Eleven Paths

CyberSecurity Report 2020 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 COMPANY

elevenpaths.com

CONTENT

This report aims to summarize latest information on cybersecurity (ranging from mobile security to cyber risk, from the most remarkable news to the most technical ones and the most common vulnerabilities), while covering most aspects of the field in order to help the readers understand the risks of the current outlook

The first half of 2020 in the field of cybersecurity has been affected by the same event that has shaken the whole world: the outbreak and effects caused by SARS-CoV-2. It is well-known that the success of video conferencing applications such as ZOOM (and the subsequent discovery of several vulnerabilities) has been largely driven by their massive use as the pandemic spread and travel and meetings were restricted. **The issue has had enough impact to be used as a bait in phishing attacks, targeted or otherwise, to deceive the recipient, hungry for information at difficult times.**

However, it was not all about SARS-CoV-2. In the mobile field, Apple introduced iOS 14, thus leaving behind an operating system that has not been a good version from a security point of view. For its part, **Google announced in January its white paper on Android where it sets out the security improvements and features of Google's mobile platform.**

No matter if you are a cybersecurity professional or enthusiast. It is important that you can follow the rhythm of remarkable news on cybersecurity: **What are the most significant facts currently happening? What is the current outlook?** This report will provide readers 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.

Here we go!

MAJOR INCIDENTS IN THE FIRST HALF OF 2020

In the following lines we will highlight those news that have had a high impact over this first half of 2020.

Bug in Android kernel

CVE-2019-2215 is a bug (use after free) that allows privilege escalation in the Android kernel.

Citrix VPN nightmare

CVE-2019-19781 is a bug in some component of the Citrix (formerly NetScaler) ADC VPN. There are about 80,000 companies at risk. This triggers the number of bots that try to find out if the device is vulnerable and if so, they launch the attack automatically.

MDHex in GE Healthcare devices

MDHex is the name for a number of vulnerabilities in the software of some GE Healthcare devices that are responsible for monitoring the vital signs of patients in hospitals. The fact that the appropriate telemetries are not sent to the staff that monitors the patient while they are not being supervised could make complications go unnoticed and cost patients their life. And even so, software issues in these critical systems are ridiculous.

The UN bans the use of WhatsApp

The United Nations bans the use of WhatsApp among its officers. After several serious security problems during the summer and the scandal of Jeff Bezos (even journalists from the Washington Post) the decision is that it is not a secure communication mechanism, and therefore should not be used for official purposes within that organization.

Shlayer on Mac

According to Kasperksy,Shlayer malware is on one out of ten Macs. But what is the operating system doing to protect itself? Since December it has introduced a total of 14 signatures in XProtect, its rudimentary antivirus. Taking into account that in 10 years it gathers a little more than 100 signatures, it may be concluded that in recent months they have been working hard.

xHelper on Android

xHelper has reached the media as a malware for Android that cannot be uninstalled not even resetting the phone to factory settings.Malwarebytes technicians are still unclear on how exactly this malware works.

Safari certificates

Safari says it will consider certificates of more than one year as invalid from September 2020.

SurfingAttack against assistants

SurfingAttack is a striking new attack against mobile assistants, although perhaps impractical in real scenarios. It is based on sending instructions to Google or Siri through ultrasonic waves inaudible to humans but not to the device's microphone.

Let's Encrypt certificates

Let's Encrypt, recently celebrating its one-billion certificate must revoke more than 3 million certificates (2.6% of the assets) due to a major issue on his Boulder platform, responsible for verifying that the person requesting the certificate is the real owner.

Web vulnerabilities

RiskSense analyzes 1622 vulnerabilities found in web systems in the last decade. The most significant conclusion is not the absolute number, but which ones have been exploited to a greater extent by attackers. WordPress, Apache Struts and Drupal are the winners.

LightSpy targets iPhone

TrendMicro discovers an interesting attack on iPhone users exploiting vulnerabilities on their browser and kernel to install a remote system of surveillance and information theft that has been named lightSpy.

Zoom hell

Zoom, the trendy application. From being able to live a sweet moment in terms of popularity and expansion, to a security nightmare in terms of bugs. Managers even apologize and try to fix them.

New RAT in Python

A new RAT in Python uses the COVID-19 (phishing) to attack the public and private sectors in Azerbaijan. The attack vector is the distribution of a Word document with macros. The RAT seems to be prepared to deploy a large number of tools, in order to automatically exfiltrate information, passwords, webcam images and so on. As a remarkable target, the attackers show interest in the energy sector, particularly in SCADA systems related to wind turbines.

Scams on Apple Store

Sophos detects 30 applications aimed at subscribing to paid services with strange arts and dubious utility. They are advertised as free but actually there is a trial period. To try it, users are asked to enter their card details.

Vulnerability in iOS

Serious vulnerability in iOS, existing in all versions since the 6th (September 2012). It allows code execution just by sending an email. And what is worse: it is being exploited by attackers. iOS version 13 is a security disaster.

Ransomware: Ragnar Locker

To make a ransomware of just 50 kilobytes go unnoticed, the attackers run (and download) a Windows XP in a VirtualBox (also downloaded). Well, that's what the developers of Ragnar Locker, specialists in ransomware against large organizations, have achieved.

Bug in Sign in with Apple

An easy-to-exploit bug has been discovered on the Sign in with Apple system. Its discoverer has received $100,000. It basically allowed an attacker to very easily compromise any service protected by Sign in with Apple.

Compromising DigiCert

Attackers had access to the Digicert Certificate Transparency log signature key. It can be considered the first known case of compromise of a structure of this type. This is achieved as a result of a bug in the SaltStack framework.

Vulnerability in Sensormatic Electronics

Johnson Controls notifies CISA of critical vulnerability affecting several products of Sensormatic Electronics, LLC, a subsidiary of Johnson Controls. The vulnerability causes the credentials of the user performing the update to be stored in clear during the update process. One of the affected products is a video surveillance and alert suite: fire, access, etc.

Tycoon Ransomware

Tycoon ransomware uses the JIMAGE file format. Unknown and little used by developers, it serves to store classes and resources from multiple modules of a JRE. It could be understood as a much less popular .JAR. In addition, it can be run on both Windows and Linux.

Serious flaw in GnuTLS

A serious flaw is discovered in GnuTLS. Two rounds are used in the TLS handshake, but the session tickets allow you to save one. Failure to implement a key rotation (STEK) in GnuTLS made it possible to bypass ticket generation and retrieve private TLS conversations in versions prior to 1.2 as well as bypass authentication in TLS versions 1.3 (intercept them).

106 malicious extensions on Chrome Store

106 malicious extensions are discovered in Chrome Store. Their main feature is that all of them involved a coordinated effort by a domain registration company (GalComm), a claim that the company denies.

Ekans Ransomware, again

Ekans ransomware (AKA "Snake") hits again: Honda forced to shut down several manufacturing plants worldwide. Meanwhile, Enel sees several of its plants affected.

Ripple20 impacts on Treck IP

Ripple20: 19 0-day vulnerabilities are detected in the implementation of Treck IP protocols. Millions of devices would be affected, including IoT devices from vendors such as Intel, Carterpillar, Schnneider Electric, etc.

January
February
March
April
May
June

SMARTPHONES

Apple iOS

Remarkable news

In the last report iOS 13 was in its version 13.3, with an update in December that fixed 15 diverse vulnerabilities. By January 2020, the year began for iOS with a small revision, 13.3.1, fixing over 30 CVEs (in addition to other performance bugs and usability improvements).

