Telefónica Tech

Cyber Security Report 2021 H1

July 2021

From mobile security to vulnerability analysis, from breaking news to privacy analysis, understand the risks in today's landscape.

telefonicatech.com

Index

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

1. Executive summary

The purpose of this report is to summarise the cyber security information of the last few months (from mobile security to the most relevant news and the most common vulnerabilities), taking a point of view that covers most aspects of this discipline, in order to help the reader understand the risks of the current landscape.

The first half of 2021 has again been marked by the effects of SARS-CoV-2 but from a more optimistic point of view thanks to the global progress of vaccination. Where there is no optimism whatsoever is in the advance of ransomware.

This first half of the year we have seen a large number of companies worldwide affected by this serious problem. From ministries to large American companies. From small companies to critical infrastructures.

The Colonial Pipeline attack in May represented a milestone in the world of ransomware in general and cyber securityin particular, as its effect was felt across the country, provoking a variety of reactions. **Among the general public, the threat of ransomware materialised as something much more tangible that not only affected their personal systems, small businesses or even large companies, but could affect their core supply resources**. Also, because of the leaks ofall kinds of personal data in companies during this half year, users have become aware of how exposed their information can be.

At the policy level, Joe Biden himself signed an executive order aimed at improving cyber security in general and treating ransomware as terrorism. The war, in many areas, is intensifying.

In the area of vulnerabilities, the 0-days found in Chrome, which are becoming more and more common, and FragAttacks, flaws from more than 20 years ago in Wi-Fi networks that fortunately have not had a major impact, havestood out.

In the mobile malware section, we have seen how, with increasing sophistication, Android trojans have discovered ways to trap notifications and attack WhatsApp contacts by automatically replying to messages that reach the victim.

This semester we are delighted to inaugurate a new section specialising in industrial threat analysis. This is possible thanks to our **Aristeo** project, a network of **industrial decoys** that use **real OT devices** to confuse attackers and extract the necessary information to generate intelligence to strengthen our clients' defences.

Whether you are an amateur or a professional, it is important to be able to keep up with cyber security news: what isthe most relevant thing going on? What is the current landscape? With this report, readers will have a tool to understand the state of security from different perspectives and will be able to understand its current state and predict possible trends in the short term. The information gathered is largely based on the compilation and synthesis of internaldata, cross-checked with public information from sources we consider to be of the highest quality.

Here we go!

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

2. The most important incidents in the first half of 2021

Here are the news items that have had the greatest impact over the course of the first half of 2021

JANUARY

- To patch or not to patch end-of-life (EOL) systems? **Cisco returns to the controversy** by not wanting to patch the latest 74 vulnerabilities in several of its popular devices, because they have reached the end of their life cycle and invites users to purchase the latest versions.
- **A fraudulent APK is capable of sending messages via WhatsApp** to the victim's contacts. It takes advantage of notifications received on the phone to respond quickly with a link that appears to be from the Play Store, but, in reality, it redirects to another URL where the malware is downloaded.
- Google uncovers an operation that exceeds any other criminal activity that would have targeted cyber security experts by its elaborate machinery to reach them. The campaign appears to have been orchestrated by the North Korean government and they bothered to build profiles of supposed vulnerability and exploit researchers on Twitter, who supported each other's work, made themselves known in the community and boasted about their skills **in order to gain each other's trust and later exchange information with other real experts.**
- On January 11th, the Norwegian company AKVA Group, which deals with industrial fish farming (including boats), announced that it had been attacked and part of its control services had been blocked. The culprit was an attack that ended up with ransomware locking down its systems. **In its first quarter accounts, AKVA put the losses generated by the cyber-attack at $6 million.**
- On 25 January, PALFINGER, a company with 25 locations worldwide and more than 11,000 employees, which offers technological solutions in the field of engineering and specialises in cranes and lifting systems, **suffered a global attack that left much of its infrastructure blocked**. Production was shut down for two weeks in a company that generates more than $1.5 billion annually.

FEBRUARY

- From version 90 onwards, **Chrome displays a certificate error when a user tries to access any website with a certificate signed by Camerfirma**. Although perhaps not the most popular CA, it is very present in Spain in many public organisations.
- After the FreeType flaw discovered at the end of 2020 and which actually consisted of two problems (one to exploit and one to escape from its sandbox), **another real 0-day (of which attackers are taking advantage) has been discovered in this browser**. It is the sixth in just a few months.
- Kenna Security has studied 18,000 vulnerabilities catalogued with their CVE and concludes that **only 473 were exploited in 2019 in a way that posed a real threat to companies**. That is just 2.6%. Of these, in turn, only 6% have become popular in their exploitation.
- Criminals gained access to a water plant in Tampa, Florida, which serves about 15,000 people. They took advantage of the Team Viewer connection to access the system and **modify the amount of sodium hydroxide (lye) to pour in a much higher amount than normally used (to control the acidity of the water)**. The case was brought to the attention of the FBI and the Secret Service.
- On February 28th, PrismHR, which manages more than **$80 billion annually in payroll for more than 80,000 companies, acknowledged a "cyber incident" affecting its payroll and employee benefits software**. Although not explicitly stated, some media reports placed it in the context of a ransomware attack.

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

MARCH

- The seriousness of the latest vulnerabilities in Exchange (specifically CVE-2021-26855, ProxyLogon) has forced Microsoft to make an interesting move: **Microsoft Defender, the "built-in antivirus", includes automatic mitigation of the security problem**. A simple update will mitigate the vulnerability (it will not be fixed until it is patched, but attackers will find it more difficult to exploit it).
- More supply chain attacks, and this time on PHP. **Someone broke into the official GIT of the PHP code and added a backdoor**. If this version is used, an attacker would have to enter the string "zerodium" in a "fake" User-Agent with a double T at the end and could execute code on the server.
- **Ransomware attack paralyses the Spanish Employment Service, SEPE, for days.** The UK Foreign, Commonwealth and Development Office reported the leak of confidential documents relating to British aid projects, including details of projects funded by a secret national security fund.

