Telefónica Tech

Security Status Report 2022 H1

From mobile security to vulnerability scanning, from breaking news to threat tracking. Understanding the risks in today's landscape.

telefonicatech.com

Índex

EXECUTIVE SUMMARY

The aim 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), adopting a perspective that covers most aspects of the discipline, in order to help the reader, understand the risks of the current landscape.

The first half of 2022 has been characterised by interesting news related, of course, to important vulnerabilities and major attacks. Two of the most relevant flaws have been found within Office, and are related to new ways of executing code in Word or Excel. Manipulation of embedded protocol calls allows code execution outside the context of macros. In January we still had problems with CVE-2021-40444 (MSHTML protocol) and in May with the so-called Follina (MSDT protocol) which again allowed code execution.

This provided food for thought as to whether macros were becoming obsolete as an attack vector in favour of more sophisticated techniques, less detected and with still a long way to go (it is believed that vulnerabilities related to the use of protocols embedded in Office will continue to appear). However, an interesting move by Microsoft has (counter-intuitively) discarded this idea. In January it was announced that, by June 2022, macros would be completely blocked for documents downloaded from the web. And so it was. When opening any of them, a much more striking red message appeared in an attempt to stop users from enabling macros. Yet, just in July, it announced that it would reverse the change. Now the old and dangerous "Enable content" was back. No further explanation was given, so macros as an attack vector had one less stone in its path... until the end of July, when it changed its mind again and blocked them again. Hopefully for good.

As far as major attacks are concerned, it is striking that two major flaws (April and July) have been found in Honda cars this semester. Analysts were able to remotely boot and unlock certain models. This has reopened the debate on cyber security in critical environments where an attack could put passengers' lives at risk.

This semester we are maintaining our specialised section on 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 information needed 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 relevant cyber security news: what is the most relevant thing happening, what is the current landscape? With this report, the reader will have a tool to understand the state of security from different perspectives and will be able to understand its current state and project possible trends in the short term. The information gathered is largely based on the compilation and synthesis of internal data, cross-checked with public information from sources we consider to be of high quality. Here we go!

HIGHLIGHTS FROM THE FIRST HALF OF 2022

The following are the most significant pieces of news that have had the greatest impact during the first half of 2022.

JANUARY

- On 2 February, the German fuel supplier Deutschland GmbH & Co. KG saw its distribution system blocked by an attack on the automated systems for loading supply trucks. The system cannot be operated manually for security reasons, so the company was unable to do anything. This supplier provides fuel to the company with the most refuelling stations in Germany, a total of 2,300, so it had to start using alternative sources of supply. The attack affected two subsidiaries of the parent company, which discovered on 29 January that they had been attacked. This attack spread to several oil terminals, located in Belgium and the Netherlands.

- **PwnKit**: local privilege escalation in PolKit affects Linux distributions. The vulnerability is in PolKit's pkexec component, a SUID-root binary with sudo-like functionality. Present since 2009, it has remained hidden all this time despite being in the default configuration of most Linux distributions: Ubuntu, Debian, Fedora, CentOS. It is easy to exploit, as it is enough to manipulate environment variables to be able to carry out an exploit and it has been found to be actively exploited.

- **EU bug hunt**: The European Commission has initiated funding for a Bug Bounty programme for five open-source applications, including LibreOffice and Mastodon, in January 2022, through the Open-Source Software Office. This move is in line with the European strategy associated with open source.

- Meta, showed the growth of the espionage-for-hire industry beyond Pegasus in a report at the end of December 2021. Meta has banned access to its platform to seven services related to this espionage industry and estimated that they could have affected more than 50,000 users. The evolution of this industry with new players confirmed espionage as a trend in 2022.

FEBRUARY

- Critical vulnerability (CVSS: 10) found in SAP. Both the software company SAP and the US agency CISA issued an alert on Tuesday 8 February for the urgent installation of a patch for the SAP ICM (Internet Communication Manager) component that provides an HTTPS server to all other SAP components that require internet access. A Shodan search shows more than 5000 exposed servers that could be vulnerable.

- Colonial 2.0: The operations of the German oil storage company Oiltanking GmbH Group were heavily affected after a cyber-attack. According to the company, the attack affected IT systems but not industrial systems. Due to the attack the loading and unloading of oil barrels had to switch to the highly inefficient manual mode.

- Many companies are beginning to have robust ransomware protection policies, which has led its creators to innovate their business models, from the initial ransom demand, to double extortion under threat of publishing sensitive information, to the use of DDoS attacks to "erase" them from the internet. The new twist, used by Lockbit, is to invite attackers to provide third-party data that will help cybercriminals break into their networks and in turn lower their "extortion". Lockbit, shortly afterwards, continued to innovate and introduced a bug bounty in its "partner" programme. It will pay those who find bugs in its software or platforms.