On March 24 Apple released version 13.4, the first release within the lockdown period due to the COVID-19 pandemic. **The number of fixed vulnerabilities rose again to thirty.** In addition to the patches included in this release, as usual, numerous fixes were included as well as new functionalities.

On April 7, version 13.4.1 was released. This did not include any security patches, only bug fixes related to FaceTime and Settings application.

On May 20, 2020, iOS version 13.5 was released, including content that was being discussed because of the always difficult balance between privacy and security: **Apple added a notification system so that official tracing applications could notify users of potential contact with victims of COVID-19 disease.** In addition, this release fixes up to 43 new security patches, many of them kernel bugs that would make it possible to execute malicious code with the highest system privileges.

As a curiosity, we can see the reference to the application programming interface regarding COVID-19 exposure notifications.

On June 1, the incremental version 13.5.1 was released with only one patch, the one corresponding to a kernel exploit discovered by the *unc0ver* group and used for *jailbreaking* on iOS 13.5 devices (not applicable in previous versions).

The new version of Apple's mobile operating system, iOS 14, was officially presented at the WWDC developers' (virtual) conference on 22 June.

In the next edition of this report, we will review the new security capabilities of iOS 14.

iOS exploits and their downward trend

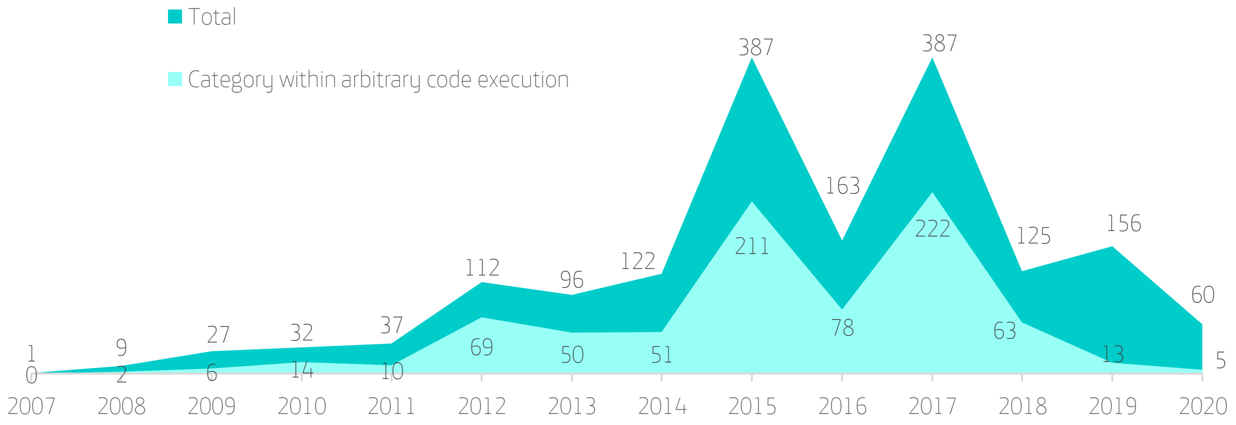
It is worth noting the statements of the exploit acquisition company, Zerodium, who reported that they were temporarily suspending the purchase of iOS exploits due to a high number of submissions. 13 has not been a good version for iOS.

Alternatively, researchers can submit their findings to Apple's security reward program (Apple Security Bounty), open to the public since late December last year. Rewards range from $5,000 to $1 million.

Vulnerability evolution in iOS - First half of 2020

VULNERABILITIES IN IOS 2020-H1

Vulnerability evolution per year



In total, **60 CVEs have been patched in the previous half year.** Of these, 5 were critical and allowed arbitrary code execution. Figures show a clear decrease (although we must wait for the second half of the year), but it has not been a good year for iOS in terms of security. Bugs have been devalued due to oversupply. **Let's remember that an exploit that allows compromising an Apple device completely was publicly priced at $2 million.** Currently, as mentioned in the previous section, Zerodium has temporarily suspended the purchase of iOS exploits.

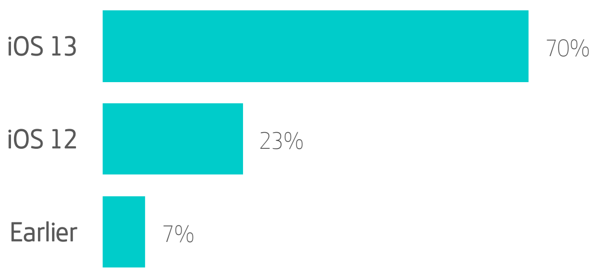
iOS fragmentation - First half of 2020

Fragmentation data for this half year show **70% adoption of the current version of iOS 13.** Followed by the previous version, 12, with 23% of installations. Only a little more than 7% of installations are versions prior to 12 and 13 (mainly iOS 11 and 10).

The adoption of iOS 13 is up 4 percentage points over the previous period. Two points for iOS 12 while older versions are down 6 percentage points.

APPLE IOS FRAGMENTATION 2020-H1

As measured by the App Store



The oldest device supporting version 13 is iPhone 6S, while version 12 is supported by at least iPhone 5S. Since 5S was released in September 2013, **most of Apple's devices are less than seven years old and more than half of these are five years old or less.**

iOS has no, or at least minor, issues when it comes to fragmentation. Apple users experience longer device support cycles. Even when the operating system changes within just over a year, relatively old versions of iPhone are usually supported. This greatly encourages the release of a new version of iOS and the replacement of older versions.

Android

Remarkable news

2020 began with a large group of security patches for Android 10. It was so early that, as a curiosity, Android received the first CVE of the year: CVE-2020-0001: a bug that allowed local privilege escalation without user interaction.

In total, Android has fixed more than 250 different security bugs, distributed in six bulletins published in the first week of each month. This release concerns the Android AOSP (Android Open Source Project) version and certain proprietary components of the base version.

Vendors learn about the vulnerabilities in advance so that they have enough time to release the corresponding patches (at least one month in advance). The idea is that they do not delay in releasing security updates in their respective Android customization and versions. Let's have a look at the main ones.

- BlueFrag: In February a patch was released for a serious vulnerability affecting Android 8 and 9, specifically the Bluetooth subsystem. An attacker could execute arbitrary code by simply getting close to a terminal with active Bluetooth, even without previous pairing. Luckily for Android 10 users, the exploitation attempt only resulted in a restart of the BlueTooth service. All vulnerable versions have been patched.

- StrandHogg 2.0: Another interesting vulnerability became known in early June. StrandHogg 2.0 is a re-release of a fixed vulnerability that affected the way Android handles multitasking. Properly exploited, StrandHogg allowed a malicious application to pose as a legitimate one. This was exploited to gain higher permissions and greater privileges in the system.

Android Enterprise Security White Paper

In January, the Android security white paper was updated. A report that outlines the security improvements and features of Google's mobile platform.

Android fragmentation

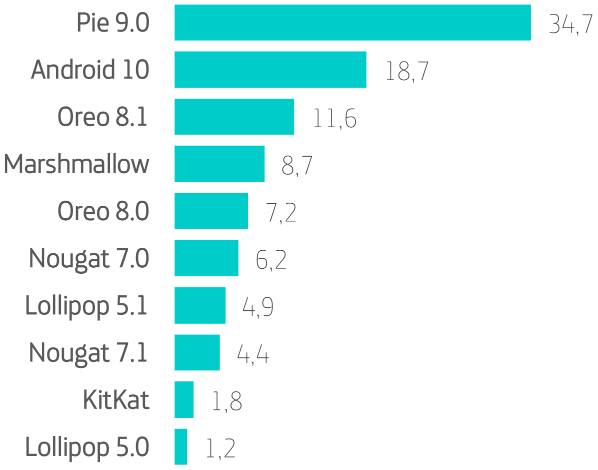
Android does not publish statistics on the developer portal to show the fragmentation status of versions, so the data here presented is that available from public sources, i.e. not checked against official sources.