APRIL

- Another step has been taken in the plan to get rid of Emotet. Initially, the domains and command and controlsused by the malware were hijacked, so that they could be "deactivated" as much as possible. **Now, the policeare going to send a message from these servers to the malware installed on the systems to remove it completely.**
- The data of more than 13 million Phone House users are made public.
- **The Natantz nuclear power plant (Iran) suffers a cyber-attack that causes a blackout, 24 hours after it was commissioned**. The Iranian government initially claimed it was an "accident", but after Israeli press reports claimed it was a cyber-attack, it described it as "nuclear terrorism".
- On 24 April, a series of cyber-attacks brought down several Spanish national services, including the websites of several ministries and the INE (National Statistics Institute).

MAY

- AXA takes a decision in France: **cyber insurance coverage will not return ransom money to customers who pay for extortion**. This decision was taken in the context of a senate roundtable in France addressing "the devastating global ransomware epidemic".
- The executive order signed by **Biden against ransomware aims to modernise cyber security defences**. This executive order will mean that companies will have to meet minimum standards, procedures will be in place,audits will be conducted... it will lead to a healthier industry.
- Mathy Vanhoef, a security academic at New York University in Abu Dhabi, discovers **the FragAttacks, a seriesof 12 vulnerabilities in WiFi that have been around since almost the initial deployment of the technology.**
- On May 4th and 5th, the Norwegian company **"Volue" suffered a ransomware cyber-attack that blocked water and wastewater facilities serving 85% of the country**. This also prompted the company itself, as a precautionary measure, to shut down and quarantine hundreds of devices it has deployed across Europe.
- On May 7th, **the company "Colonial Pipeline", which supplies hydrocarbons to a large part of the US east coast, was blocked by a cyber-attack that encrypted its systems**. This caused an average 4% increase in fuel prices and the total blockade lasted 6 days. Investigations suggest that a compromised password for access tothe company's VPN may have been the criminals' entry point.
- On May 14th, Ireland's public health service, the HSE, was hit by a ransomware cyber-attack that forced the cancellation of appointments and diagnoses at several hospitals.

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

JUNE

- **A new type of TLS attack**, ALPACA, is unveiled. **It would allow browser traffic to be redirected to a different service in order to access or exfiltrate sensitive information.**
- On June 4th, news broke that the **US Department of Justice was going to equate ransomware attacks with terrorist attacks** in terms of prioritising investigations and prevention of these crimes.
- On June 8th, **the FBI announced that they had recovered 63.7 Bitcoins out of the 75 that were paid to the criminals who attacked Colonial Pipeline**. Despite recovering more than three-quarters of the total, the valueof the Bitcoin at the time of the recovery brings the total recovery to $2.3 million, whereas when the paymentwas made, the same amount was more than $3.8 million.

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

3. Mobiles

3.1. Apple iOS

Highlights

We left 2020 with iOS 14.3 and it wasn't until 26 January, of a brand new 2021, that version 14.4 saw the light of day. **It was loaded with security patches, as many as 55 fixed CVEs**. Almost half of them were to prevent the execution ofarbitrary code, the jewel in the crown of the exploit.

Halfway between iOS 14.4 and 14.5, an urgent patch had to be released on March 8th: 14.4.1. It fixed a very dangerous vulnerability (CVE-2021-1844) for arbitrary code execution that could be exploited by simply visiting a malicious website. The fright, provided by the researchers of the Google Threat Analysis Group, did not stop there and on March26th, in the same way, version 14.4.2 was released as a matter of urgency. It was another vulnerability (CVE-2021- 1879) with identical impact.

On April 26th, iOS 14.5 was released, a major revision in the life cycle of version 14. Up to 60 vulnerabilities were fixed, 12 of them involving the execution of arbitrary code. This version of iOS brought an interesting unlocking option based on facial recognition. In the case of an unlocked Apple Watch and at close distance, the user can unlock the terminal while wearing a mask.

In addition, iOS 14.5 brought a new privacy protection feature. By default, unless otherwise provided in the settings, iOS will block all attempts and requests by apps to track the user. Another new option allows you to enable automaticinstallation of security updates. That is, the system will not wait for the user's decision to install a patch (e.g., 14.4.1 and 14.4.2). Once iOS detects that it is a security patch, it will choose to install it directly.

On May 3rd, a new minor version was released ahead of iOS 14.6. **14.5.1 fixed two new security holes in WebKit**, Safari's web rendering engine, which could lead to arbitrary code execution when visiting a malicious website.

Finally, version 14.6 was released on May 24th. The new version comes with **43 vulnerabilities fixed, 8 of which are arbitrary code execution vulnerabilities.**

iOS vulnerabilities evolution during the first half of 2021

An exploit that guarantees remote execution of arbitrary code on iOS is still priced at $2 million. Half a million below its Android equivalent.

The first half of 2021 closed with more than 200 vulnerabilities patched, 50 of which are considered high-risk, with thepossibility of executing arbitrary code. Some of them affect the kernel of the system itself.

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

IOS VULNERABILITIES 2021-H1
Vulnerabilities evolution by year

Version fragmentation during the first half of 2021

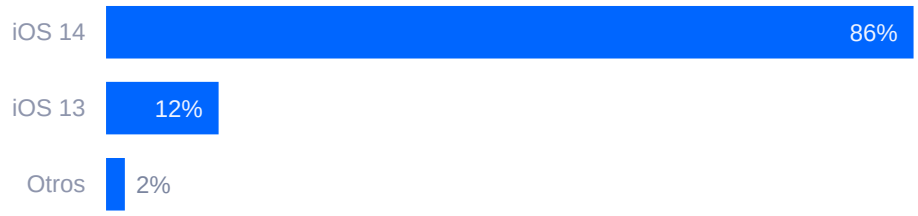
Historically, fragmentation has never been an issue for iOS developers. The advantage of having a homogeneous platform is indisputable and continues to produce almost identical figures every time we review iPhone users' adoption of a new version of the operating system.

If last semester iOS 14 held a 72% share of devices, six months later iOS 14 increases its population to 86% of devices. As usual, the outgoing version is a discreet, but still significant, second place with a 12%. In the same place was iOS 13with 18% six months earlier.