- A new attack on a cryptocurrency platform, in this case the victim was Wormhole and the attackers managed to steal around 322 million dollars. Attacks on these platforms are becoming more and more frequent, denoting a lucrative business behind them.

- In February, Toyota was forced to shut down all its factories in Japan due to a cyber-attack on one of its main suppliers. The supplier, Kojima Industries, provides plastic parts to the brand, making it impossible for the 14 plants of the world's largest carmaker to continue operating. It is worth remembering that in the automotive industry, manufacturers do not usually stock components for many days, but save storage costs by receiving the parts they need on an almost daily basis. Toyota stopped making 10,000 vehicles in a single day.

MARCH

- **Dirty Pipe: New privilege escalation in the Linux kernel.** It affects the Linux kernel from version 5.8 onwards and also extends to Android. It is fixed in versions 5.16.11, 5.15.25 and 5.10.102 allows privilege escalation by writing to read-only locked files, exploiting files with SetUID, etc. The splice function, which allows moving data between files, does not initialise the variable where the flags are stored since 2016. 2020 arrived and a new flag PIPE_BUF_FLAG_CAN_MERGE was defined, its function is to indicate that the data of a pipe on a page can be grouped without the need to rewrite the data in memory. This, in combination with the above, created the vulnerability.

- **ContiLeaks:** The Panama Papers of ransomware. After an apparently internal and political disagreement, two years of private messaging from the Conti Group were published. The information reveals very interesting data from an intelligence point of view: for example, aliases used that coincide with those previously seen in other ransomware groups, infrastructure belonging to the famous TrickBot banking trojan, passwords, how the group is organised, and so on.

- **New fuel for the spread of the Muhstik botnet.** A flaw has been found in the Redis database under Debian and Ubuntu, which allows to escape the sandbox by executing LUA code and thus controlling the system. This adds a new form of propagation for this botnet, which has been exploiting the Log4Shell and Confluence vulnerability since December and September last year. Muhstik is responsible for, among other activities, carrying out distributed denial-of-service attacks.

- **The personal information of more than 800,000 New York City students has been compromised.** It stems from a security incident suffered this January by Illuminate Education, a provider of learning platforms widely used in the city. It is now discovered that the attacker gained access to a database that stores student profiles containing gender, racial, identifying information, age or even family financial status information.

- CISA and the FBI issued a threat advisory directly targeting SATCOM, the United States' international satellite communications system. Attached to that advisory, they issued mitigation measures for service providers, and customers, through SATCOM. These entities have also considered that some countries may already be using attacks against third country satellite infrastructure in conjunction with other physical actions of a military nature. It is also important to remember that satellite networks are often shared, so that an attack on satellites in one country has a direct impact on other countries in the vicinity.

APRIL

- **0days everywhere**: In AppleAVD (audio and video decoding library) and the second in Intel's graphics driver. This trend does not only affect Apple, far from it, Chromium, and therefore Edge, Chrome and Opera, have been affected by an insistent campaign of attacks for some time now. Not surprisingly, the engine is now in two of the most widely used browsers, so the profitability of each flaw is multiplied.

- Project Zero, the Google group dedicated to trying to find and disseminate 0-days, has published an interesting report. In the conclusions of their work, we can see that in 2021 they discovered 58 0-days, a very significant record since the beginning of their activity in 2014 (the previous record was in 2015 with 28). We note that almost all of these 0days follow known practices: building on existing exploits and vulnerabilities to develop new and derivative exploits. This is important, because if they use known methods, techniques or procedures, they should be easier to detect and quicker to respond to.

- On 5 April, **Kaiser Permanente**, a healthcare delivery consortium with a large presence in the United States, discovered a theft of medical information on thousands of patients. Although they acted quickly and shut down the access, it is estimated that nearly 70,000 people had been compromised. The entry vector was a login from the account of a user with permissions and access to e-mails containing such information. However, the company did not want to guarantee the extent of the intrusion. The announcement of the leak took place on 3 June.

- **Psychic Signatures:** A cryptographic error in Java in the Elliptic Curve Digital Signature Algorithm (ECDSA). This flaw is a strong candidate for cryptographic (or rather cryptographic implementation) flaw of the year due to its ease of exploitation and the problems it causes. It turns digital file signing into a farce and would even allow malicious downloads to pass for legitimate content. Classic example of refactoring without sufficient impact analysis. In 2020, when Java 15 was released, a check establishing the verification algorithm was omitted when code related to elliptic curves was rewritten from C++ into Java.

- After a long wait, the use of a security.txt file, has become standard as a first step when a company is contacted about a bug related to/affecting its cyber security. The file describes, in a standardised way, what policy the company prefers to follow when someone wants to report a cyber security breach to the company. It has features such as the point of contact, the expiry of the policy, the company's public encryption keys to encrypt the messages to be exchanged, etc. The standard reflects that the file must be located within the /.well-known/ path and not in the root where many companies used to place it.