Statcounter data suggests that currently only 18.69% of Android terminals have the latest version, Android 10. Most of them are still using its predecessor, Android 9, with a share of 34.66%. They are followed by a range of versions from 8.1 (11.62%) and 8 (7.15%), to Android Lollipop 5.0 with still a small 1.2%.

As we can see once again, **older Android terminals refuse to take retirement.** Average Android user extends the lifetime of their terminal beyond the security patch support term. In short, a risk often not detected.

External sources indicate that there could be over a billion Android devices without security patch support.

ANDROID FRAGMENTATION 2020-H1



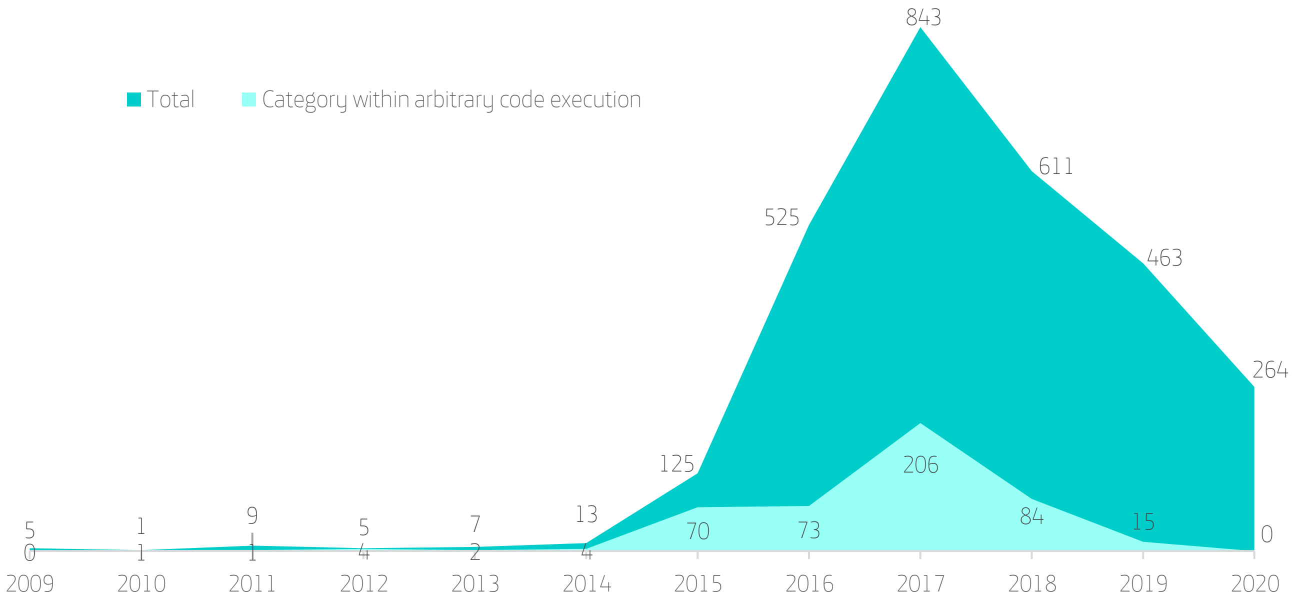
Vulnerability evolution in Android - First half of 2020

So far this year, **a total of 264 vulnerabilities have been released for Google's mobile platform.** Seven allow arbitrary code execution. **One serious Android vulnerability is priced at $2.5 million, according to Zerodium.** Note that this price is paid if an exploit with the ability to compromise an Android device "without" victim's intervention is already submitted. Finally, these prices must be considered with caution, since negotiations between researchers and brokers are not public and final prices are rarely disclosed.

The number of vulnerabilities leaves no room for doubt. Android is a popular platform for vulnerability hunters. This does not mean that it should be considered insecure. It is simply more attractive or interesting for various reasons, including the reward program and the marketing of exploits.

VULNERABILITIES IN ANDROID 2020-H1

Vulnerability evolution per year



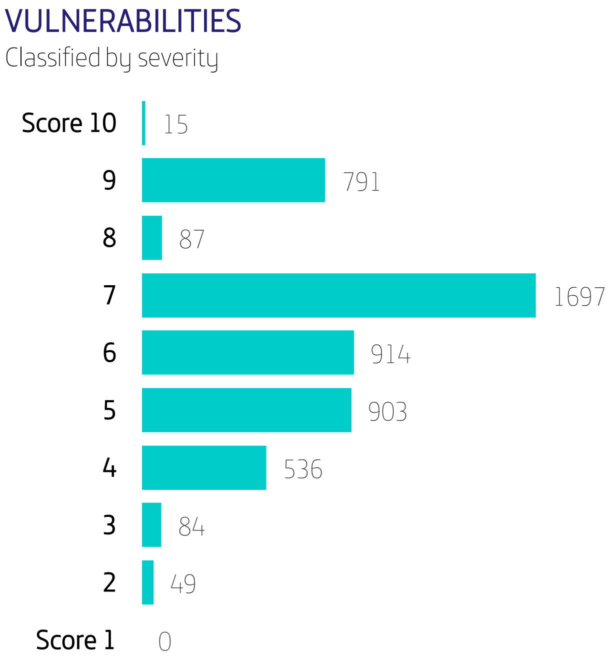
KEY VULNERABILITIES

This section addresses some of the vulnerabilities -maybe not so popular but notable from our point of view- of this first half of 2020. That is, those that must be highlighted for their particular significance or danger.

CVE ID	TARGET	DESCRIPTION	SCORING
CVE-2020-0796	Windows operating system	SMBGhost is hackable code execution issue in SMBv3, similar to the one exploited by WannaCry but in other versions of the protocol only present in Windows 10 versions 1909 and 1903. It was interestingly announced, only by Talos and Fortinet, but not by Microsoft, during a short period of time. It seems that they had access to privileged information and Microsoft decided at the last minute not to release the patch for this bug, so these companies removed the notice. Some days later it would release the patch.	10.0
CVE-2020-11896 CVE-2020-11897 CVE-2020-11901	Treck IP implementation	Ripple20 was actually a set of 19 vulnerabilities in the implementation of Treck IP protocols. As this manufacturer licenses its implementation, millions of devices would be affected, including IoT devices from vendors such as Intel, Carterpillar, Schneider Electric and so on. Within this set of flaws, three vulnerabilities stand out for their severity and reach.	10.0
CVE-2020-5902		This bug was in the F5 Big IP TMUI. A system usually present in the perimeter of companies and used for many purposes, usually critical. It is a Local Traffic Manager and has total power over the traffic that passes through it. Therefore, the impact of this remote code execution issue is more serious than it seems, since whoever exploits it will have access not only to the F5 system itself, but also to the service it manages on the network. From a DNS to a TLS certificate manager, anything within that network. Shortly after the issue was announced, attacks as a proof of concept were observed and later a functional exploit was made public.	10.0

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:



Top 25 companies with the highest number of CVEs gathered

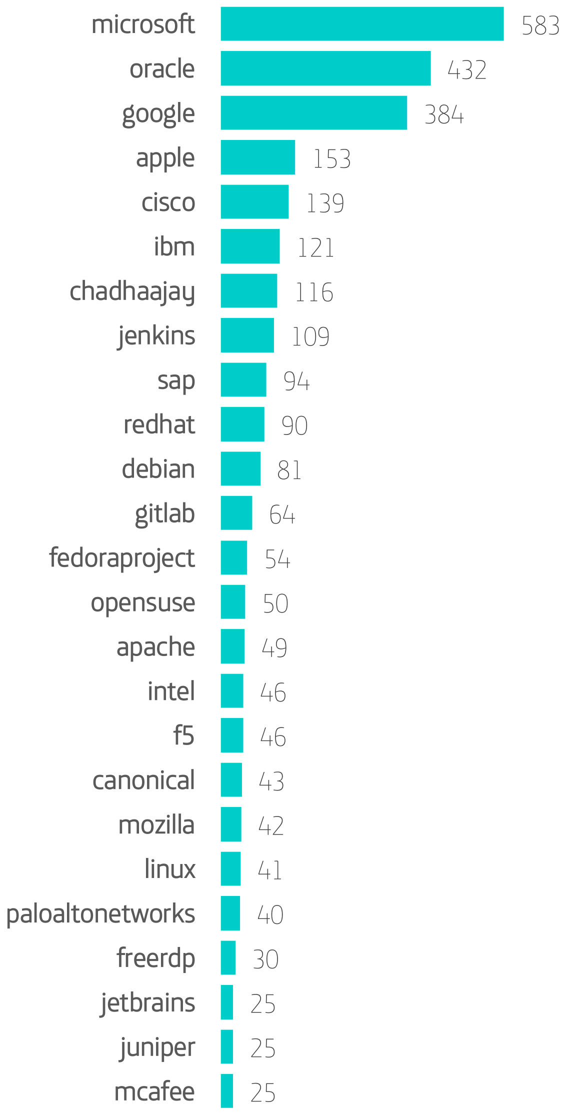
As on other occasions, data here presented must be relativized. This is due to the fact that some vendors have various products that may be candidates for getting a CVE, such as Oracle and its large product portfolio (high dispersion). Conversely, companies with a lower number of products that might 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.

It must be also highlighted 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: Linux kernel. When they share the same vulnerability or CVE, the relevant patch is distributed among all the vendors, who create a package for their particular distribution.

Even so, there are three leading vendors: **Microsoft, Oracle and Google**, the latter two exchanging positions with respect to the previous report. Also with respect to the previous report, a decrease in the number of CVEs gathered can be observed, in addition to the fact that from the 4th position onwards the decrease is much more pronounced.

VULNERABILITIES

Top 25 vendors by CVEs gathered



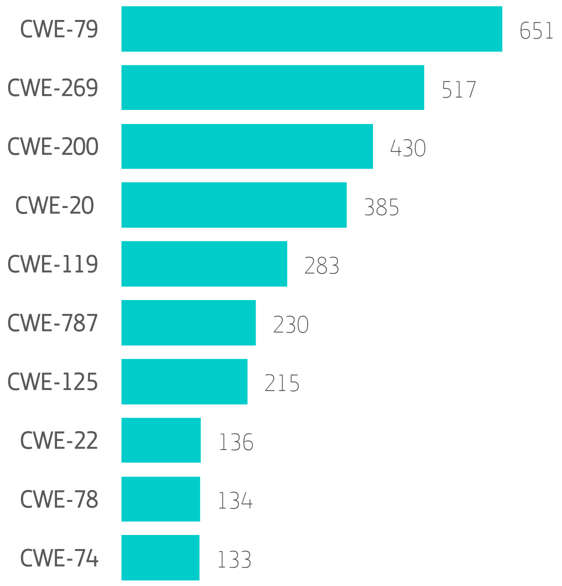
Top 10 the most representative CWEs

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 over the period analyzed.

VULNERABILITIES

Top 10 the most representative CWEs



Description 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	651
CWE-269	Improper Privilege Management	The application does not properly manage the permissions and privileges granted to a user	517
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	430
CWE-20	Improper Input Validation	Generic category that includes errors consisting of an inappropriate or non-existent control of user data input	385
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	283
CWE-787	Out-of-Bounds Write	Related to CWE-125, it groups those vulnerabilities that allow writing beyond the designated limits to a reserved buffer region	230
CWE-125	Out-of-bounds Read	Highly related to CWE-119, it includes read memory operations exceeding the control bounds of an intended buffer	215
CWE-22	Improper Limitation of a Pathname to a Restricted Directory	It is possible to manipulate the paths to files managed and used by the application, allowing access to resources protected or unrelated to the scope of the application	136
CWE-78	Improper Neutralization of Special Elements used in an OS Command	The application does not validate or filter values or fields from one component to another in the application when building operating system command calls	134

CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component	Basically, it refers to the non-validation or filtering of values or fields from one component to another in the application. This can lead to SQL-type injections or format string injection vulnerabilities.	133

Conclusions

Once again we observe as the attacks related to XSS are at the top. However, this half year the weaknesses related to insecure configurations in the management of user permissions are in second place, replacing those related to improper restriction of operations within the bounds of a memory buffer (reading/writing) (CWE-119), those related to the protection of sensitive information (CWE-200), or those based on improper input validation (CWE-20).

Regarding the latter three, in general terms, although the number of weaknesses identified with respect to the previous half year is down slightly, a year-on-year analysis (i.e. with respect to the same period of the previous year) shows that the rate of decline is much lower.

WHO IS WHO IDENTIFYING MICROSOFT VULNERABILITIES

Who finds more vulnerabilities in Microsoft products? **What percentage of vulnerabilities are discovered by Microsoft, other companies or vulnerability brokers? How many flaws have unknown discoverers?** Over this report we have analyzed the data of the last three and a half years with the aim of understanding who fixes what in the world of Microsoft products as well as the severity of these flaws. **Thanks to this report we will gain an interesting insight into who really investigates Microsoft products, reports them in a responsible manner, as well as how many vulnerabilities are attributed to someone and how many are not** (which might suggest that they are discovered by attackers).

On the second Tuesday of each month, Microsoft publish their traditional security patches in a single package to update Windows. Such update fixes a number of CVEs or vulnerabilities. However, this has not been always the case. For many years, they published bulletins hiding several CVEs, usually grouped by product.

For many years, Microsoft have incorporated in their Security Development Lifecycle practices an audit of their own code with the aim of improving their security. We wished to know exactly how many security flaws are found by the company over their internal audits **to get an idea not only of how much Microsoft contribute to the improvement of their products in terms of security, but also of how much the rest of usual 'bug hunters' of the industry do it.**

Methodology

We have performed a very simple analysis. We have collected and processed all the information of attributed CVEs during the second half of 2019. The source of information has been mainly the following webpage:

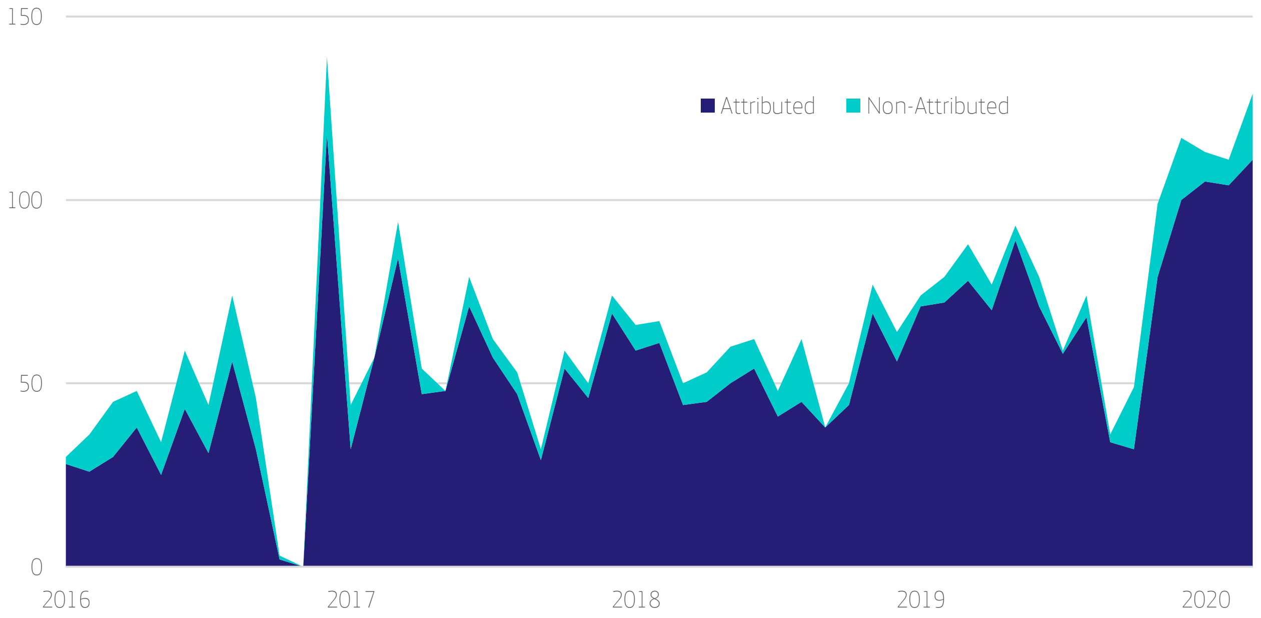
https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

These are the attributed vulnerabilities (that is, the ones reported by a given identifiable user, either individual or company). During this period, we have analyzed 390 attributed vulnerabilities. From all of them, we have extracted their severity through the NIST's official CVSS.

Nevertheless, these figures do not represent the total number of flaws discovered (more than 600). We consider that most of these flaws may come from vulnerabilities found in 0-days or under other circumstances where the author is not known and the vulnerability has not been reported anonymously. In such cases, Microsoft do not attribute the finding to anyone in particular. This difference between attributed and 'non-attributed' vulnerabilities (which is not the same as 'anonymous') is represented in the following chart.

NOT ALL VULNERABILITIES COME FROM ATTRIBUTED SOURCES

Number of vulnerabilities (Attributed and Non-Attributed) from 2016 to 2020 H1



From the credits, we have extracted the company that found the vulnerability. **If there were several discoverers, we have considered only the one that appeared in the first place in order to make the calculations simpler** and since we understand that the one who reported them first is shown as the main analyst. While this might be inaccurate, it results in the simplest formula. Moreover, we have considered two flaws found by the Hiper-V team as discovered by Microsoft.

From that point, we have performed different calculations to analyze who contributes more and better to improve the security of Microsoft products, in a responsible manner.

The Data

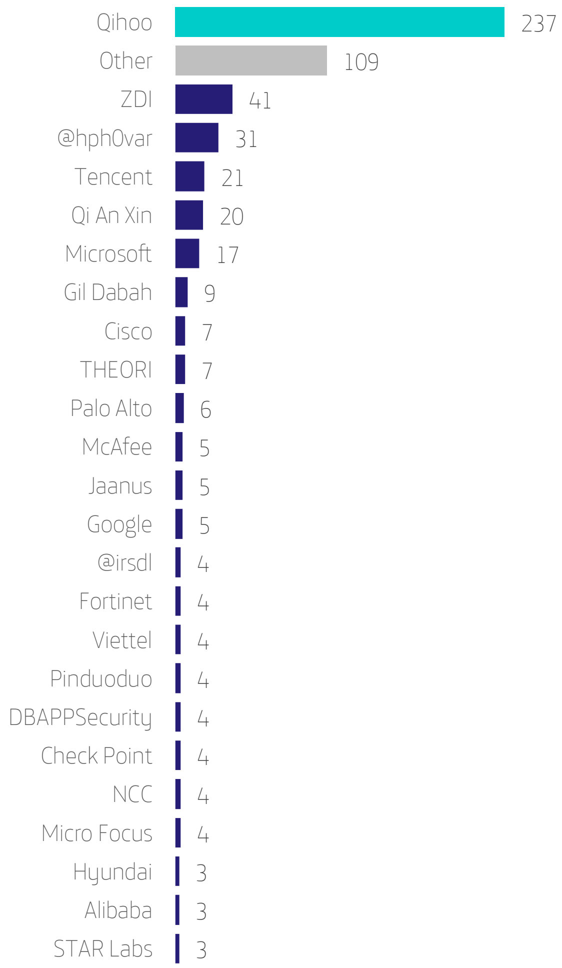
Qihoo is again the most popular with a total of 237 vulnerabilities reported to Microsoft. But compared to the previous quarter, the numbers have changed substantially.

Qihoo and ZDI report the highest number of vulnerabilities

Google falls, and heavily. While last half year it was in fifth place, this half year it has fallen to 14th place. Microsoft, which was in third place, falls to sixth. Has the pandemic impacted the major vendors? Have they spent less time on vulnerability research? On the contrary, **Qihoo not only continues to be the first company to find Microsoft security flaws, but has also substantially multiplied its number, from 79 to 237 this half year.**

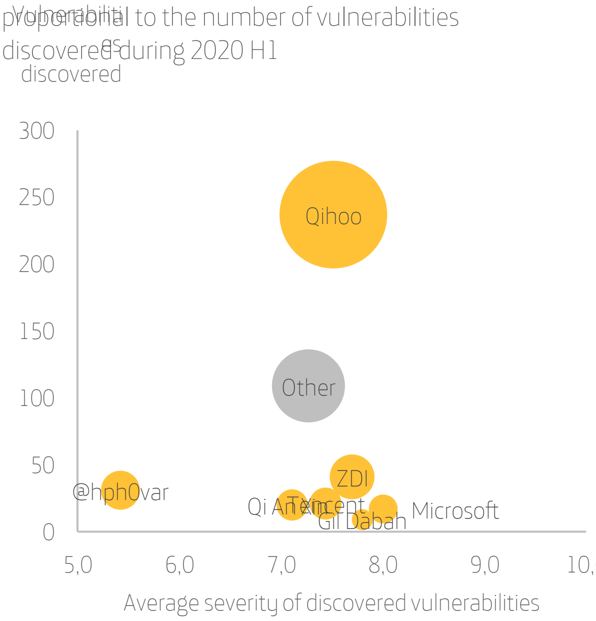
QIHOO DISCOVERS THE HIGHEST NUMBER OF VULNERABILITIES IN MICROSOFT PRODUCTS

Total number of vulnerabilities per discoverer in the first half of 2020



QIHOO REPORTED ALMOST HALF OF THE VULNERABILITIES

Distribution of vulnerabilities by severity and discoverer; the size of the bubble is proportional to the number of vulnerabilities discovered during 2020 H1



Conclusions

In a six-month period when Microsoft has exceeded 100 fixed vulnerabilities, Qihoo has found 237, many more than the previous quarter and substantially displacing Microsoft itself and Google, which were the other companies that found the highest number of bugs in Microsoft software.