The numbers vary from previous years in the sense that Apple's mobile devices are adopting the new versions with a higher degree of acceptance.

In addition, iOS 14 will continue to be supported on iPhone 6s and SE models, handsets that are almost six years old. A considerable amount of longevity when it comes to mobile platforms.

Apple iOS Fragmentation 2020-H1 (According to App Store data)



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

3.2. Android

Highlights

Android 12 is just a few days away from taking over. If the same release schedule as the last few versions is followed, Android 12 will see the light of day in September 2021. The Android 12 beta was announced and released on 18 February. In the next report, we will take a look at what's new in the security and privacy chapter.

As for Android 11, the operating system we have been using since September 2020, it has released six major cumulativesecurity patches. One per month, typically, released in the first week.

As an advance in the chapter of new security features, Android 12 will come with a dashboard in which the user will be able to check what data has been accessed from the device and how often. For example, we will be able to see which application has accessed the microphone and how often.

As with iOS, Android will display a small icon in the status bar when the microphone or camera is currently activated. This warns the user of the use of these functionalities. The new version of Google's mobile operating system will also display a message alerting the user that the active application is reading the clipboard.

Fragmentation on Android systems

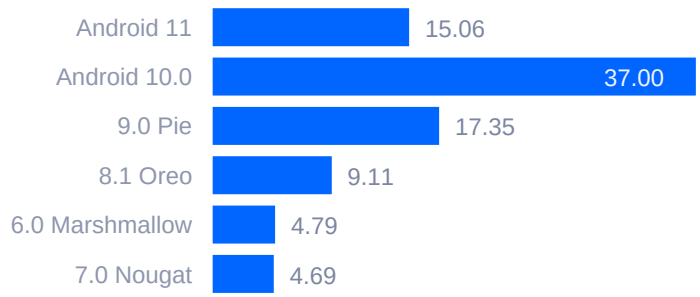
Android does not publish statistics showing the state of fragmentation between versions. The data obtained are frompublic sources, i.e., they are not checked against official sources.

Statcounter's latest publication at the time of writing this report shows that the most widely deployed version of Android is still Android 10, with a 37% share, only three points less than the previous edition. It is followed by Android9 with just over 17% (dropping up to six points).

Android 11, the current system, only stands out with 15%, almost a quarter to a year after its release.

The remaining portion is shared by versions lower than 9, where none of them exceeds 10% of the market. Nonetheless, it is surprising that Android versions such as 8, 7 and 6 have a total share of almost 20%. Remember thatAndroid 6 (or 5.1.1 "Lollipop") was released in 2015.

ANDROID FRAGMENTATION 2021-H1



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

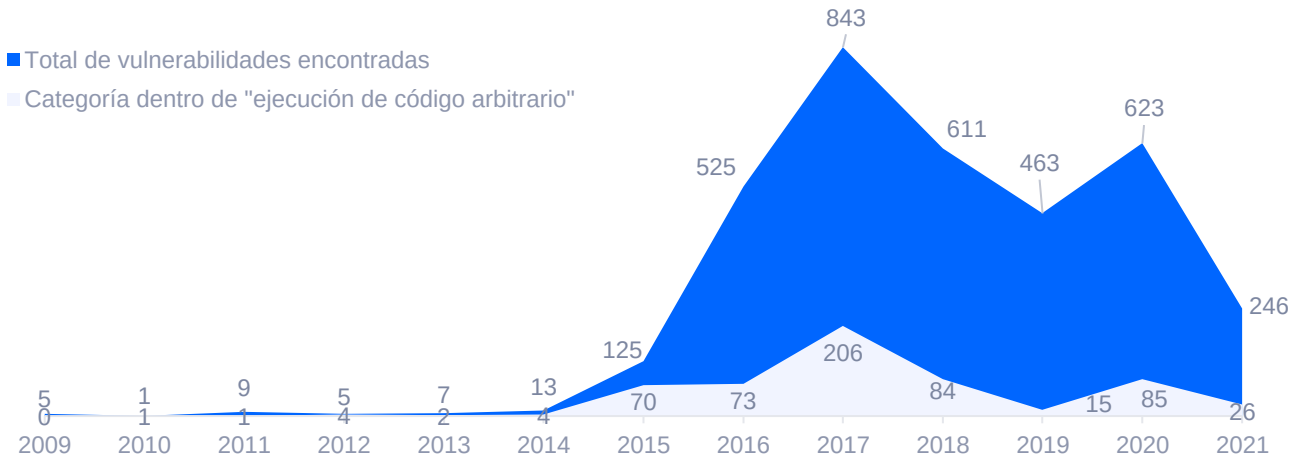
Android vulnerabilities evolution during the first half of 2021

An exploit that guarantees the remote execution of arbitrary code on Android continues to be priced at two and a halfmillion dollars. There has been no change to the remuneration amount for quite some time.

Google typically releases a set of security patches every month. So there have been six bulletins released, with a totalof 246 CVEs or vulnerabilities fixed. **26 of them critical**.

However, many of these flaws affect software or firmware from particular manufacturers, which means that the same vulnerability does not necessarily affect the entire Android device fleet, but only those with the affected components.

ANDROID VULNERABILITIES 2021-H1
Vulnerabilities evolution by year



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

4. Significant vulnerabilities

In this section we will comment on some of the most significant vulnerabilities, in our opinion, in the first half of 2021, meaning those that stand out due to their special relevance or danger.

