Eleven Paths

CyberSecurity Report 2019 H1

From mobile security to cyber risk, from the most relevant news to the most technical ones and the most common vulnerabilities, this report covers the risks of the current outlook

Telefónica CYBER SECURITY UNIT

elevenpaths.com

CONTENTS

2019 © Telefónica Digital España, S.L.U. All rights reserved.

This report aims to summarize latest information on cybersecurity (ranging from mobile security 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.

Over the first half of 2019, the key actors have been again privacy and potentially "wormable" flaws, reminiscent of the infamous WannaCry. In January, the greatest number of passwords with their corresponding mail accounts were leaked in the largest breach in history. This caused quite a stir, since it caught users' attention on how it was possible to gather such a significant amount of private data in one go as well as on how they got there. Passwords remain the most common protection formula, but their importance was brought into focus due to this type of events. Services such as *haveibeenpwned* started to be widely used, to the extent that over this six-month period they announced that it is available on the market, since the project is overwhelmed. Even so, Windows 10 has taken a step forward encouraging people to not change system passwords so often.

At the end of this six-month period, BlueKeep has reawakened the ghosts of WannaCry. The issue addressed by Microsoft on the Remote Desktop Protocol still had a great part of the community on tenterhooks. The issue may be "wormable" and cause a chaos similar to WannaCry due to the number of compromised systems. Fortunately, the exploit was not developed immediately; even though it was known that it may be developed, and that it was not available to the public. No malware to be spread through this formula has been freed so far.

Moreover, the security researcher known as PolarBear has kept Microsoft in check due to the release of several security issues that would enable privilege escalation. This opened again the discussion on responsible dissemination of security issues among the community. The community precisely thanked the NSA for having freed GHIDRA, the open and free program that allows binary analyses and reversing. This program is a direct competitor of IDA, so shaking a market that had been stagnated for years. We do not know if Tavis Ormandy used this analyzer to uncover in May perhaps the first formula to execute shell from a Notepad vulnerability.

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.**

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.

2019 © Telefónica Digital España, S.L.U. All rights reserved.

RELEVANT INCIDENTS OCCURRED IN THE FIRST HALF OF 2019

In the following lines we will highlight those news that have had the highest impact over this first half of 2019.

January

Microsoft's Newsletters
Microsoft publishes a new series of security newsletters, where it highlights a dangerous vulnerability that could make it possible to run arbitrary code on the DHCP server.
Read more

Phishing with Modlishka
Modlishka –a kit intended to perform phishing attacks– is released. It is easy to use, powerful, and enables to bypass 2FA. Contrary to other similar tools, Modlishka is not based on templates simulating the original website, but it interacts with the target domain through a reverse proxy.
Read more

Malicious Chinese Application
Secure-D uncovers a malicious application from China, pre-installed on Alcatel smartphone models Pixi 4 and A3. Among other operations, it extracts sensitive data and subscribes the user to paying premium services via SMS.
Read more

February

DNS Flag Day
We start February with the so-called "flag day", a day highlighted in the industry datebook in order for EDNS to be adopted by all servers. EDNS is a mechanism to extend the DNS protocol and improve its security. In theory, after February 1st those DNS servers that don't respond to EDNS messages will be ignored.
Read more

Botnet TheMoon
Interesting concept of botnet profitability. "TheMoon" –a botnet identified in 2014 and specialized in denial-of-service attacks– adds a new "service": proxy renting. This allows attackers to rent botnet resources, a broad range of possibilities: from activity anonymization to fraudulent YouTube videos views to artificially increase visits.
Read more

Hashcat Password Cracking
Improvements in computational capacities and a new update of the well-known password cracker, Hashcat, allow to reduce the time required to obtain an eight-character password from a NTLM hash up to 2.5h. For example, for just $25 in a computational cloud service, a NTLM password hash may be obtained without prior calculations.
Read more

March

Magecart Saga
Compelling analysis by RiskIQ on Magecart saga, that keeps giving us news. Groups that are behind the tool have developed it to the extent that they have achieved a reduction in the number of necessary lines, user-agent discrimination and use of metadata embedded in images with the aim of getting URLs from data collection servers.
Read more

NSA's Ghidra
The US National Security Agency (NSA) releases a reverse-engineering tool: Ghidra. An immediate and direct competitor of IDA Pro. Curiously, shortly after being freed, it has been reported that Ghidra opens up port 18001 in all the interfaces, an inherent feature of JDWP in debug mode. This exposed users to arbitrary code execution attacks.
Read more

FIN7 Activity
Despite the arrests that took place in summer 2018, there are signs that the FIN7 cyber-crime gang, commonly known as Carbanak, is still active. Evidences have shown a new malware contained in e-mail attachments, called SQLRat. This would use SQL queries to rebuild binary without leaving any trace on the system. Moreover, a second malware has been discovered, DNSbot, that disguises itself to operate over DNS traffic.
Read more

April

Vulnerability on Apache
Appealing and dangerous vulnerability affecting Apache HTTPd web server. This flaw (CVE-2019-0211) would allow a user to elevate privileges on UNIX systems through a CGI. This vulnerability is particularly significant in shared hosting environments. In this scenario, a malicious user that could create a CGI may gain control of the server, and consequently of all those sites hosted by such server.
Read more

Windows build 1903
Due to the release of Windows build 1903, Microsoft modifies its security policy in a bold and interesting manner: 256-bit Bitlocker is no longer required, so now the minimum is 128. It allows users to lock applications using speech while the system is locked. Now, all binaries must be signed by Microsoft to be loaded by 'svchost.exe'. Finally, the most re-markable modification: password expiration is no longer recommended, since Microsoft describes this measure as obsolete and insignificant.
Read more

Problems in WPA3
WPA3, the new Wi-Fi security standard, starts to show its security flaws. Two researchers have published a full research where they provide details on several attacks against WPA3 that may cause from Wi-Fi access point denial of service to downgrade against WPA2 or side-channel attacks. As a whole, the attacks are named Dragonfly.
Read more

May

Exploits by SandboxEscaper
The researcher known as SandboxEscaper publishes a series of 0-day exploits to elevate privileges in Windows systems. It's not the first time she brings out this type of publications. Exploit codes were made public in a Github repository [but they have been deleted].
Read more

Microsoft's Patches
Microsoft releases its usual batch of security patches, including CVE-2019-0708, a vulnerability in Terminal Server that enables remote arbitrary code execution. It has a CVSS score of 9,8; so there are concerns that it may be used as a exploit for a worm. There is such a great concern that patches for unsupported versions of Windows have been included as well..
Read more

June

Cryptomining with Nansh0u
Cryptocurrency mining malware, in spite of their decrease due to cryptocurrency low profitability, keep giving headlines. Guardicore publishes a detailed report on Nansh0u, a malware that has infected 50,000 servers to mine the cryptocurrency named TurtleCoin.
Read more

Flaw on EXIM Mail Server
A serious flaw uncovered in EXIM mail server. This vulnerability would enable arbitrary code execution. In addition to this, the patch was not categorized as "security". This made that many distributions did not published it with priority, so leading critical mail systems in production to remain exposed even though there was an official solution.
Read more

Fallos en pila TCP de Linux
Netflix engineers have identified vulnerabilities on the implementation of the Linux kernel TCP sack that may cause denial of service with an especially mishandled TCP packet. In particular, it is related to how Linux kernel handles SACK packets (an improvement that enables granular retransmission of lost TCP packets that, in turn, allows to save traffic).
Read more

2019 © Telefónica Digital España, S.L.U. All rights reserved.

SMARTPHONES

Apple iOS

Remarkable news

iOS starts 2019 with a fairly complete security update. On 22 January 2019 the version **12.1.3** of Apple mobile operating system is released. Among the security flaws addressed, several corresponded to Kernel, and they would enable privilege elevation or arbitrary code execution. Another significative flaw is patched to **FaceTime (the Apple app to make video calls). This flaw would allow an attacker to initiate a FaceTime call causing arbitrary code execution[1].**

Not long after version **12.1.3**, Apple releases the next version **12.1.4**, on 7 February 2019. This time with the aim of addressing four relevant security flaws affecting FaceTime (again), IOKit, Foundation and Live Photos. Perhaps, the flaw having the highest media resonance was the one affecting FaceTime. It allowed the initiator of a Group FaceTime to force any recipient to answer. As it may be seen, they are not always flaws enabling arbitrary code execution whose exploitation requires highly specialized expertise. On this occasion users' privacy could be endangered simply with an easy-to-exploit technique[2].