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 significant 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 with the aim of diverting attention and undermining them.

Significant APT operations detected over the first half of 2020

Within this framework, SARS-COV-2 virus has been a key player as one of the main baits in the actions of APT groups. Other groups have been involved in cyberespionage, and others are simply back with their umpteenth campaign. The most outstanding groups in this half year have been the following:

Kimsuky (Aka"Velvet Chollima"): By land, sea and Office.

This group, active since 2013, has used the impact of COVID-19 to extend its influence with spear-phishing attacks and Office documents. Their preferred tactics have been the injection of templates using CVE-2017-0199 vulnerability and the malicious use of macros. This group has been linked to attacks against U.S. and South Korean targets, including South Korea's nuclear power plants in 2014.

Winnti: Non-stop

In the previous report we mentioned this group as one of the most remarkable for its activity, and they are again in this list. This time, using RTF files and a backdoor called "Chinoxy", based on another used by the same group during a campaign against Vietnam in 2014.

APT32 (Aka "OceanLotus Group"): Truth is out there

If other groups are linked to COVID-19 for trying to gain profit from fear and confusion of others, this group (supposedly supported by the government of Vietnam) stands out for having launched attacks against the Chinese administration in its search for information about COVID-19. At least, that is what Mandiant researchers think, claiming that the group has been detected attacking Wuhan regional government as well as the Chinese Ministry of Emergency Management in an attempt to gather information.

APT39 (aka “Chafer”): About espionage

This Iranian group has been detected in a cyberespionage campaign against critical infrastructure in Kuwait and Saudi Arabia using such an important element in the supply chain as telecommunication providers. These tactics are common in the group and have already been linked to similar attacks in other countries such as against Turkey in 2014.

PROMETHIUM (aka “StrongPity”): Will always go back

This group, first identified in 2002, is again active and spreading its threat of software impersonation between Europe, America and Asia (Middle East, India, Vietnam and so on). Cisco and Bitdefender researchers have managed to track down up to 72 C&C servers with different targets. The researchers suspect that the attack vector is a "Watering Hole" attack, although they cannot confirm this. Without a doubt, one of the great achievements of this group is that they remain active for so long, since usually such active and long-lived groups tend to fall apart unless they are supported by states. More info.

Bonus Track: ShadowBrokers collection continues to make headlines

ShadowBrokers group went down in history in 2016 for publishing NSA files. What also deserves a note in history is that a few files leaked in 2016 are still a topic after 4 years. Juan Guerrero-Saade, a security researcher and associate professor at the Johns Hopkins University School of Advanced International Studies, has published a study saying that behind some of the files leaked by ShadowBrokers there is a group not yet detected that could be of Iranian origin. Although it is only a (well-based) hypothesis, the fact that this half year another interesting thread related to the files leaked by ShadowBrokers has been found, well deserves a space in this report.

CYBER RISK RATING BY SECTOR

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

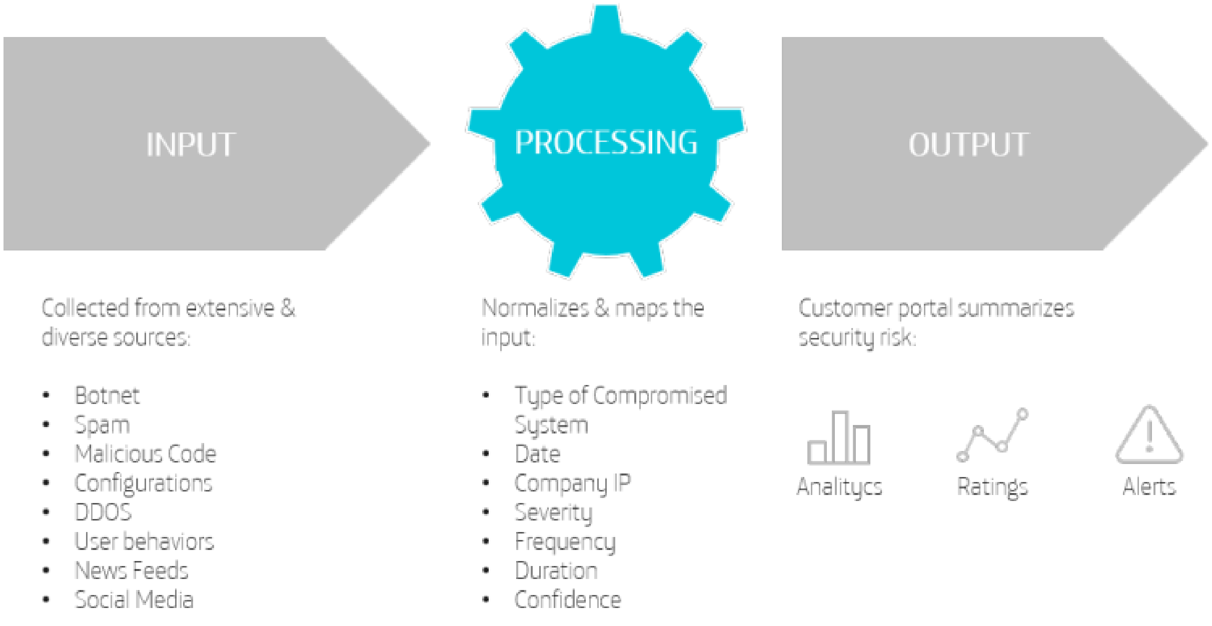
BITSIGHT®
The Standard in SECURITY RATINGS

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 significant 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), for both Europe and Spain.



Collected from extensive & diverse sources:

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

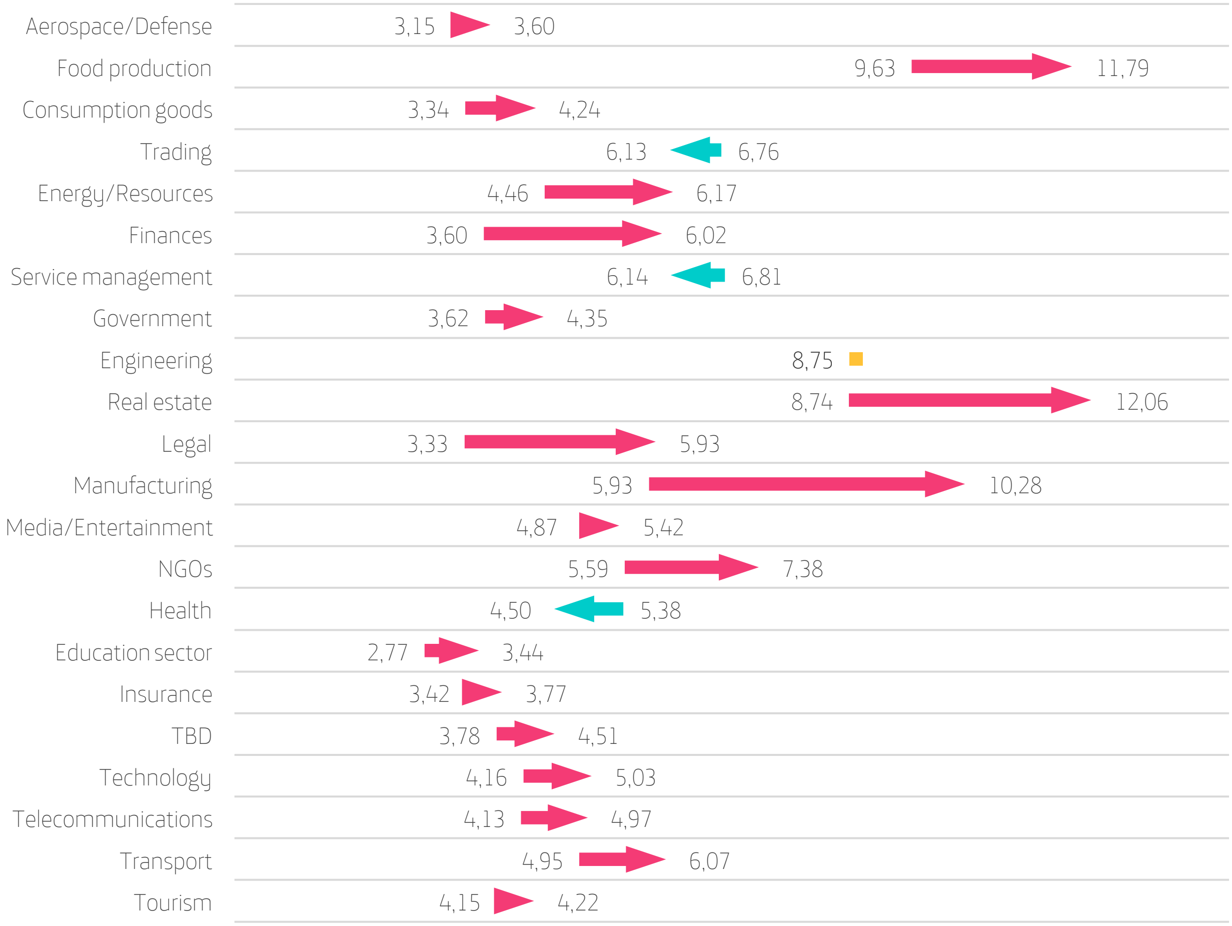
Normalizes & maps the input:

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

Customer portal summarizes security risk:

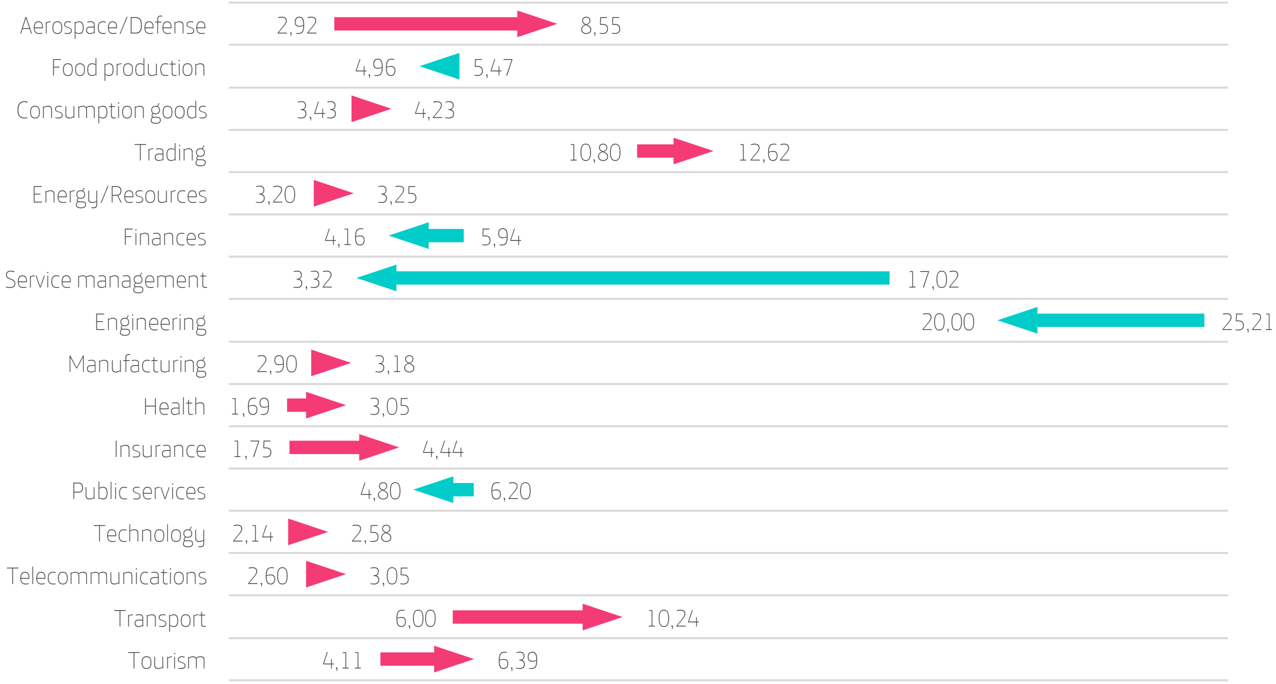
SECURITY PRACTICES IN EUROPE

Evolution from 2019-H2 to 2020-H1 of the average number of effective **days** needed by a **European company** to fix a malware threat (grouped by sector)



SECURITY PRACTICES IN SPAIN

Evolution from 2019-H2 to 2020-H1 of the average number of effective **days** needed by a **Spanish company** to fix a malware threat (grouped by sector)

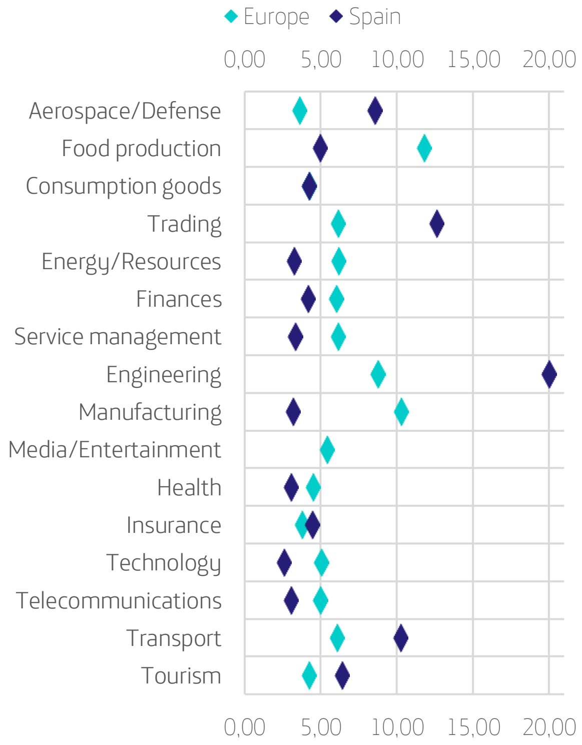


In these graphs we can see how the response by sector differs from the previous six months. **The drop in "Service Management" from more than 17 days to just over three days is noticeable.**

The following graph compares the response time between Spain and Europe during the first half of 2020 (grouped by sector).