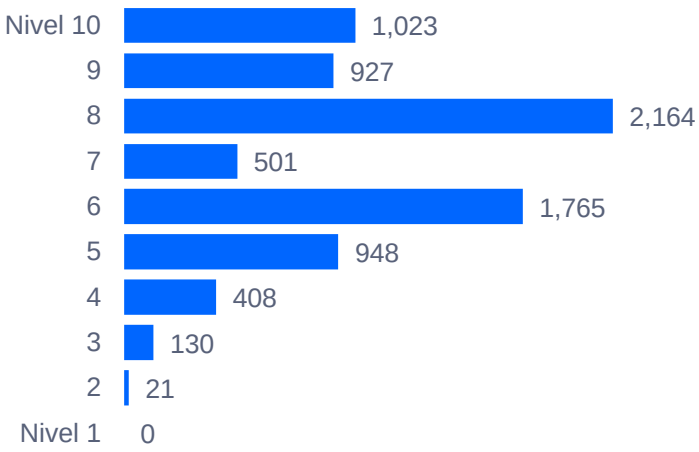
CVE ID	TARGET	DESCRIPTION	*SCORING*
CVE-2021-24092	Windows Defender	A privilege escalation in BTR.sys when analysing files. The curious thing is that it had been hidden for more than 12 years. Perhaps because the file did not always remain on disk but was occasionally stored and loaded when needed.	7.8
CVE-2020-9592 y CVE-2020-9596,	Adobe reader (although the problem is with the PDF standard)	The flaw, also called "Shadow attacks", allows changes to be made to a PDF even after it has been cryptographically signed, leaving the signature intact.	7.8
CVE-2021-21972	vCenter from VMWare	With a simple HTTP request to the vCenter API it is possible to exploit the vulnerability and allow an unprivileged attacker to access all virtual machines managed by the system.	9.8
CVE-2021-22986	F5 BIG IP y BIG IQ	Combined with other existing vulnerabilities to provide authentication, this flaw allowed full control of the system. Mass scans for vulnerable services were detected during the first half of the year due to the easiness to exploit the problem.	9.8
CVE-2021-3604	Primion-Digitek Secure 8	This access control device allows the attacker to extract user and administrator account information stored in the DBD through a Blind SQL Injection.	9.8
CVE-2021-28111	Dräger X-Dock	These gas detectors store embedded credentials and could be exploited by an attacker for remote code execution.	8.8
CVE-2021-22667	Advantech BB-ESWGP506-2SFP-T	A 0-day has been published about these industrial PoE Switches. They allow telnet access to the administrator password that they store in clear.	8.8
CVE-2021-28797	QNAP Surveillance Station 5.1.5.4.3 and 5.1.5.3.3	An overflow vulnerability in the NAS for video surveillance would allow an attacker to execute arbitrary code.	9.6

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

4.1. Vulnerabilities in figures

In specific numbers of vulnerabilities discovered during this semester, the distribution of published CVEs by risk level (scoring based on CVSSv3), was as follows:

VULNERABILITIES RISKS
Vulnerabilities distribution by risk

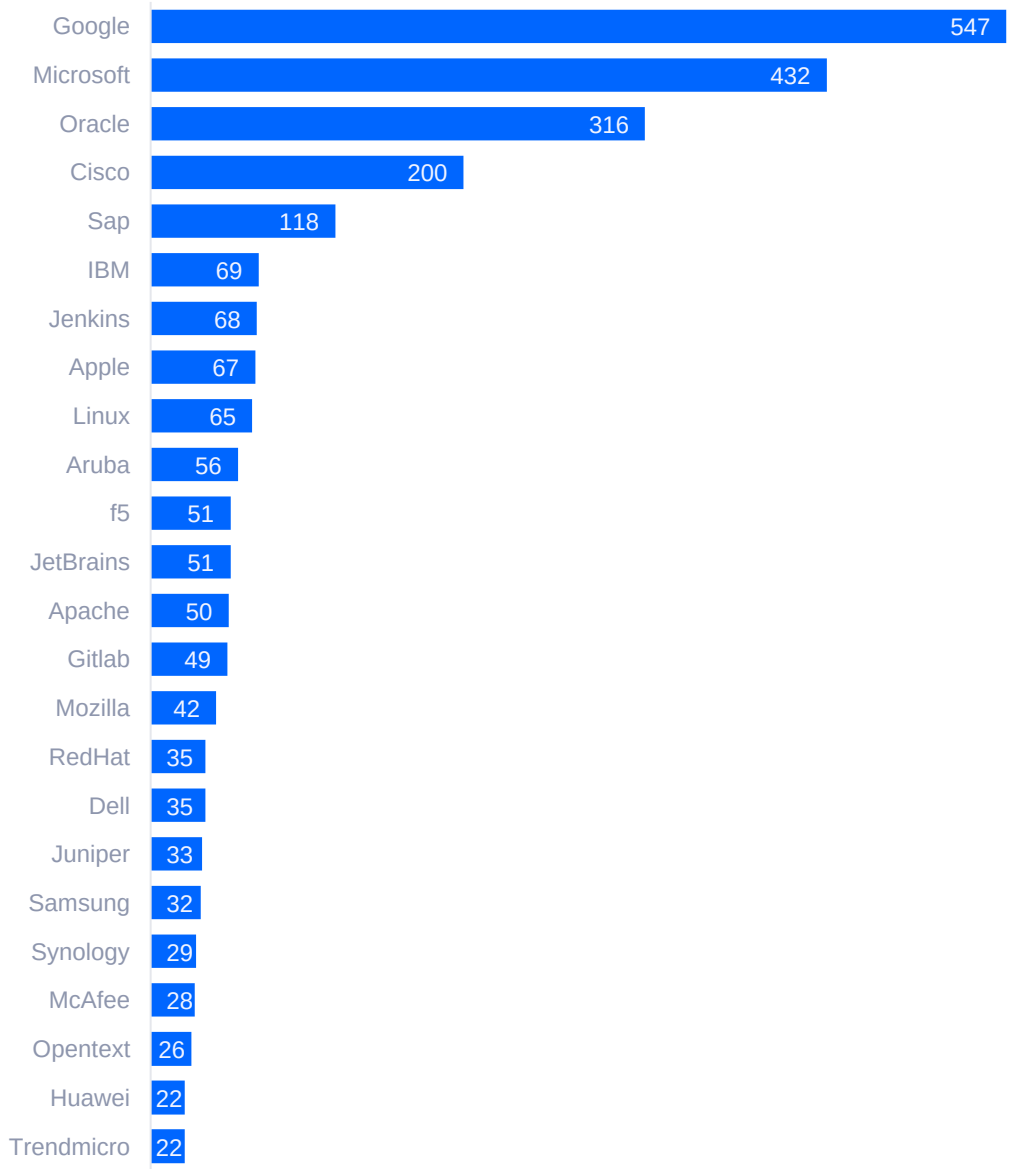


2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

Top 25 companies with the most accumulated CVEs

During this six-month period, Google has led in terms of number of known vulnerabilities. It is followed by Microsoft and Oracle.