On 25 March, iOS changes to **12.2.** As it is a minor version release (from **12.1** to **12.2**), it includes improvements in user experience. Nevertheless, the most striking fact is the great amount of security issues addressed in this version: up to 51 patches that affected a broad range of iOS subsystems[3].

Interestingly, there are not patch versions between versions **12.2** and **12.3**. On 13 May, the latter comes into existence, addressing a high number of flaws, as the previous one did. A significant number of flaws focused on Safari's browser engine, WebKit, can be highlighted. As security-unrelated functionality, Apple updates the image of the AppleTV icon in this version[4].

A little more than a week after version **12.3**, the **12.3.1** one is released. This patch-level version addresses functional flaws and no CVE or associated security error is assigned. However, one of the issues addressed by this version is that spam messages are no longer notified by iMessages[5].

Finally, on June 10, a new version is born: the **12.3.2** one. It only provides a patch to address an issue raised when taking photos with the model iPhone 8 Plus.

Concerning version **13**, it is presented at the annual event for WWDC developers, where Apple announces that it is expected to be freed over the third quarter of this year. In the next report we will see the security updates introduced by Apple in this new iteration of its mobile operating system. That said, we can anticipate that the single sign-on system ("Sign in with Apple"). It will allow users to authenticate through their Apple ID, in a similar way as it is already done with Google or Facebook accounts, **but focusing on user's privacy (for instance, it allows to quickly create disposable mail accounts).**

[1] https://support.apple.com/kb/HT209443

[2] https://support.apple.com/kb/HT209520

[3] https://support.apple.com/en-us/HT209599

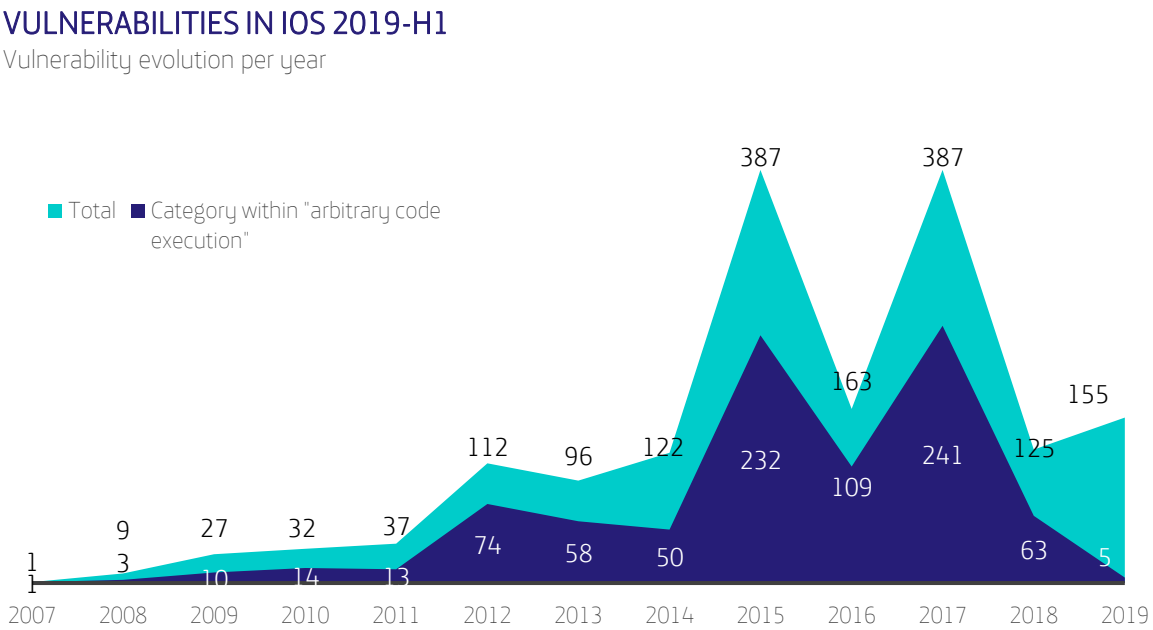
[4] https://support.apple.com/es-es/HT210118

[5] https://support.apple.com/en-gb/HT201222

2019 © Telefónica Digital España, S.L.U. All rights reserved.

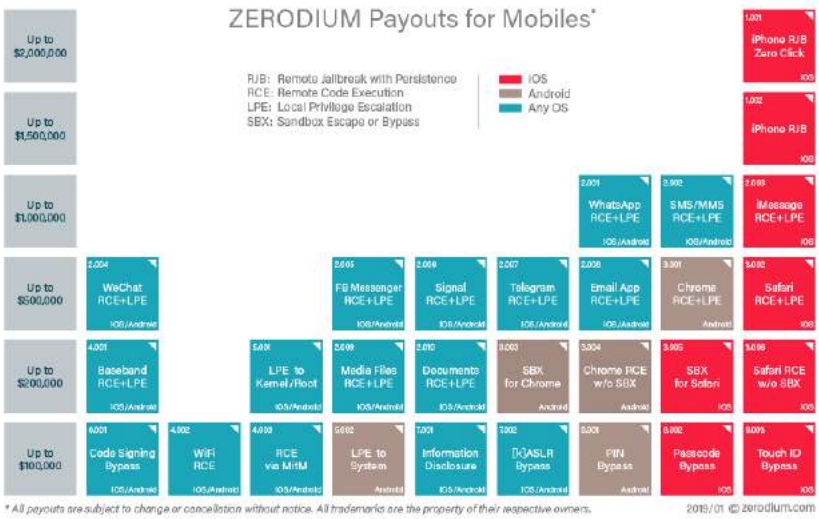
Vulnerability evolution in iOS over the first half of 2019

Interestingly, in 2015 and 2017 the number of vulnerabilities was the same: 387.



Apple smartphone has been, and remains, a precious object for researchers, both for the good reputation acquired after finding an issue on these systems as well as for the reward they may get on the black market from those with greater severity.

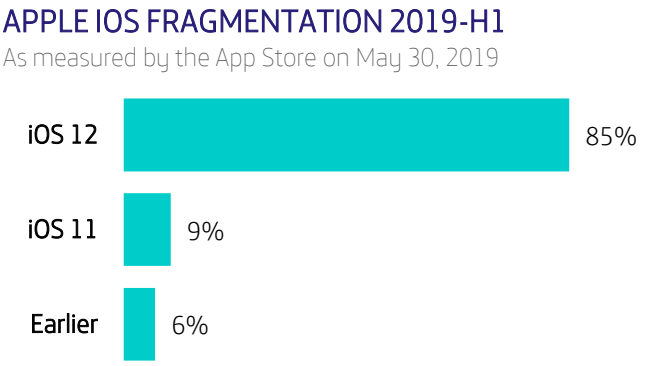
Issue detection is still a growing market. Over the first half of 2019 alone more issues have been detected than during the whole 2018. Despite this, only a few are categorized as arbitrary code execution. Consequently, **according to Zerodium over this first half of 2019 the market price of this type of vulnerability has increased up to 2 million.**



2019 © Telefónica Digital España, S.L.U. All rights reserved.

iOS Fragmentation

iOS fragmentation presents the following distribution, as measured by the App Store on May 30, 2019:



Fragmentation does not constitute a problem for Apple mobile device. Even though mobile developers have to deal with different types of screens (given the range of devices following the same line) and pixel densities, they cannot be compared to the diverse scenario of API levels corresponding to the various Android versions, which would make development on this platform more difficult.

Removing requests of applications from Apple store

Apple publishes a transparency report about which governments requested them to remove apps from their market. Furthermore, they disclose as well how many times these governments requested them user or device data or actions on accounts. The period analyzed covers the second half of 2018.

- **Apple has removed 634 apps from the market of 770 apps specified in the requests.** 517 of the removed apps were requested by China (since they were related to illegal gambling and pornography) and 0 by the U.S., in addition to other 10 countries. Norway, Saudi Arabia and China were the countries that the highest number of takedown requests submitted.
- However, **the U.S. did submit 4,680 device access requests, more than any other country**; although it includes stolen devices and emergency situations.
- Regarding account access, **4,875 requests to access a total of 22,503 accounts were submitted (most of them by the U.S. as well)**. In 82% of the cases data on the accounts were provided, but in the remaining cases only information non directly related to the data was provided.
- Account preservation for 90 days may also be requested. Of 1,823 requests on 5,553 accounts, the data of 3,963 accounts was preserved (for example, for future legal purposes). Only 2 accounts were deleted worldwide at the request of governments.