- The use of the NSO group's Pegasus spying software is discovered in many European and international political bodies, including those of the United Kingdom and Finland. **The European**

Commission decides to rule out its own investigation into the misuse of these technologies, stating that it should be a matter for each member state.

MAY

- Follina: A critical vulnerability in MS Office document processing. A new formula for executing code in Office documents has been detected that does not require the use of macros and perhaps more worryingly, the document may not contain anything malicious, but instead download the payload on the fly. This vulnerability allows an attacker to remotely execute malicious commands by simply opening a Microsoft Office document. The initial examples, for example, show that the attackers used a Word document that fetches HTML from a server that in turn uses the MS-MSDT protocol to load Powershell code.

- Ransomware paralyses Costa Rica: Rodrigo Chaves, the newly appointed president of Costa Rica, had to declare a national state of emergency as one of his first acts of government in order to mitigate and respond to a massive ransomware attack. The attack began in April, with the finance ministry being the first to detect it and report impacts on the tax and customs system.

- Texas InfoLeak: The information of more than 1.8 million people in the US state of Texas was exposed after a security incident at the Texas state insurance department. A configuration error left publicly exposed a part of the application that should have been private from 2019 to January 2022. The exposed information included names, dates of birth, addresses, phone numbers, and perhaps more relevantly, information about workers' injuries and claims to mutual insurance companies.

- Creative disguises for malware. Antivirus typically detects cracking or patching tools as malicious. Users who really want to use these programmes disable the antivirus or create exceptions for them. With the well-known KMSauto, for example, which requires Windows to remain after patching, the user gets used to this antivirus detection. The Lazarus attackers took advantage of this to hide their attack under the KMSAuto directory and appearance. Not that the patch was malicious, but they disguised their KMSAuto attack by inserting a malicious payload into it. The antivirus detected it, but all engines figured out that it happened because it was a patching tool or crack and not because it was actually malware.

- AGCO, a global agricultural equipment manufacturer and distributor, was hit on 5 May by a ransomware attack that blocked its production and management for days. The company had a turnover of $11 billion last year, supplying several brands of tractors and other farm machinery.

JUNE

- The US agency CISA warns that the under-reporting of ransomware incidents affects the agency's protection of US organisations and their ability to retaliate against the criminal groups that lead them. CISA estimates that only about 20-25% of ransomware incidents are reported. A report reveals that in 2021 more than 2,300 similar attacks have been launched against local governments, schools and healthcare providers. A legislative process is being initiated to encourage greater incident reporting, current legislation only covers critical infrastructure, but it could take years for final approval.

- Mozilla enables Total Cookie Protection by default in its latest version of Firefox. The use of cookies by third parties has been the subject of much controversy in recent years, in particular their use for profiling user behaviour. The problem lies in the fact that there is a single container for all cookies from a given domain. Mozilla has eased this problem by creating specific containers for each domain that is visited and only that container is accessible from that domain, thus limiting the ability to collect and analyse cookies. Therefore, if a website inserts a tracking cookie, it will only be accessible by and from that domain, without the possibility of accessing the rest of the cookies.

- The environmental analysis company, Montrose Environmental Group, with offices in 80 countries, reported on 14 June that it suffered a security breach that affected part of its network of laboratories. This has led to delays in part of its analysis. Its subsidiary, Enthalpy Analytical, which operates 11 laboratories doing enthalpy testing, was particularly affected.

- Cloudflare stops the largest volumetric HTTPS DDoS attack to date. Internet infrastructure company Cloudflare claimed to have stopped an attack of more than 26 million requests per second. The botnet used was reportedly no more than 5,000 devices, which is by no means a large number, but it is worth noting that in this attack the use of cloud infrastructure, probably through the hijacking and use of powerful virtual machines rather than more numerous personal or IoT devices, but with less attack capacity, was used to stop the attack.

MOBILE

Apple iOS

Highlights

We started 2022 with iOS 15.2 and just 12 days later the first patch, 15.2.1, was released, fixing a denial-of-service vulnerability in HomeKit. A peculiar patch, released for a single vulnerability that isn't even critical. However, the release of this patch is attributed to functionality flaws in the Messages app and CarPlay.

Not long after, on 26 January, version 15.3 was released, this time with 10 security patches: half of them severe in various components of the mobile operating system, including its kernel.

And now, something important. An urgent patch for Safari's rendering engine, Webkit. A known vulnerability was being exploited in the wild, so the digital patch didn't take long and 15.3.1 was released on 10 February.

A little over a month later, Apple released iOS 15.4, with no less than 43 security patches, more than a dozen corresponding to vulnerabilities that allow arbitrary code execution.