Vulnerabilities by manufacturers (TOP 25 manufacturers by accumulated CVE)



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

5. Who is who discovering Microsoft vulnerabilities

¿Who finds most of the vulnerabilities in Microsoft products? What percentage of vulnerabilities are discovered by Microsoft itself, by companies or by vulnerability brokers? How many flaws are discovered without knowing who found them? In this report we have analysed data from the last three and a half years to understand who fixes what in the world of Microsoft products and the severity of these flaws. It also gives us an interesting insight into who actually researches Microsoft products, reports them responsibly, as well as how many vulnerabilities are accredited and how many are not (which could mean that they are discovered by attackers).

Every second Tuesday of the month Microsoft releases its traditional security patches in a single package that updates Windows. That update addresses a number of CVEs or vulnerabilities. But this was not always the case. For many years, bulletins that hid several CVEs, usually grouped by product, were issued.

For many years Microsoft has been incorporating into its secure development policy the auditing of its own code in order to improve its security. We wanted to know how many security flaws exactly does the company itself find in its internal audits, in order to get an idea not only of how much Microsoft itself contributes to improving the security of its products, but also of how much the other usual bug hunters in the industry contribute as well.

5.1. Methodology

We have done something very simple. We have collected and processed all the information of accredited CVEs during the first half of 2021. The source of information has been mainly the following website:

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

These are the identified vulnerabilities, i.e., reported by an identifiable individual or company. In this period, we have analysed 384 reported vulnerabilities. From all of them we have extracted their severity through the official NIST CVSS.

This number does not represent the total number of discovered flaws (more than 440). We understand that most of the uncredited flaws may come from vulnerabilities found in 0-days or other circumstances where the author is not known and has not been reported anonymously. In these cases, Microsoft does not credit anyone in particular. This difference between accredited and "unaccredited" vulnerabilities, which is not the same as anonymous, is reflected in the following chart:

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

Not all vulnerabilities come from accredited sources.
Number of Accredited and Non-Accredited Vulnerabilities from 2016 to 2021 H1.

From the credits, we have extracted the company that discovered the vulnerability. In the case of multiple discoverers,we have counted only the one who was listed first, to simplify the calculations and because we believe that the one who first reported the vulnerability is shown as the lead analyst. While this may be inaccurate, it results in a simpler formula.

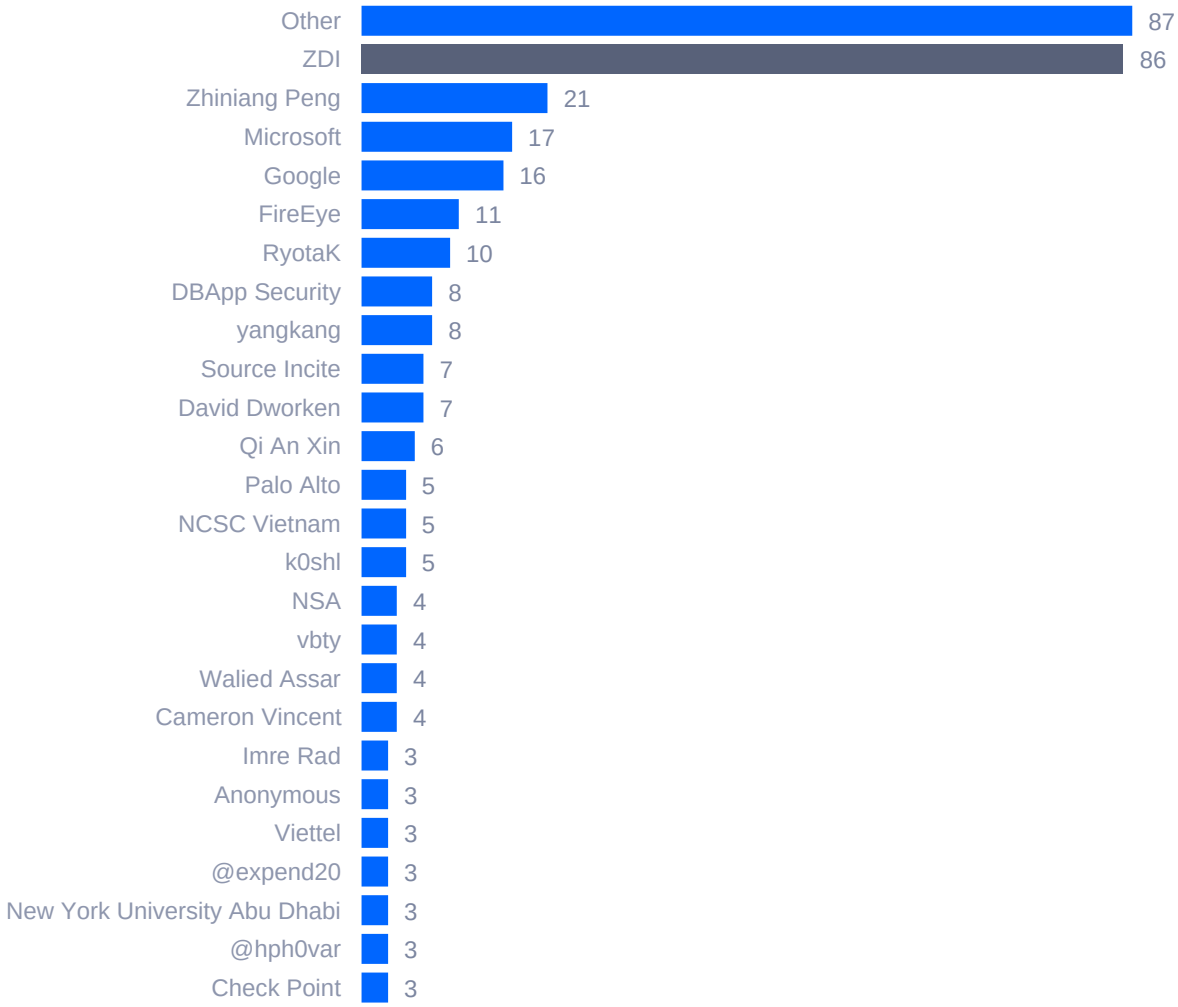
From there, we have performed different calculations to be able to analyse who contributes most and best to improving the security of Microsoft products, in a responsible way.