COMPARISON DETECTION-NEUTRALIZATION BETWEEN SPAIN AND EUROPE - 2020-H1 (BY SECTOR)

In average number of days



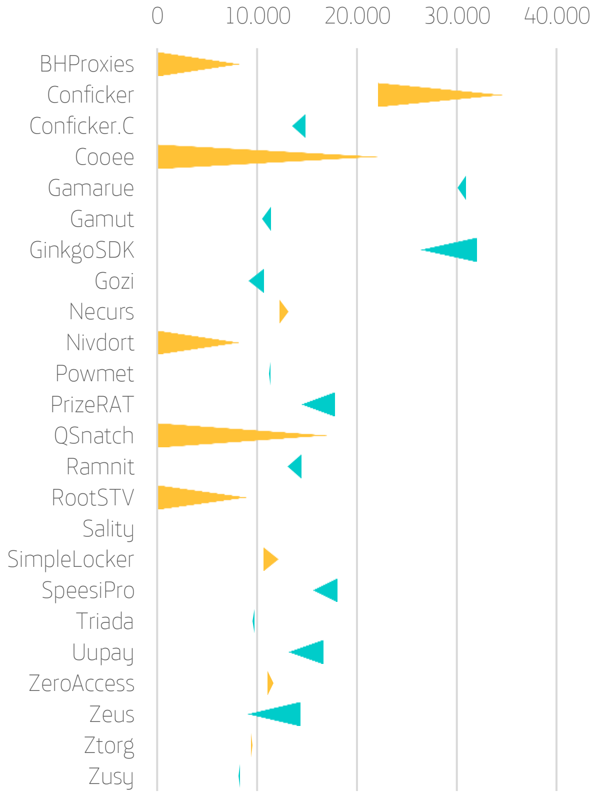
This means that, for instance, the Spanish trade sector needs about 14 days on average to neutralize a threat, while generally in Europe they need about 7. Generally speaking, Spain needs fewer days on average than other European countries to neutralize a security incident.

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.

EVOLUTION OF THE 25 MOST AGGRESIVE MALWARE FAMILIES IN EUROPE

Increase (orange) or decrease (blue) experienced from 2019-H2 to 2020-H1 (measured on infected systems)



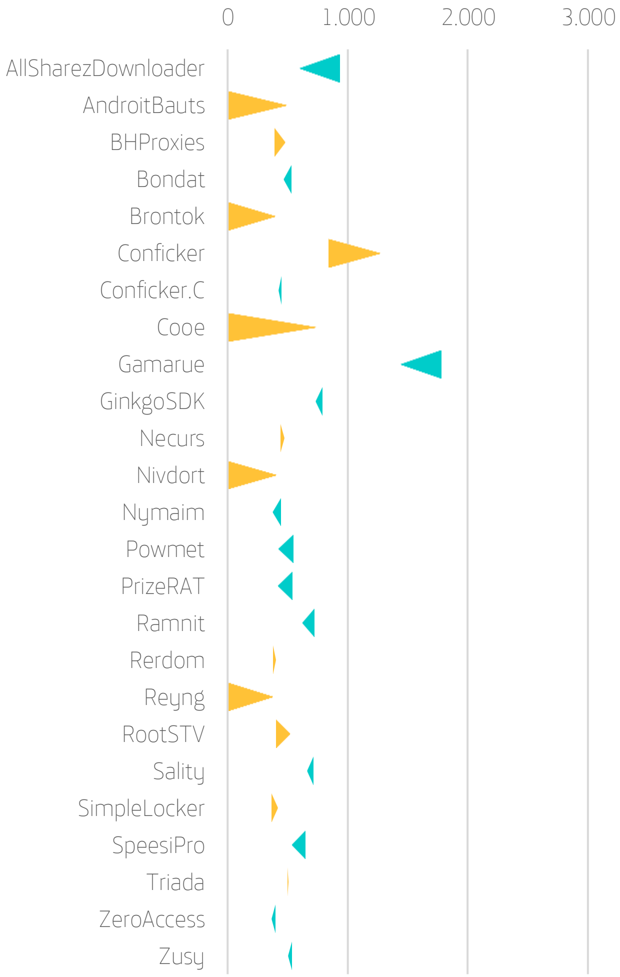
The 25 families of malware and infections detected in Spain

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

In Spain, there is a very different leading malware from the other European countries. Firms such as *AllSharezDownloader* and *AndroidBauts* are leading, while in Europe they are not representative.

EVOLUTION OF THE 25 MOST AGGRESIVE MALWARE FAMILIES IN SPAIN

Increase (orange) or decrease (blue) experienced from 2019-H2 to 2020-H1 (measured on infected systems)



SUMMARY

In the field of smartphone security, **the high number of exploits for IOS 13**, the announcement of IOS 14 and Android fragmentation have marked the first half of 2020.

With regard to **vulnerabilities and weaknesses, there has been a clear decrease in the figures for vulnerabilities (especially Level-10 ones) but the three vendors with the highest number of associated CVEs remain the same.** Regarding weaknesses, those where insufficient or no security configuration is key in the management of user permissions stand out, allowing an escalation of permissions.

The APT groups have also introduced "SARS-CoV-2" factor in their operations. Some to make a profit, and others in cyberespionage operations to find out "the truth" about the virus.

This half year Microsoft has exceeded 100 fixed vulnerabilities every month, **Qihoo has identified 237, many more than the previous quarter and substantially replacing Microsoft itself and Google**, which were the other companies that found the highest number of bugs in Microsoft software.

Bitsight's data shows that the unbreakable Conficker is once again on the throne of the most aggressive threats, while we also note a worrying fact: **In most sectors there is a substantial increase in the time required to neutralize a threat.**

Useful Links

Don't stay only in the top layer of cybersecurity analysis. Our half-yearly reports are cumulative and summarized. On our ElevenPaths blog there is much more information and news that may interest you. Below are the most outstanding posts from the first half of 2020.

CRYPTOGRAPHY

RSA contra las cuerdas: 1.001 razones por las que está cayendo en desgracia (I y II) [Only in Spanish]

SHA-1 no celebrará más cumpleaños, ha muerto [Only in Spanish]

Criptografía eterna: cómo cifrar los datos hasta el final de los tiempos [Only in Spanish]

Si WhatsApp cifra las comunicaciones, ¿dónde está la clave? [Only in Spanish]

Criptografía Ligera para un mundo doblegado bajo el peso del IoT [Only in Spanish]

OpenPGP: Desperately Seeking Kristian

MALWARE

Apple introduces up to 14 signatures in XProtect given the malware flood for Mac

APTualizator (II): Deconstructing Necurs Rootkit and Tools for Detecting and Removing It

CARMA: Our Free Research-Focused Set of Android Malware Samples

Most Software Handling Files Overlooks SmartScreen in Windows

PRIVACY

What Differential Privacy Is and Why Google and Apple Are Using It with Your Data

Let's Encrypt revoca tres millones de certificados por culpa de un &amp; en su código [Only in Spanish]

More and Shorter Certificates with a Lower Lifetime: Where Is TLS Going to?

Las "Third Party Cookies" y cómo las maneja cada navegador [Only in Spanish]

CORONAVIRUS

How to Detect and Protect Yourself from Phishing Attacks in Times of Coronavirus

Fake News and Cyberthreats in Times of Coronavirus

DataCOVID-19: Fighting the Coronavirus by Using the Approximate Location Data of Your Smartphone

20 Questions about Covid-19 Tracing Apps

The Security behind Apple's and Google's API for Tracing COVID-19 Infections

Anti-Coronavirus Cryptography

Vendetta Group and the COVID-19 Phishing Emails

ElevenPaths Radio – 2×10 Interview with Elad Rodríguez [Only in Spanish]

About ElevenPaths

At ElevenPaths, Telefónica's Cybersecurity Company, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We are always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

We combine the freshness and energy of a start-up with the power, experience, and robustness of Telefónica to provide solutions that enable prevention, detection, and response against everyday threats in our digital world.

We build strategic alliances to provide a strengthened security to our clients. Moreover, we work jointly with organizations and entities such as the European Commission, Cyber Threat Alliance, ECSO, EuroPol, Incibe, and the Organization of American States (OAS).

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.