Exactly the same thing happened with 15.4 as with iOS 15.3. Apple was forced to release an emergency patch due to a new bug that was being actively exploited in the AppleAVD component (an audio and video encoder-decoder). A dangerous bug, affecting the operating system kernel, with all the consequences that this entails (installation of rootkits, interception of system calls, etc.).

It is on mid-May when Apple releases version 15.5 with 38 security patches, 18 of them correcting bugs that allowed arbitrary code to be executed.

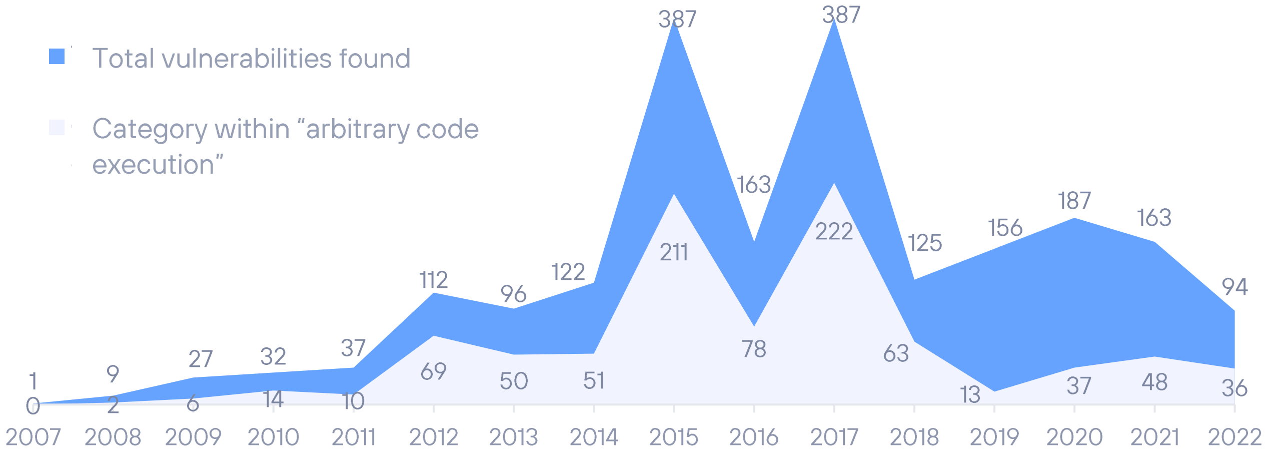
We end the semester with iOS version 15.5 with no minor revisions. It is a quiet period perhaps, relatively speaking, until 15.6 arrives, but that will be in the next half year.

iOS vulnerabilities evolution during the first half of 2022

The first half of 2022 has been closed with 94 patched vulnerabilities, 36 of which are considered high-risk, with the possibility of executing arbitrary code. Some of them affect the kernel of the system itself.

IOS VULNERABILITIES 2022-H1

Evolution of vulnerabilities by year



Fragmentation of versions during the first half of 2022

Traditionally, fragmentation has never been an issue for iOS developers. The advantage of having a consistent platform is undeniable and continues to produce almost unchanged figures every time we review iPhone user adoption of a new version of the operating system.

At the time of closing this report, version fragmentation data was not available from Apple, so the figures below are from StatCounter.

The new version, as usual in Apple's release cycle, reaches full user numbers in the next six months, with a combined share (15.5, 15.4, 15.3) reaching just over 75% of the release pie. Behind iOS 14 and curiously, a survivor (though not unexpected): iOS 12.5.

What's the reason for this? Undoubtedly the iPhone 6 and 6+ which is a version owned by many users and which only supports iOS 12.5. This operating system ceiling on this particular model means that a relatively high percentage of Apple's mobile fleet, a relatively large 2.33%, is still stuck on version 12.5.

All due to the popularity and longevity of a popular and enduring iPhone model. Let's remember that the iPhone 6 was released in 2014, no more and no less than 8 years ago.

FRAGMENTATION ON APPLE 2022-H1	
iOS 15.5	57,43%
iOS 15.4	14,70%
iOS 14.8	4,31%
iOS 15.3	3,53%
iOS 12.5	3,23%
iOS 14.7	2,33%

Android

Highlights

2022 begins with the mature version of Android 12. There is still a long way to go until Android 13. The latest development version was released on 27 June, for developers only.

Android 13 is expected to bring privacy improvements, for example in the selection users can make about which photos and videos apps are allowed to manipulate or a new permission for apps to detect nearby WiFi devices.

As a curiosity, Google released Android 12L on 7 March, with internal API number 32. A refined version of Android 12 for devices with larger screens, specific to users' needs.