All the information about this report of Apple may be found graphically summarized in the following blog entry:

https://business.blogthinkbig.com/a-government-is-known-by-the-apple-data-it-requests/

2019 © Telefónica Digital España, S.L.U. Todos los derechos reservados.

Android

Remarkable news

With Android Q still in the oven pending its publication scheduled in principle by August this year; Android Pie (or Android 8) remains the reference version of the mobile operating system developed by Google.

Still at a beta stage, Android Q will bring along improvements in user privacy, in terms of how users share personal information through their installed applications. Data use transparency of such applications will be improved as well. An aspect related to data sharing between apps that will be also enhanced is the access to information stored on external devices (SD cards mainly). In particular, application access requirements will be more granulated and filtered.

One more interesting aspect that Q is expected to include is to **prevent applications executed in the background from getting the focus.** That is, when users are running an application, they will not view anymore how a background application changes to foreground if they did not request it. **This will limit the advertisement abuse problem caused by some applications**

Regarding users' identity in public or potentially hostile network environments, it is limited to static property spreading. These would be those elements on the system that would allow a straight identification of the user, such as: IMEI, MAC address of network interfaces, etc. For instance, **in order to prevent the user from being tracked through the MAC address of its terminal, random MAC addresses will be used when the device is connected to Wi-Fi networks that are not considered secure.**

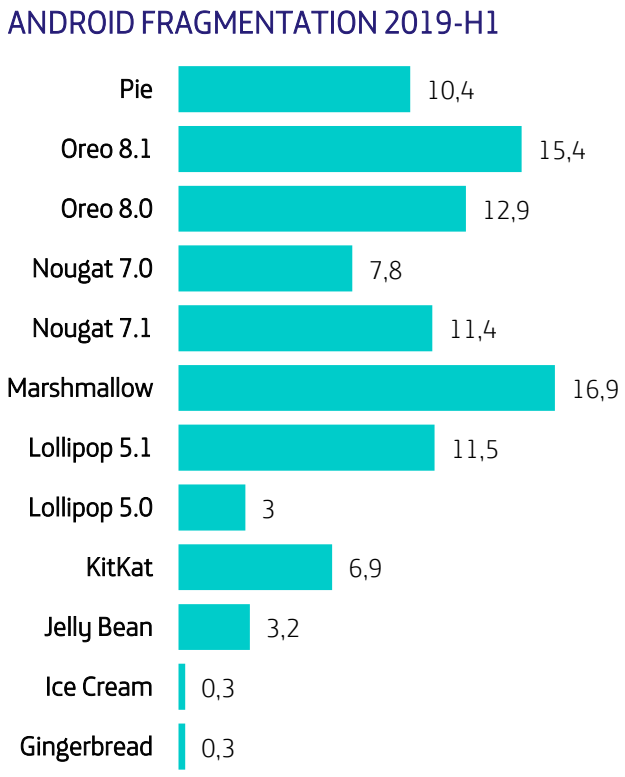
Finally, biometric support is improved, adapting it to facial recognition. Version 1.3 is supported regarding TLS cipher specification. This will be enabled by default when setting secure connections. In the next report we will see in full detail the security improvements that the new Android version will bring along.

Android Fragmentation

Android fragmentation situation is not likely to change in the short term. As we already mentioned in our previous report, this fragmentation is the greatest complaint of developers, since they must carefully measure the API level used by their applications, in addition to provide backwards compatibility if they do not want to lose a significant percentage of incomes.

In contrast to its major competitor –a homogeneous iOS with great coverage of its main version– **Android ecosystem must cope with multiple API levels as well as with a significant number of systems considered obsolete but still perfectly working.** This makes an important number of devices within installation pools to be unsupported in terms of security, which results in a too lengthy exposure.

The fragmentation state of the mobile operating system developed by Google, Android, is as follows[6]:



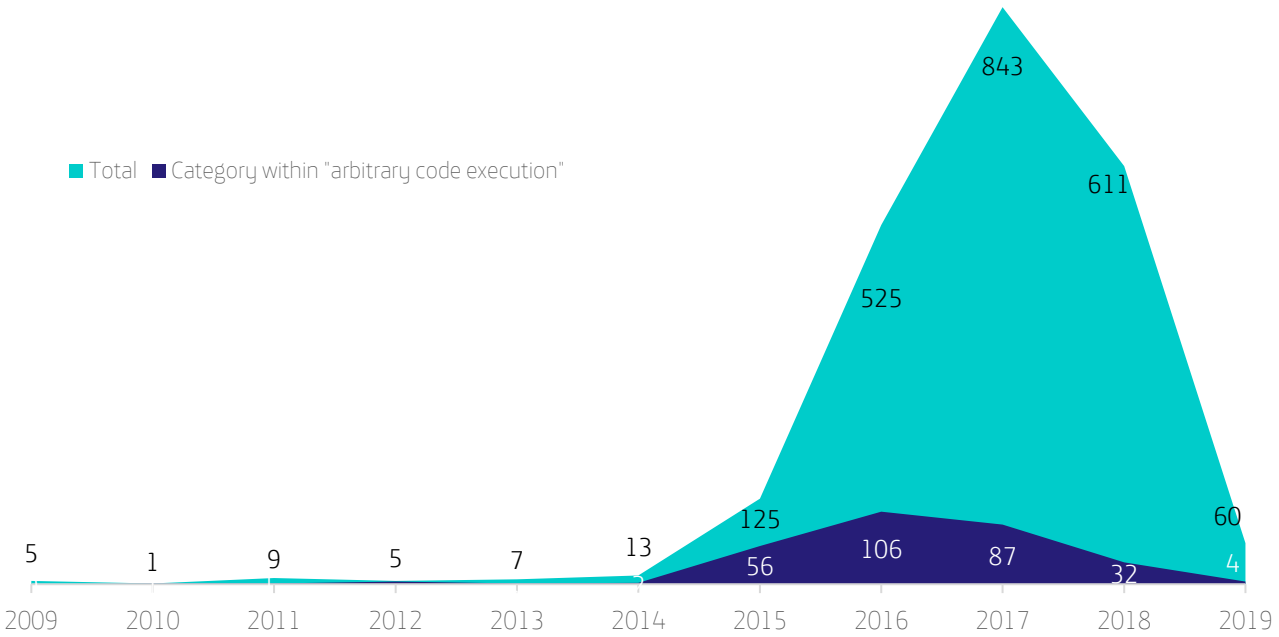
[6] https://developer.android.com/about/dashboards/

2019 © Telefónica Digital España, S.L.U. All rights reserved.

Vulnerability evolution in Android over the first half of 2019

Even if there are still six months left to end the annual chapter, the number of uncovered vulnerabilities has been significantly lower in comparison to the immediately preceding periods. In fact, the counting does not exceed the 60 entries so far and only four of them have been categorized as arbitrary code execution

VULNERABILITIES IN ANDROID 2019-H1
Vulnerability evolution per year

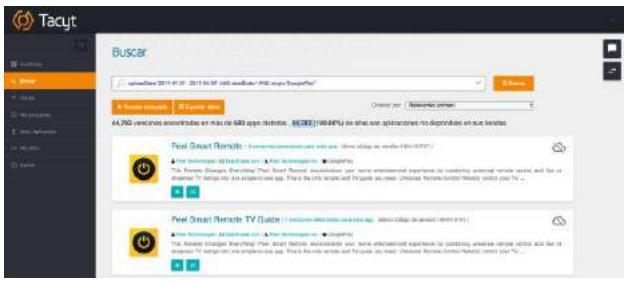


At the end of the year we will see if the trend continues or, on the contrary, there is a palpable reduction in the search for security issues on the mobile operating system developed by Google.

Average removing time of malicious applications from Google Play

We have examined again the average time that Google Play spends to remove malicious applications. **The first point that catches our attention is the great amount of application that have been removed from the app store (almost three times more) compared to the previous period.** This may suggest either that a deeper "cleaning" over the app store is being performed, or that it is still relatively easy to slip through low-quality applications on this app store.

We have analyzed the time that Google Play (the official app store of Android applications) spends 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.