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

Compared to the previous semester, the data look very different. The long line of "others" leads the list. This means that they are discovered by researchers with less than 5 cumulative failures. The ZDI initiative remains (increasingly) the favourite formula for researchers. This quarter, Zhiniang Peng is again a very relevant actor with 21 bugs discovered.

ZDI IS THE GROUP THAT MOST VULNERABILITIES DISCOVERS IN MICROSOFT PRODUCTS

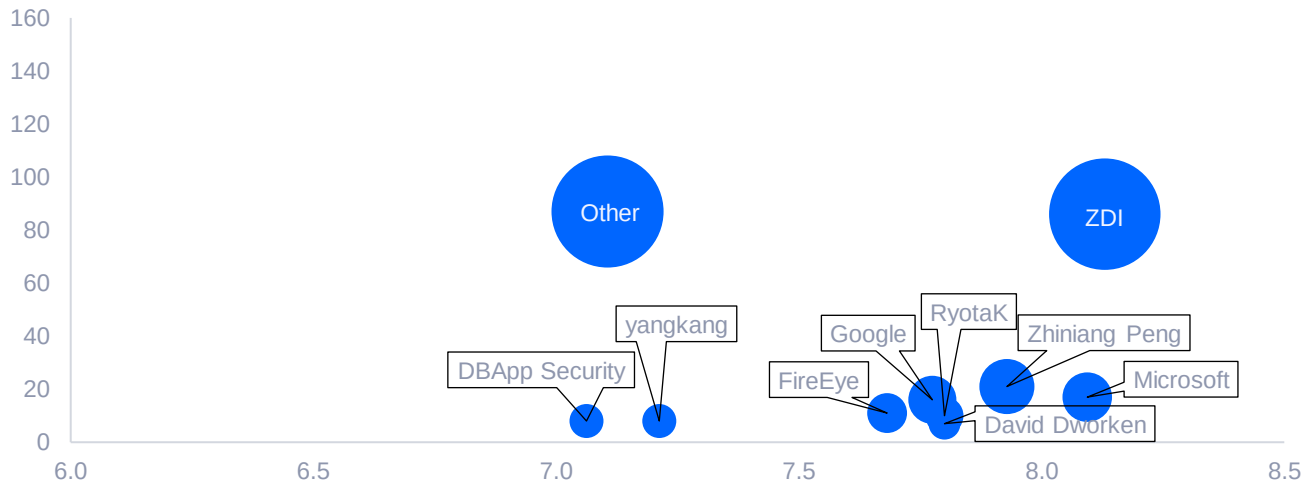
Total number of vulnerabilities per discover in the first half of 2021



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

ZDI ALSO DISCOVERS THE MOST SERIOUS FLAWS

Disttribution of vunerabilities by severity and by discoverer; the size of the blue bubble is proportional to the number of vulnerabilities discovered during 2021 H1.



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

6. APT operations, organised groups and associated malware

We reviewed the activity of the various groups attributed with responsibility for APT operations or notable campaigns.

We warn that the attribution of such operations, as well as the composition, origin and ideology of organised groups, is complex and cannot necessarily be completely reliable.

This is due to the capacity for anonymity and deception inherent in this type of operation, in which actors may use means to manipulate information in such a way as to conceal their true origin and intentions. It is even possible that in certain cases they may act in the modus operandi in order to divert attention or harm other groups.

Significant APT activity detected during the first half of 2021

Pinchy Spider: Lethal bite.

This group, which offers its well-known "REvil" ransomware in a "RaaS" (Ransomware-as-a-Service) model, is backin the limelight because its "service" has recently been used in attacks such as the one against Quanta Computer, one of Apple's official assemblers. It was also used against JBS Food, the world's largest meatpacker.

This is not the first time the spider has bitten. Its previous creation, also in RaaS format, was GandCrab. And that was a big one... GandCrab was detected in 2018 and after a year and a half it left more than one million victims. Injust two months it collected more than $600,000 from around 50,000 victims.

And if all this wasn't enough, according to Flashpoint researchers, the malware that hit the Colonial Pipeline entity,and which put the hydrocarbon supply of the US east coast in check, was based on REvil. Could the Darkside group be an affiliate of REvil? Could it be a spin-off of the spider? What is certain is that their network appears to be quite extensive and difficult to detect.

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

Judgment Panda: Judge, party and panda.

In March, the Finnish intelligence and security service (SUPO) announced that the attacks against the Finnish parliament in autumn 2020 were part of an espionage campaign carried out by this group (also known as APT31) linked to the Chinese government.

While the attribution news is from 2021, the events took place in 2020.

Agrius APT: New in town (or not)

"Agrius" is a new group, detected in 2020, linked to Iran and other nearby countries. Its TTPs include the use of a wiper previously shared by APT-33 and APT-34, two groups also of Iranian origin.

According to one of the groups of researchers who have been tracking their activity since 2020, the highest activity of this group this year coincides precisely with the return of tensions in the Gaza Strip and the launching of missiles between Israel and Hamas (and other groups): at the beginning of May.

Could this be a coincidence?