In total, 230 patches have been released to fix various vulnerabilities spread across the six bulletins, corresponding to each month of the past six months. Of these 230 patches, 21 fix vulnerabilities that have been rated as critical and could facilitate remote execution of arbitrary code.

Fragmentation on Android systems

The latest release from Statcounter at the time of writing this report shows that the most widely deployed version of Android is Android 11, with a 31.65% share, followed by Android 10 with a 21.92% share.

These are practically the same numbers as in the previous edition.

Android 12 settles for bronze in third place, but with a respectable 17.54%, a higher share than Android 11 in its day under the same circumstances.

Traditionally, the Android ecosystem takes time to propagate new versions, as manufacturers have to adopt them to their own builds, with applications and services inherent to the different brands.

The remaining portion is shared by versions below version 10, where none of them exceed 10% of the market, except for version 9, which still accounts for 11.06% of the market. The oldest Android version with significant market share, 2.64%, is Android Nougat or 7.0, a system that was released in August 2016.

These latest figures are very similar to the previous half-year, as is also the case with new versions. The useful life limit of versions prior to version 10 is approaching and percentages are being scratched, even if they are minimal.

FRAGMENTATION ON ANDROID 2022-H1	
12	17,54%
11	31,65%
10.0	21,92%
9.0 Pie	11,06%
8.0 Oreo	5,90%
7.0 Nougat	2,64%

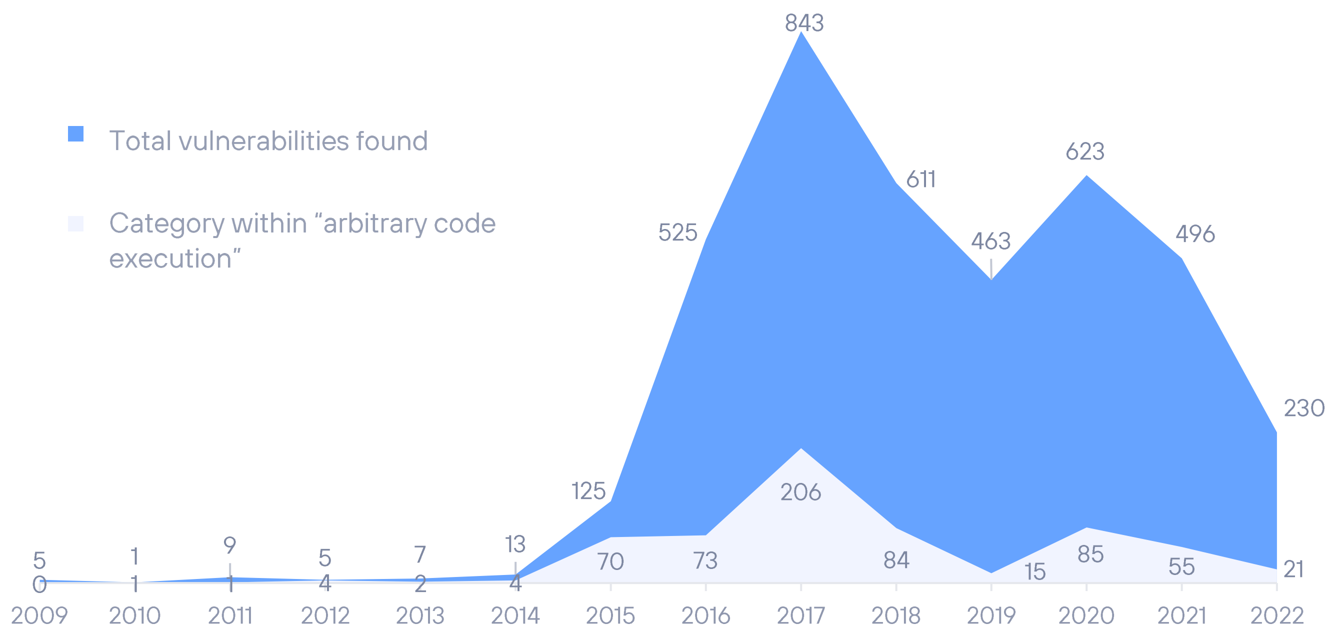
Evolution of Android vulnerabilities during the first half of 2022

Google typically releases a set of security patches every month. So, six bulletins have been published, totalling 230 CVEs or vulnerabilities fixed in that six-month period. 21 of them critical. These figures are very similar to those for the whole of the last six months. The graph shows the accumulated figures up to 2022, first half of the year.