For our purpose, we have taken into account not only the fact that the app has been removed (since this is a quite common operation that does not involve that the

2019 © Telefónica Digital España, S.L.U. All rights reserved.

app is malicious): **the app must also have been detected as malware by at least one antivirus engine.**

Our analysis covers the period from **January 1st, 2019 to June 30th, 2019.** The selected group of applications includes **44,782** applications removed at any moment within the period considered.

We have analyzed a representative subgroup of more than **5,000** applications, and we have got **115** malicious applications. **Therefore, we can conclude that roughly 2% of the apps that were removed may be considered malware.** Finally, the comparable data –in terms of the time spent to remove these apps from the app store (measured in days)– yield the results presented on the graph, compared with the previous six-month period.

These figures mean that, on average, **Google Play removes those apps considered as malware in just over 51 days, even if some of them were available to the public up to 138 days.** Moreover, these data do not represent a significant change compared to the second half of 2018.

In next analyses we will determine if indeed there is a trend, or conversely the figures remain stable.

AVERAGE REMOVING TIME FROM MARKET

Measured in days

2019 © Telefónica Digital España, S.L.U. All rights reserved.

VULNERABILITIES

In this section we will discuss some of the most remarkable vulnerabilities over the first half of 2019. That is, those that may be highlighted due to their special relevance or severity.

CVE ID	TARGET	DESCRIPTION	SCORING (CVSS V3.0)
CVE-2019-12735	Vim and NeoVim Text Editors	Vim and NeoVim use a specific type of metadata on plain text files to configure certain properties of the editor. There is a flaw allowing several options of this mechanism (called "modeline") to avoid the sandbox and execute arbitrary system commands. As the description suggests, it is only necessary to add a commented line to a malicious plain text file and wait until a user open the file with this text editor for the content to be executed on the system. https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=930020	9.3
CVE-2019-11683	Kernel Linux	An error over UDP packets process may cause a denial of service on the system via mishandled UDP packets. It only affects Linux kernel 5. https://www.openwall.com/lists/oss-security/2019/05/05/4	10.0
CVE-2019-0708	Microsoft Windows (Terminal Server)	Known as "BlueKeep", this vulnerability would allow an unauthenticated attacker to execute arbitrary code using especially mishandled RDP packets. No evidences of exploit intended to execute arbitrary code have been known so far. However, several versions causing denial of service on unpatched systems have been made public. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708	9.8
CVE-2019-11477	Kernel Linux	Netflix engineers have identified a vulnerability on the implementation of Linux kernel SACK. SACK enables one-by-one selection of those TCP packets that have not been received, so that they may be retransmitted. This function saves traffic, since without SACK if a non-received packet is required, the other party will send the non-received packet as well as the subsequent ones; even if such packets were received by the client. It happens that this flaw has been 10	N/A

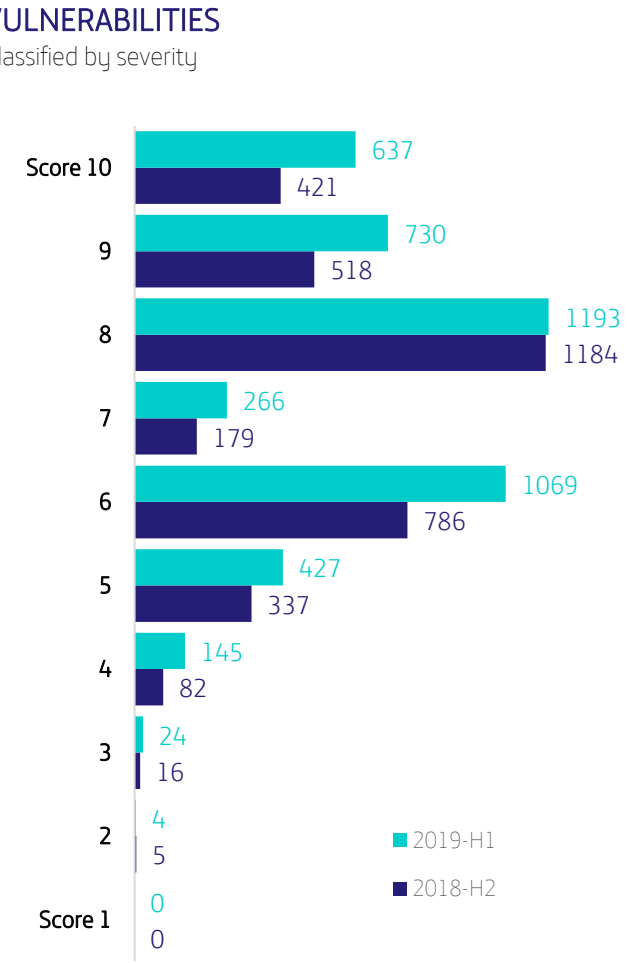
2019 © Telefónica Digital España, S.L.U. All rights reserved.

		years without being discovered, or at least there has been no information on it has been exploited over such a long period. https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md	
CVE-2018-12130 (ZombieLoad)	**Multiple Intel CPUs**	New security vulnerability affecting Intel Core and Xeon CPUs. This issue may allow to access sensitive data from other processes. This type of issues exploits speculative execution of processors –that is, the anticipation in the execution of instructions, that may be discarded or not. A kind of optimization that allows to "advance" CPU work before the execution flow reaches that point. https://zombieloadattack.com/ https://www.cyberus-technology.de/posts/2019-05-14-zombieload.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html	6.5

2019 © Telefónica Digital España, S.L.U. All rights reserved.

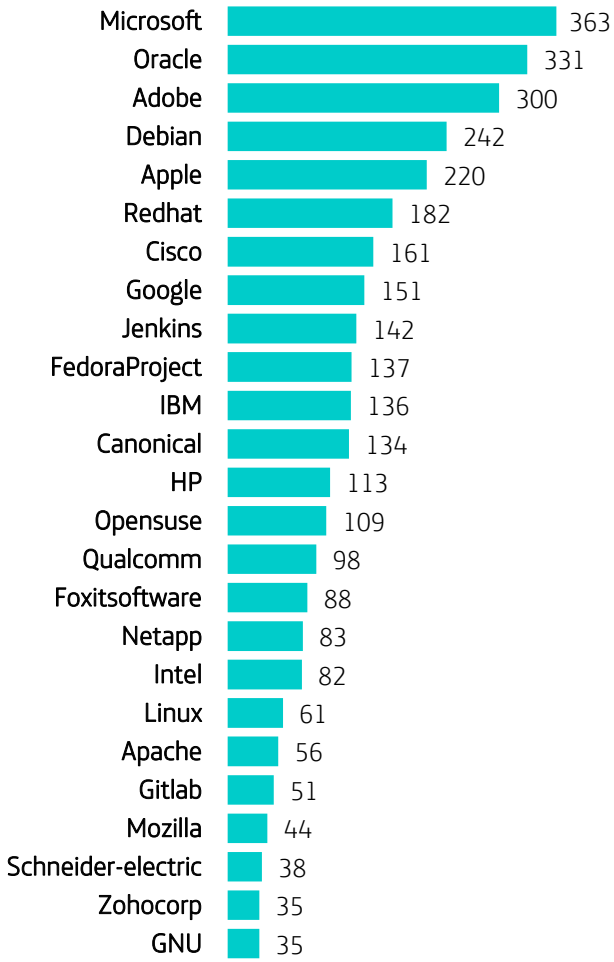
Vulnerabilities in figures

In the following graph 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:



A great number of them are focused on high scores, from 8.0, when the severity is considered as high and the impact triggers major consequences. **The reward programs implemented by technological companies partly encourage researchers to focus on the most critical findings (thereby the highest-rewarded ones) instead of on those that don't opt for the reward or are lower rewarded.**

Top 25 companies with the highest number of CVEs gathered



As on other occasions, data here presented must be relativized. This is due to the fact that some vendors have various products that may be candidates for getting a CVE, such as Oracle and its large product portfolio (high dispersion). Conversely, companies with a lower number of products that may get a CVE do have a high concentration of CVE in some products. Examples of this are Adobe with Flash and Reader, that gather a high number of vulnerabilities.