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

7. OT threat analysis

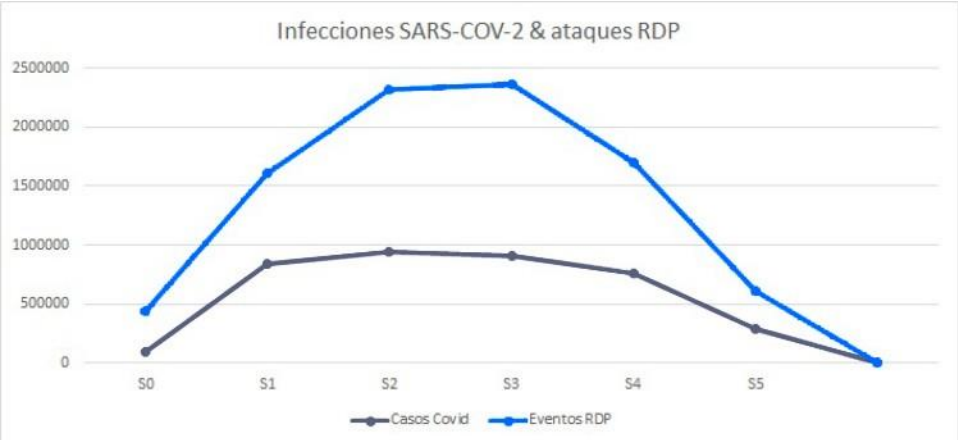
The following information comes from the OT threat capture and analysis system, Aristeo. Aristeo incorporates a network of decoys, made of real industrial hardware, that look and behave like real industrial systems in production, but which at the same time extract all the information about the threats accessing the system. With the information from all the devices deployed in the different decoy nodes, Aristeo applies connections and intelligence to go beyond the data, being able to proactively detect campaigns, targeted or sectorised attacks, 0-day vulnerabilities, etc.

Each node-signature has its own characteristics and reproduces a different process. Therefore, the protocols, devices, productive sectors... change in each one of them. In addition, the nodes are alive, which means that they can undergo alterations in their configuration at the will of the team of researchers working with them, or of the client who has temporary or permanent use of them. This variability may lead to slight discrepancies in the data shown in this section when compared between semesters.

More information: https://aristeo.elevenlabs.tech/

Information analysis

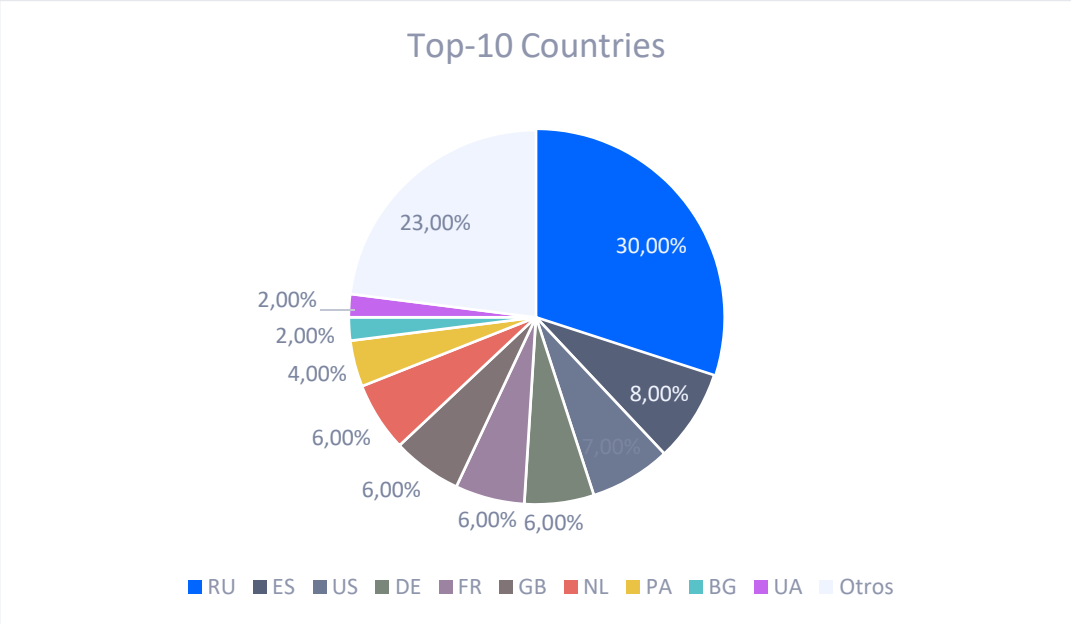
We open this section with one of the hot topics in recent months. Cyber Security and COVID-19. It has always been said that criminals are the ones who know society and its realities, its legislation... best. When we deployed the first Aristeo node, we began to perceive a variation in the data as the pandemic increased or decreased in incidence. We decided to analyse the data to see if our perception was correct. The answer is the graph below, which plots the Covid data versus the RDP event data for the month of January 2021 separated by week. S0 is the last week of December 2020 (to observe the change since the beginning of that wave).



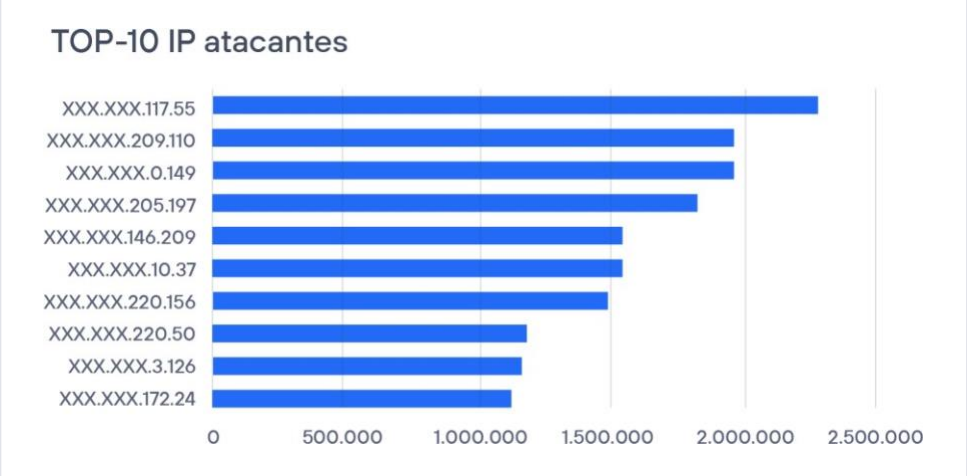
The data on cyberthreats comes entirely from our system, while the data on the SARS-COV-2 threat comes from a number of governments and reputable research organisations. However, given that these data have been aggregated from Spain, France, Germany, Italy and the United Kingdom, and that the updating and traceability of this information is not always the best, the comparison has been a great challenge. In the end, though, the graph does show the trend that we sensed. Attackers increased the number of attacks against devices exposing an RDP (in our case, an engineering bay that controls the industrial process and serves to manage industrial devices on a node).