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

ANDROID VULNERABILITIES 2022-H1

Evolution of vulnerabilities by year



SIGNIFICANT VULNERABILITIES

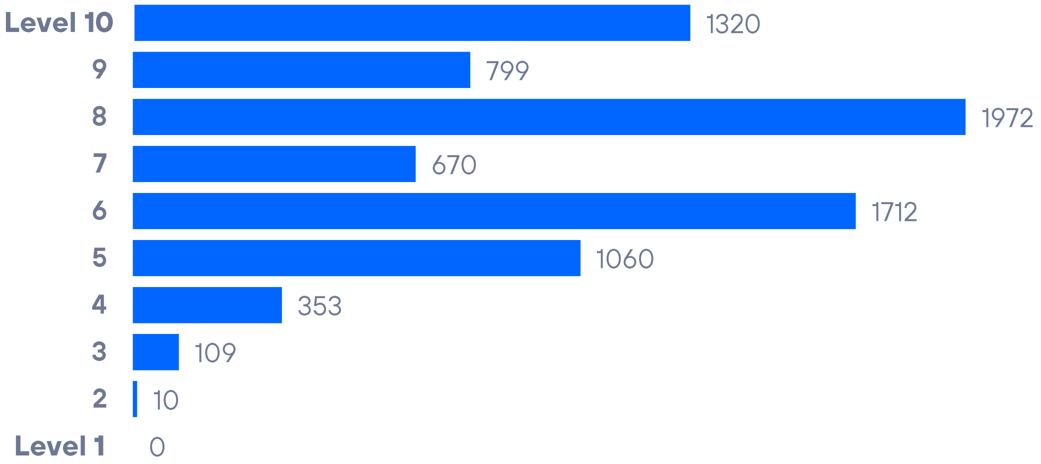
We will comment in the following section on some of the noteworthy vulnerabilities, in our opinion, of the second half of 2021, i.e., those that stand out for their special relevance or dangerousness.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2022-26784	Philips: Miscellaneous	Philips discloses a vulnerability in Windows Cluster Shared Volume (CSV) that allows an attacker to execute a DoS attack on some medical devices, such as the DigiTrak XT Holter Recorder	6.5
CVE-2022-1300	Trumpf: Miscellaneous	TRUMPF has published a critical vulnerability that would allow unauthorised access, even allowing to execute a complete outage.	9.8
CVE-2022-22720	Apache Server 2.4.52	A vulnerability has been detected that would allow "HTTP request smuggling" actions on Mitsubishi air conditioning products.	9.8
CVE-2022-22965	Miscellaneous SCI	Spring4Shell affects several industrial control systems from various vendors, enabling RCE on top of the Java Spring Framework, which is widely used in the Java environment and in certain industrial device applications. Including authentication systems.	9.8
CVE-2022-34265	Django	SQL injection vulnerability in Django's main Django branch	9.8
CVE-2022-1096	Chromium	Type confusion in JavaScript V8 engine	8.8
CVE-2022-0540	Altassian Jira	Authentication bypass sending HTTP requests	9.8

Vulnerabilities in figures

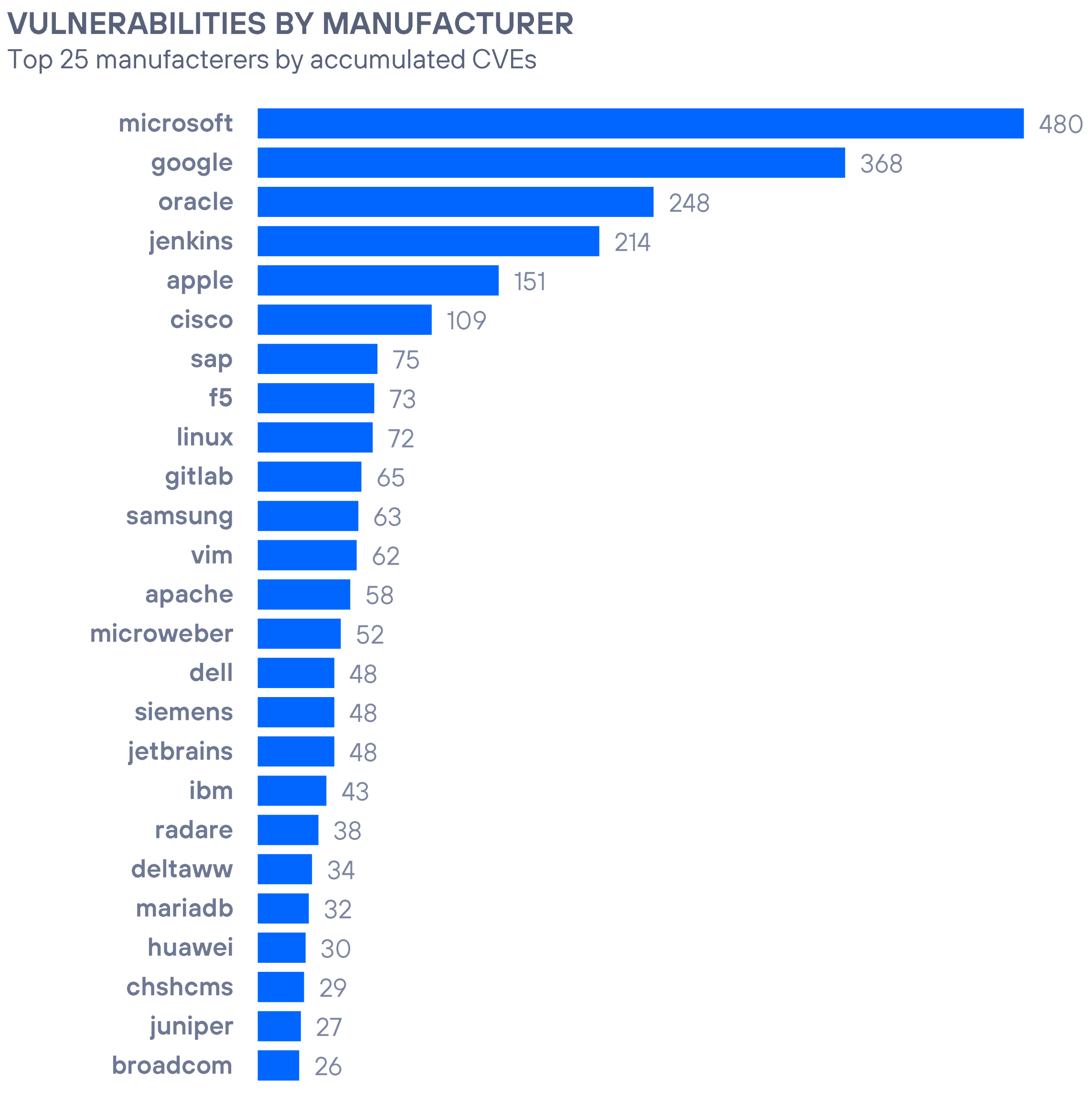
Regarding specific numbers of vulnerabilities discovered, the distribution of published CVEs by risk level (scoring based on CVSSv3), was as follows:

RISK OF VULNERABILITIES
Distribution of vulnerabilities by risk



Top 25 companies with the most accumulated CVEs

In the first half of 2022, Microsoft has led the world in terms of number of known vulnerabilities.



WHO IS WHO. DISCOVERING MICROSOFT VULNERABILITIES

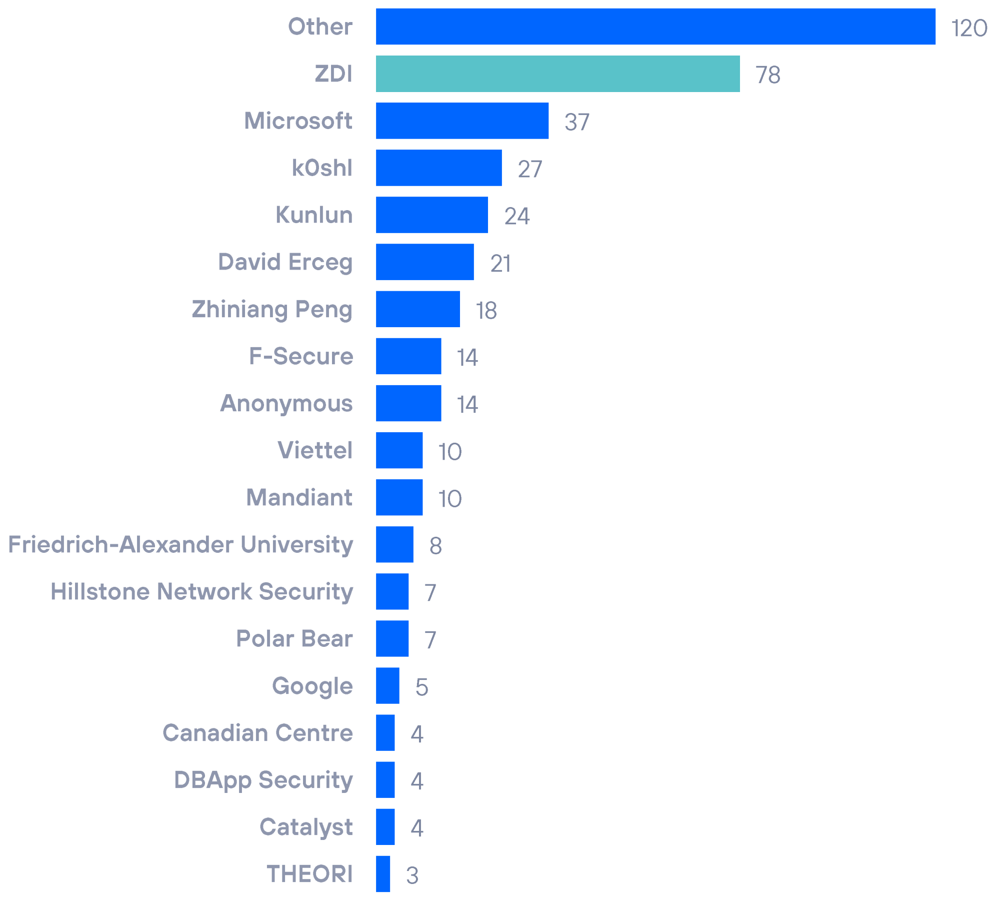
We have extracted the company that discovered the vulnerability from the credits of vulnerabilities discovered in Microsoft systems. In the case of multiple discoverers, we have only counted the one that appeared first, mainly to simplify the calculations and because we understand that the one who reported the vulnerability first is shown as the main analyst. While this may be inaccurate, it results in the simplest 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.