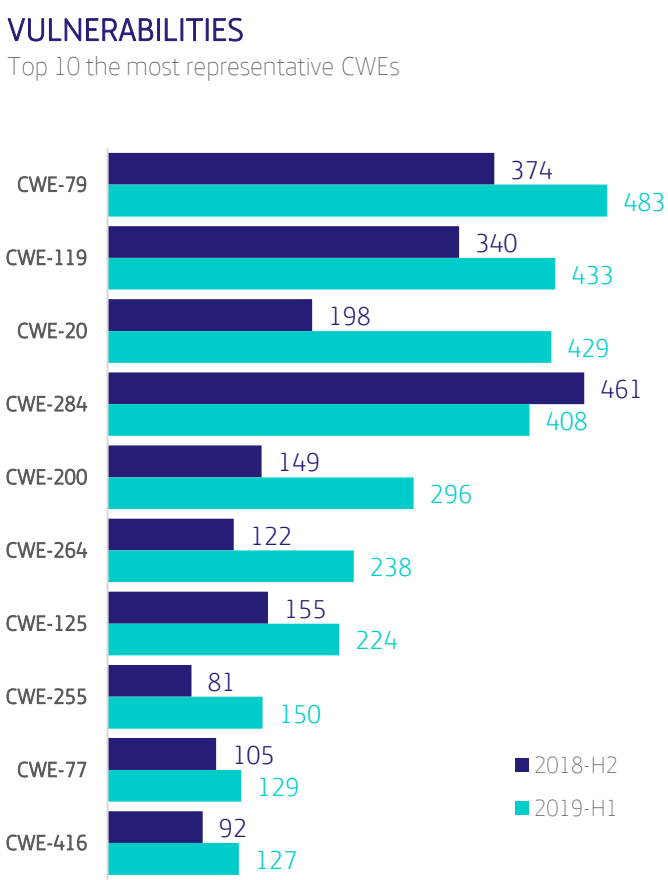
2019 © Telefónica Digital España, S.L.U. All rights reserved.

We must also highlight that there are shared vulnerabilities. That is, Canonical (synonymous with Ubuntu), Debian, FedoraProject, openSUSE and ReadHat share a high number of binaries and libraries, in addition to the same operating system kernel: the Linux kernel. When they share the same vulnerability or CVE, a patch is distributed among all the vendors, who create a packet for their particular distributions.

Top 10 the most representative CWEs

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

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



2019 © Telefónica Digital España, S.L.U. All rights reserved.

Descriptive table of each CWE

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	483
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 reading and writing operations	433
CWE-20	Improper Input Validation	Generic category that includes errors consisting of an inappropriate or non-existent control of user data input	429
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	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	296
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)	238
CWE-125	Out-of-bounds Read	Highly related to CWE-119, it includes read memory operations exceeding the control bounds of an intended buffer	224
CWE-255	Credentials Managenements	It includes all those vulnerabilities affecting how user credentials are managed. For example, their storage, delivery and creation	150

2019 © Telefónica Digital España, S.L.U. All rights reserved.

CWE-77	**Improper Neutralization of Special Elements used in a Command**	It refers to the lack or flaw of chain elements filtration that may enable arbitrary command execution on the system	129
CWE-416	**Use After Free**	Failure of memory management over a process. It allows to call an object or reference a heap from a previously freed memory region	127

Conclusions

Broadly speaking, vulnerabilities are mainly due to the lack or flaw of data inspection coming from users, or process-exogenous. That is, they are values occurring over data input but that are not inspected enough before being processed. This situation causes misuses of a given function or call that finally result in arbitrary code execution.

Another relevant aspect is that memory management is still an unfinished business for developers. Even though new programming languages and their corresponding dynamic execution environments (that automatically manage memory) have been introduced, unmanaged languages are still (and will remain) essential to develop services with an adequate performance.

Finally, **there are still vulnerabilities resulting from carelessness or security unawareness as the main concept in development.** Insecure credential management, privileged accesses to entities that must not have or do not need them, etc.

Many of the vulnerabilities currently present within the lists of CVEs -with figures that don't stop growing year after year- **could be avoided just with the appropriate integration of a secure development cycle and unitary tests that include memory management analyses.**

2019 © Telefónica Digital España, S.L.U. All rights reserved.

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.

We point out that 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.

This is due to the anonymity and deception capacity inherent in this kind of operations. This way, actors may use the means to mishandle information in order to hide their actual origin and purposes. It is even possible that in certain cases some groups adopt other groups' modus operandi, so that they can divert attention and undermine them.

Significant APT operations detected over the first half of 2019

DARKHYDRUS

2019 started with a notable peak of activity of the group DARKHYDRUS, which we already mentioned in our previous report. A technique that did not go unnoticed for analysts and the concerned media was the use of Google Drive API as a command and control channel by the malware RogueRobin; created and used by the group.

This is just a small example of the innovation developed within the group. We must also mention the use of fairly new file formats, that makes it difficult detection based on file format patterns used by analysts on their automated detection systems, as well as the use of cutting-edge techniques to avoid AppLocker.

This actor continues to gain importance, even though its operations area is exclusively in the Middle East. In particular, it targets government agencies and educational institutions in the Middle East. It is certainly a new player that uses the latest resources and even innovates with new techniques.

MuddyWater

This group (presumably Iranian) remains active. In one of their last analyses (April 2019), Check Point researchers found new samples which show the persistent activity of the group in countries such as Belarus, Turkey and Ukraine. This suggests that they are expanding their line of action, mainly based in the Middle East, the United States and Europe.

The group uses again a combination of malicious documents and spear-phishing. These are simple yet

2019 © Telefónica Digital España, S.L.U. All rights reserved.

effective infection techniques to steal internal documents from the target organizations, and later use them as a bait to execute its characteristic PowerShell-based POWERSTATS payload.

As a new feature, for these active operations a customized window in the language of the targets has been included, so the users are more likely to enable the macros, which is an essential step for the POWERSTATS payload to be triggered.

Something to be highlighted regarding the new modus operandi of the group is the inclusion of external documents templates including the infection mechanisms. This allows that, to an extent, the preliminary analysis result of the attachment will not be positive since it does not include malicious payload.

Soon after, by early June, Trend Micro researchers uncover a new campaign of the group. The evolution even over such a short period is evident. In addition to what has been previously discussed, the group uses malware targeted at Android devices and false flag techniques with the aim of hiding their real origin or involving third parties.

On this occasion among the victims there were a Jordanian university and the Turkish government. Both were attacked under spear-phishing schemes. Interestingly, this time accounts under the mail domain of the respective agencies were used, instead of falsified mail accounts. Something that, of course, significantly increased the level of reliability.

Mails always include Office documents with malicious macros which lead a new iteration of their malware POWERSTATS v3 to be downloaded. Curiously, this time they did not use the template injection technique that we mentioned above.

FIN7

It is probably that the name Carbanak will not go unnoticed for many people. Carbanak, Anunak or Carbon Spider is the group behind the attacks specifically targeted at bank employees intended to gain control over financial assets, such as ATMs or POS systems.

Although the group was partially dismantled after the arrests of several of its members by law enforcement bodies (including Spain), a number of its remaining members, as well as other groups with which it shares tools and modus operandi, continue with criminal activities.

This time, **Kaspersky Lab has published a report where it details the last activities of the FIN7 cybercrime rig, one of the groups linked to FIN.** Among these activities, there was the creation of "legal" job offers to hire remote pentesters, developers and interpreters to meet the needs of the criminal group in terms of tools, phishings, etc.

It even happened that several former employees of companies linked to FIN7 included them in their resume, ignoring that they had been working for a criminal organization.

https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

2019 © Telefónica Digital España, S.L.U. All rights reserved.

New actors detected over the first half of 2019

BlindEagle

APT activity of a new group suspected coming from South America has taken place. It is called APT-C-36 or BlindEagle, and their modus operandi consists in impersonating members of the Colombian cybersecurity agency or the office of the attorney general with the aim of stealing confidential information from Colombian targets or foreign companies with branches in Colombia.

This group uses Office documents with malicious macros to install a variant of "Imminent Monitor RAT", a remote management tool. You can read an interesting technical analysis written by the Chinese company Qihoo 360, which uncovered the activities of this group.