We turn to the generic statistics of the recorded information. In the first half of 2021, more than 246 million cyber security events were detected. Most of the events were related to more or less sophisticated RDP attacks. The distribution by country is as follows:

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

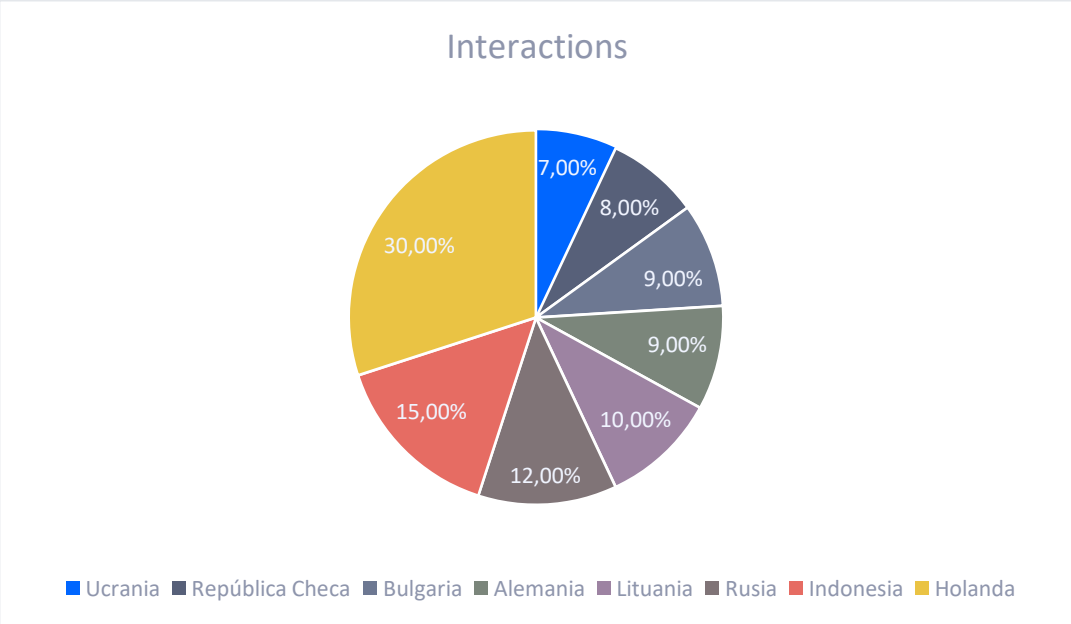


Below, we can see the Top-10 IP addresses with the most interaction with the Aristeo system and their countries of reference.



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

Below, we can see how the IPs with the most activity are distributed. As a curious fact, the IP address with the most interactions apparently corresponds to a governmental environment in one of the countries shown in the graph **(and it is not Russia)**.



2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

8. Useful links

You should not stop at just the top layer of cyber security analysis, the half-yearly reports are cumulative and summarised. In Telefónica TECH's cyber security blog we have much more information and news that may be of interestto you. Here are our most relevant articles in the first half of 2021.

CRIPTOGRAPHY

Plausibly Deniable Encryption or How to Reveal A Key Without Revealing It - Think Big (blogthinkbig.com)

Snitch Cryptography: How to Crack Tamper-Proof Devices - Think Big (blogthinkbig.com)

Functional Cryptography: The Alternative to Homomorphic Encryption for Performing Calculations on Encrypted Data - Think Big (blogthinkbig.com)

A Trillion-Dollar on Offer to the Puzzle Solver - Think Big (blogthinkbig.com)

NFT Fever: The Latest Cryptocurrency Killing It Online - Think Big (blogthinkbig.com)

Unravelling the Quantum Tangle of Cybersecurity: Quantum Computers, Quantum and Post-Quantum Cryptography - Think Big (blogthinkbig.com)

The Future of University Credentials Points Towards Blockchain And Open Badges - Think Big (blogthinkbig.com)

Nobody on The Internet Knows You Are A Dog, Even If You Use TLS Certificates - Think Big (blogthinkbig.com)

26 Reasons Why Chrome Does Not Trust the Spanish CA Camerfirma - Think Big (blogthinkbig.com)

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

MALWARE

Mobile Malware, part of the Generation Z - Think Big (blogthinkbig.com)

Using DIARIO Through FOCA For Malware Analysis - Think Big (blogthinkbig.com)

Fileless Malware: A Growing but Controllable Attack - Think Big (blogthinkbig.com)

And the President Said, "Enough Is Enough". The New Cyber Security Proposals from The White House - Think Big (blogthinkbig.com)

What On Earth Is Going on With Ransomware And Why We Won't Stop It Any Time Soon - Think Big (blogthinkbig.com)

Your MacOS System Is Also A Target for Cybercrime - Protect It! - Think Big (blogthinkbig.com)

ARTIFICIAL INTELLIGENCE

How to Trick Apps That Use Deep Learning for Melanoma Detection - Think Big (blogthinkbig.com)

2021 © Telefónica Cybersecurity & Cloud Tech, S.L.U. All rights reserved.

About Telefónica Tech

Telefónica Tech is a holding company owned by the Telefónica Group. The company offers a wide range oftechnological solutions reaching more than 5.5 million clients in 175 countries.

Telefonica TECH will be able to host other digital businesses in the future, including the B2C segment.

More information

telefonicatech.com

2021 © Telefónica Cybersecurity & Cloud Tech S.L.U. with Telefónica IoT & Big Data Tech S.A. All rights reserved.

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. (“Telefónica Tech”) with Telefónica IoT & Big Data Tech S.A. and/or any other entity within Telefónica Group and/or its licensors. Telefónica Tech and/or any Telefonica Group entity or Telefónica Tech’s licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice.
Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of Telefónica Tech .
This document is intended only to assist the reader in the use of the product or service described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use.
Telefónica Tech shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product or service. The use of the product or service described in this document are regulated in accordance with the terms and conditions accepted by the reader.
Telefónica Tech and its trademarks (or any other trademarks owned by Telefonica Group) are registered service marks.

.