiza
884
Dynamer
876
Mebroot
825
VKShare
821
Alureon
781
Rovnix
773
Rootnik
752
Mirai
748
Pykspa
722
Qakbot
718
Nemucod
715
Andromeda
710
FlyStudio
705
MilkyDoor
662
Clikug
661
Dorkbot
647
IrOpsSpy
703
AndroidLocker
630
Citadel
552
Malicious
JavaScript
523
FastDiscountz
697
Matsnu
574
Dipverdle
519
Zloader
501
Conficker
20026
Gamarue
14399
Uupay
9758
Powmet
7774
SpeesiPro
6501
Sality
5800
Ramnit
5518
Gozi
5242
Zeus
4318
Necurs
4241
AndroidBauts
3951
Zusy
2522
Rerdom
2371
Ghokswa
2322
Gamut
2289
HummingBa
d
1587
Skeeyah
1567
Conficker.C
1558
Ztorg
2222
Mkero
1533
Cutwail
1431
Vawtrak
1429
Cryoloa
der
1388
PrizeRAT
3194
Bifrose
1878
ZeroAcces
s
1493
Chir
1270
BHProxi
es
1159
Bedep
1128
PushDo
3178
Nymaim
1604
Bondat
1461
Blakamb
a
1258
Kjworm
1016
Dofoil
1012
1,000
INFECTIONS
20,000

FINAL SUMMARY

- Over the second semester 2018, a total of 125 vulnerabilities for iOS were made public, **56% of them with a 7/10 severity or higher.** Consequently, iOS gathers 1496 vulnerabilities from 2007.
- Over the second semester 2018, a total of 173 vulnerabilities for Android were made public, **18% of them with a 7/10 severity or higher.** Consequently, iOS gathers 1950 vulnerabilities from 2009.
- Around **a third of the malicious applications detected were available on Google Play between 22 and 42 days.** The total average (time malicious applications were published) is 47.45 days.
- **11% of iPhones execute an iOS earlier than 11.** In case of Android, half of the current devices working with Android execute an unsupported version.
- 3,528 vulnerabilities have been analyzed over the second semester 2018. **65% of them have a severity score of 7 or higher.** Oracle, Adobe and Microsoft are the manufacturers with the highest number of CVEs assigned.
- Most of the security problems detected from our clients are **information leakages through sensitive files and metadata, as well as the poor implementation of HTTP headers** aimed to protect from attacks.
- Spear-phishing and malicious office documents (mainly through macros) **are the most common infection methods used** among the most sophisticated groups of attackers.
- A European company **needs an average of almost 3 days to solve a malware threat. The fastest are insurance companies** (they need less than 2 days), **while the slowest are food production companies** (more than 4 days).
- In Spain, **entertainment industry needs up to 10 days to neutralize a malware threat.**
- **Gamarue and Conficker remain the most popular malware threats** in Europe.

About ElevenPaths

At ElevenPaths, the Telefónica's Cybersecurity Unit, we believe in the idea of challenging the current state of security, since security constitutes a feature that must be always present in technology. We are continuously redefining the relationship between security and people, with the aim of developing innovative products capable of renovating the concept of security. Thanks to this, we stay a step ahead of attackers, that are increasingly present in our digital life.

More information

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com

Information contained herein is owned by Telefónica Digital España, S.L.U. ("TDE") and/or by any other entity within Grupo Telefónica or their licensors. TDE and/or any other entity within Grupo Telefónica, or TDE's licensors, reserve all industrial and intellectual property rights (including any patent or copyright) derived from or applied to this document, including its design, production, reproduction, use and sale rights, unless such rights have been expressly granted to third parties in written form. Information contained herein can be modified at any time without prior notice.

Information contained herein may not be totally or partially copied, distributed, adapted nor reproduced by any means without prior and written consent of TDE.

This document is only intended to assist the reader in the use of the product or service herein described. The reader is committed and required to use information herein contained for their own use and not for any other purpose.

TDE shall not be liable for any loss or damage derived from the use of the information herein contained, for any error or omission in such information, or for the unappropriated use of the service or product. The use of the product or service herein described shall be regulated in accordance with the terms and conditions accepted by the user.

TDE and its trademarks (or any other trademarks owned by Grupo Telefónica) are all registered trademarks. TDE and its subsidiaries reserve all rights over these trademarks.