Noteworthy techniques and tools used

FINTEAM

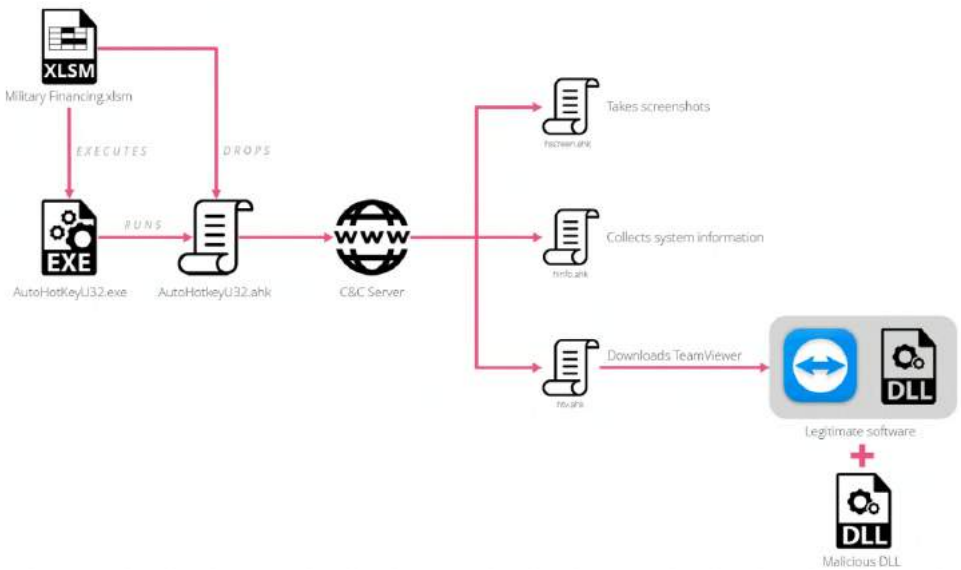
Again, Check Point researchers spot a particular (but not original) method of introducing a remote-control tool upon a legitimate product: Team Viewer.

Over a spear-phishing campaign against several embassies in Europe, an Excel document with malicious macros that downloaded an executable was detected. It was the remote administration and control software Team Viewer.

Nevertheless, the attackers delivered a malicious DLL that modifies software functionalities in order to add more features to Team Viewer that it did not include before, for example: hiding of TeamViewer interface, so that the user would not know it is running (original Team Viewer clearly notifies the user when it transfers control), gathering and filtration of credentials, sending of technical information to the team, and downloading and execution of additional malicious binaries.

Although the use of RAT (Remote Administration Tool) tools is recurrent in the APT field, the reuse of legitimate software as a backdoor, such as Team Viewer, is not. It is, as it were, a low-technology solution that allows attackers to save efforts in the building or purchase of a real RAT.

https://research.checkpoint.com/finteam-trojanized-teamviewer-against-government-targets/



Infection chain (Source: Check Point).

2019 © Telefónica Digital España, S.L.U. All rights reserved.

CYBER RISK RATING BY SECTOR

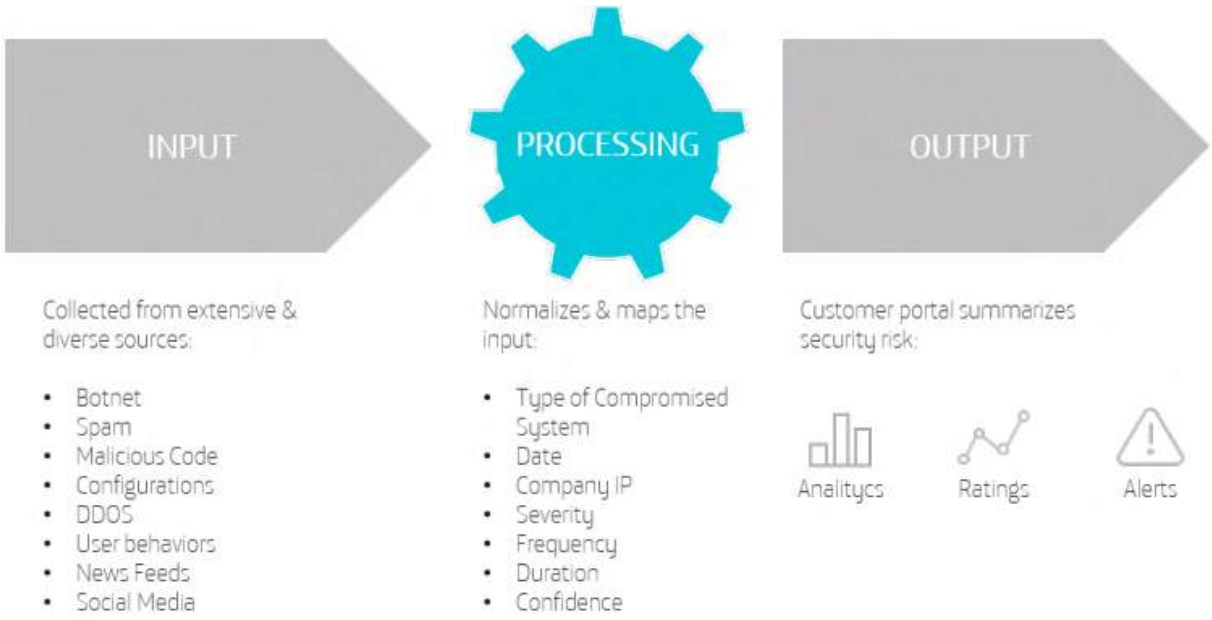
We have used the BitSight Security Ratings Platform to set out a security comparison between industries.

BitSight measures the security performance of a company based on externally-observable data. Instead of evaluating the existence of policies, rules and controls, BitSight rates the effectiveness of any controls and policies based on these non-intrusive external measurements. Evidence of compromised systems, file sharing, diligence and disclosed breaches all are factored into BitSight's algorithm, with each company receiving a daily rating from 250 to 900 indicating the security posture of each company.

Using BitSight's data, 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 examples.

Data on infections detected and neutralized (by economical sector)

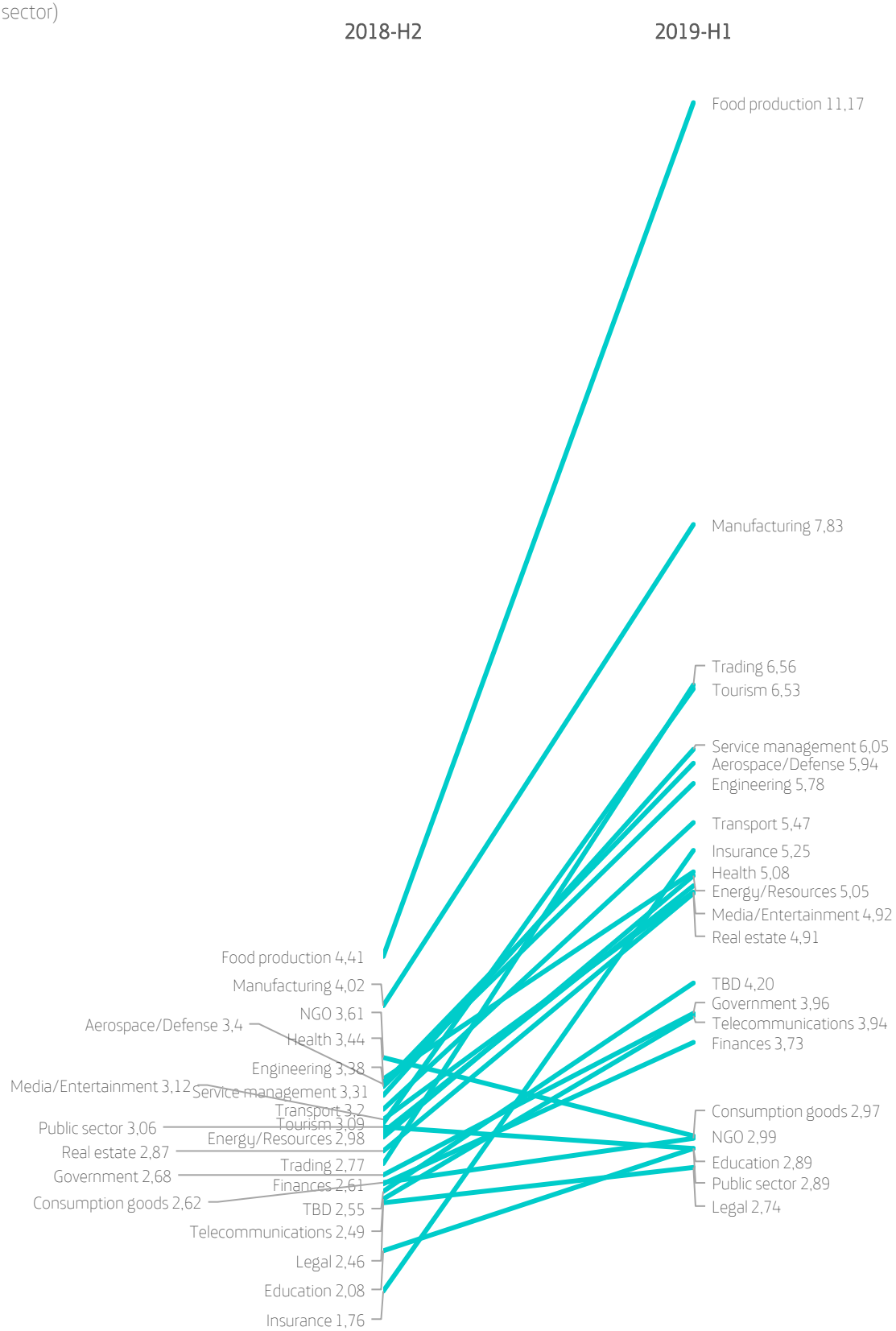
The following figures show the average number of effective days from threat detection to its neutralization by the organization (grouped by affected economical sector).



2019 © Telefónica Digital España, S.L.U. Todos los derechos reservados.

SECURITY PRACTICES

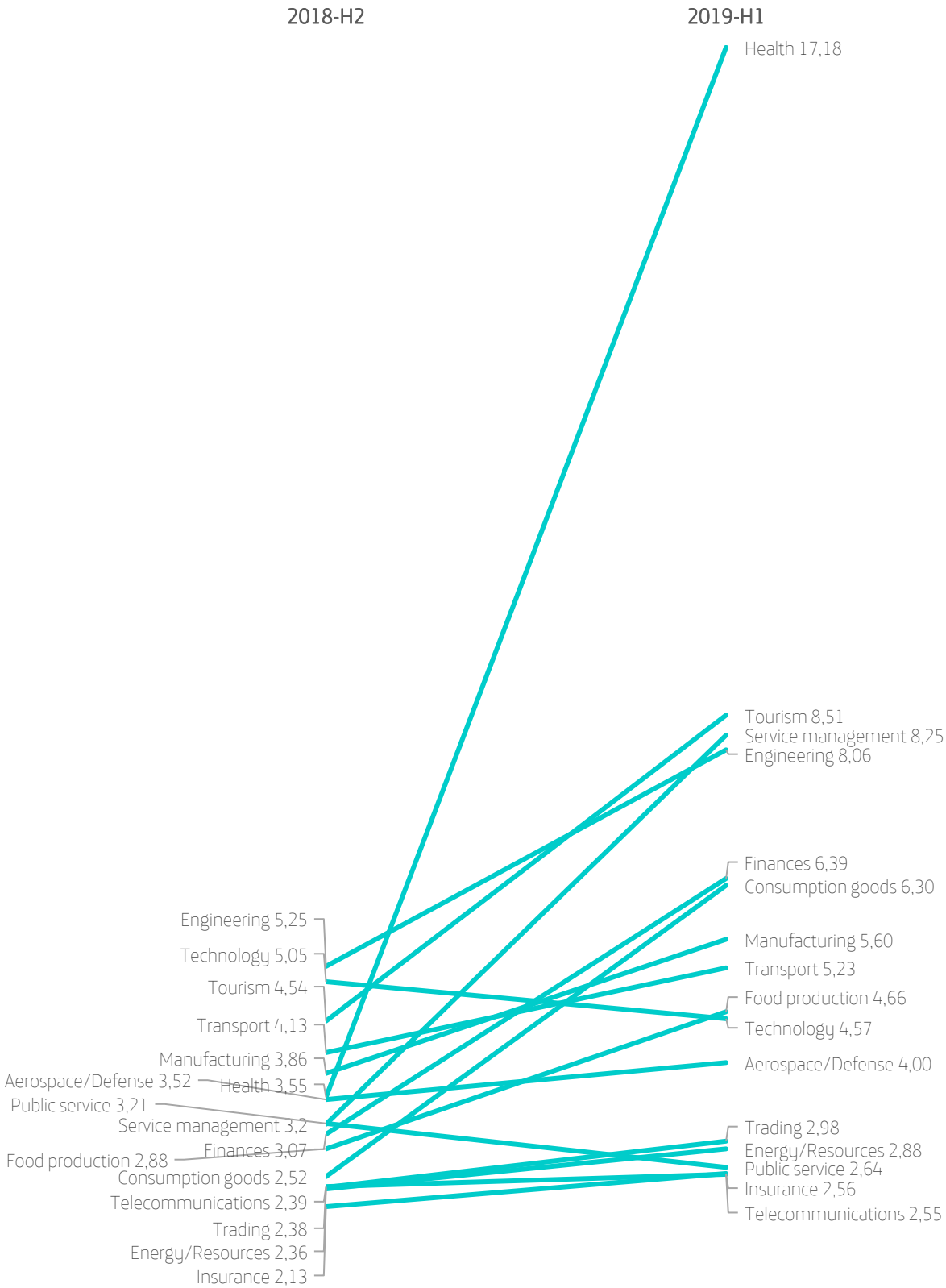
Average number of effective **days** needed by a **European** company to fix a malware threat (grouped by sector)



2019 © Telefónica Digital España, S.L.U. All rights reserved.

SECURITY PRACTICES

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

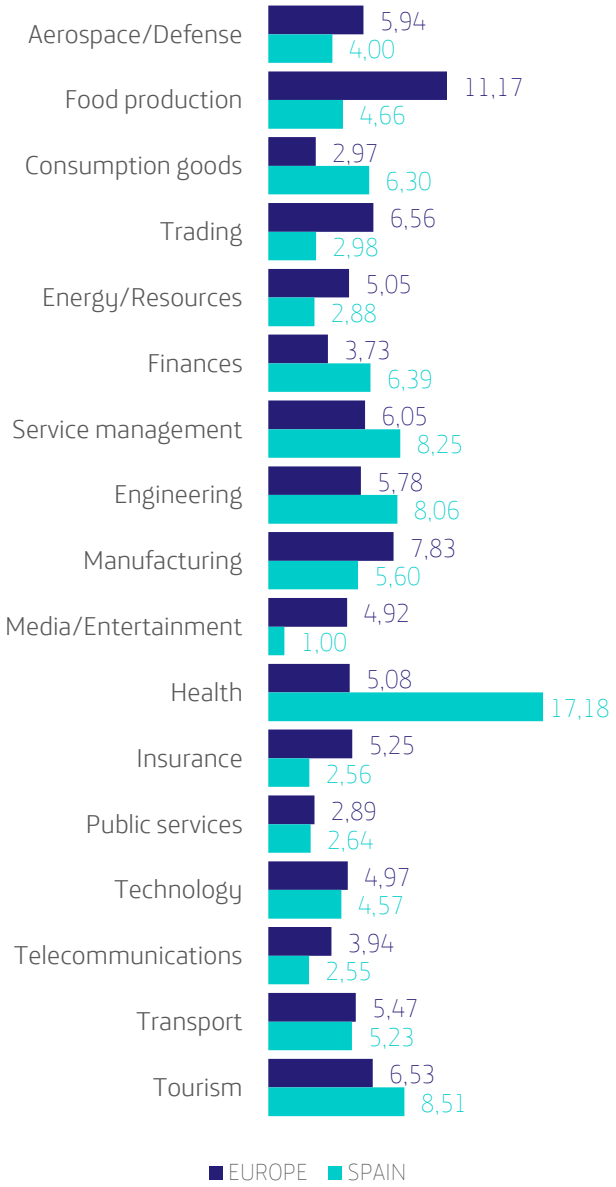


2019 © Telefónica Digital España, S.L.U. All rights reserved.

There has been **a great increase in the health sector**, affected in recent times by ransomware worldwide.

The following graph compares the response time between Spain and Europe over the first half of 2019 (grouped by sector).

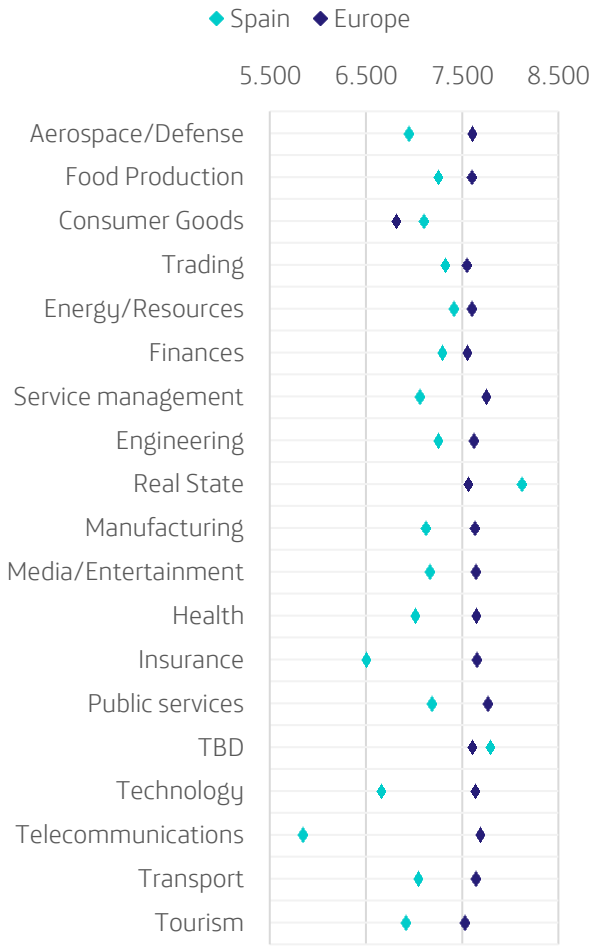
COMPARISON DETECTION-NEUTRALIZATION BETWEEN SPAIN AND EUROPE OVER 2019-H1 (BY SECTOR)



BitSight **measures the security performance of states, industries and companies of critical infrastructure.** The following graph shows the security differences between various sectors in Europe and Spain, according to BitSight's rating.

COMPARISON BETWEEN SPAIN'S AND EUROPE'S RANKING

BitSight Sovereign Security Ratings



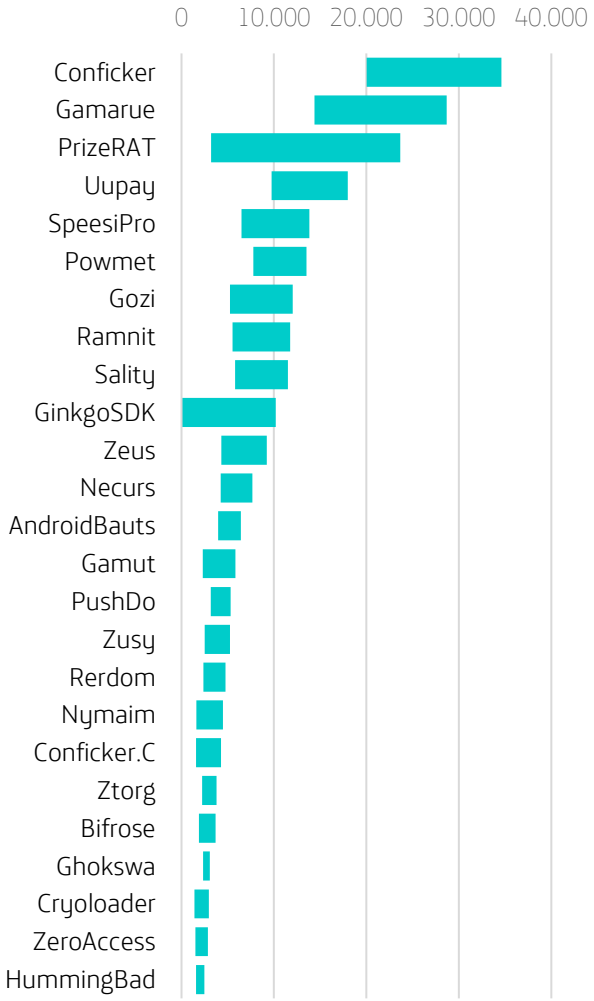
2019 © Telefónica Digital España, S.L.U. Todos los derechos reservados.

The 25 families of malware and infections detected in Europe

The 25 malware families affecting most systems in Europe are detailed below, **as well as their increase compared to the previous scoring.**

INCREASE IN THE 25 MALWARE FAMILIES AFFECTING MOST SYSTEMS IN EUROPE

Growth experienced from 2018-H2 to 2019-H1

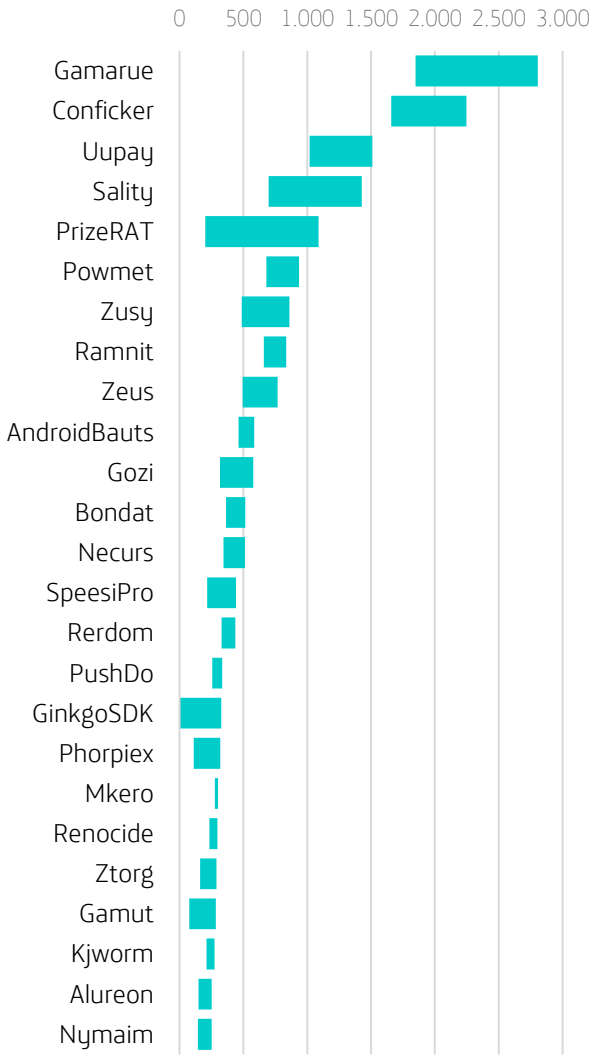


The 25 families of malware and infections detected in Spain

The 25 malware families affecting most systems in Spain are detailed below, **as well as their increase compared to the previous scoring.**

INCREASE IN THE 25 MALWARE FAMILIES AFFECTING MOST SYSTEMS IN SPAIN

Growth experienced from 2018-H2 to 2019-H1



2019 © Telefónica Digital España, S.L.U. Todos los derechos reservados.

FINAL SUMMARY

- Over the first half of 2019, a total of 155 vulnerabilities for iOS were published, **although only 5 of them serious enough** to enable code execution. Consequently, iOS has gathered 1656 vulnerabilities since 2007.
- Over the same period, a total of 60 vulnerabilities for Android were published, **although only 4 of them serious enough to enable code execution.** Consequently, Android has gathered 2014 vulnerabilities since 2009.
- Around **2% of the malicious applications removed from Google Play were detected by antiviruses (in absolute terms, over this six months Google has removed a higher number of applications).** On average, they stayed on the app store 51 days.
- 6% of iPhones execute an iOS earlier than 11. Regarding Android, **less than half of the current devices execute version 8 or later.**
- 4,495 vulnerabilities have been analyzed over the first half of 2019. As the previous six-month period, **62% of them have a severity score of 7 or higher.** Oracle, Adobe and Microsoft remain the vendors with the highest number of CVEs assigned.
- **Spear phishing and malicious office documents (mainly through macros) remain the most common infection methods used** among the most sophisticated groups of attackers.
- **A European company needs an average of almost 5 days to fix a malware threat.** Two more days compared to the previous period. The fastest are the legal sector (they need just over 2 days), while the slowest are again food production companies (but now they need 11 days).
- In Spain, the health sector needs up to 17 days to neutralize a malware threat.
- Gamarue and Conficker remain the most common malware threats in Europe, with higher figures compared to the previous period.

2019 © Telefónica Digital España, S.L.U. All rights reserved.

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.

2019 © Telefónica Digital España, S.L.U. All rights reserved.

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.

2019 © Telefónica Digital España, S.L.U. All rights reserved.