"Other" is leading the list. The ZDI initiative remains (increasingly) the favourite formula for researchers. Google has dropped considerably as a discoverer, whereas in other years it has been a key player. Many independent researchers are also included in this semester.

ZDI IS THE GROUP THAT DISCOVERS MOST VULNERABILITIES IN MICROSOFT PRODUCTS

Total number of vulnerabilities per discoverer in the first half of 2022



APT OPERATIONS, ORGANISED GROUPS AND ASSOCIATED MALWARE

Below we review the activity of the various groups that have been attributed with the authorship of APT operations or notable campaigns.

We note 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 of other groups in order to divert attention or damage the latter.

Significant APT activity, detected during the first half of 2022.

Wicked Panda: As bad as they come

Winnti (another name for this group) is the pure definition of APT: "advanced persistent threat". And especially the "persistent" part.
After a 12-month investigation, the cyber security company "Cybereason" has concluded that this group, of Chinese origin, was responsible for the "Cuckoo Bees" operation.

This operation, so complex that it began in 2019 and was not detected until 2021, would have been able to extract "hundreds of thousands of gigabytes" of information related to the intellectual property of very relevant companies in the energy, defence, biotechnology, pharmaceutical sectors...
The current and future economic impact... is incalculable (literally), although some sources estimate it at billions of dollars.

In 2020, the US Department of Justice identified APT41's structure and some of its members, several of whom are linked to the cyber security company "Chengdu 404 Network Technology". This company is said to be a front company that works in conjunction with another company that sells virtual money for online games, SEA Gamer Mall, where two other members of the group have been identified.

More information: https://www.cybereason.com/blog/operation-cuckoobees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation

Lazarus: They always come back

This group deployed a phishing campaign between December 2021 and mid-January 2022, sending out supposed job offers at a renowned engineering and defence company. Their intention, judging by the recipients of the campaign, was to compromise US military personnel.

Malwarebytes researchers detected that the C&C server was a Github account, making it much more difficult for security systems to discern between legitimate and non-legitimate traffic.

Finally, the researchers also noted that the documents were dated April 2020, which again demonstrates that the professional and business-like behaviour of these groups is the norm.

More information: https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/

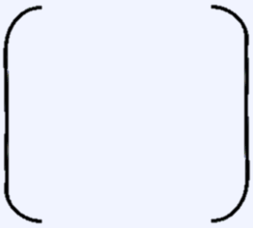
Aoqin Dragon: The king of the South Seas emerges

The South Sea Dragon King, Ao Qin, has been operating undetected since 2013. Recently catalogued by Sentinel Labs researchers, it is assumed to be based in China and has been operating all this time in Southeast Asia and Australia without arousing suspicion. Its targets have been government entities, educational institutions (possibly research-related) and telecommunications companies.

How has this group managed to remain unclassified? Because they have been changing TTPs precisely for that purpose. In security, "cyber" or not, identifying the criminal behind the crime helps to understand the real aspirations and impact of the crime. So far, these cyber-incidents were just isolated elements of no particular interest. Now, however, they are part of a "plan" executed by someone with much deeper interests than expected.

More information: https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

Lapsus$: Live fast, die young...



... and leave a nice corpse. This must have been what the members of this group thought in March of this year.

And what they did was no small feat:

- They stole more than 70,000 credentials of Nvidia employees, as well as the development code for their next flagship graphics card model.
- They published 190GB of code from various Samsung handsets.
- They leaked 37GB of code from various Microsoft services.
- They accessed the source code and data of (300,000) Mercado Libre users.

And all this... in the middle of March and publishing their actions on their Telegram channel (with 48,000 subscribers).

Although the group was catalogued in December 2021, after locating the group in Brazil, following their great successes, the spotlight was put on them and it was discovered that they were a 17-year-old boy living with his mother in Oxford. On the 25th, several members of the team were arrested (and released) in London. However, it is not excluded that there is a small offshoot in Brazil.

This group is another clear demonstration that the hard part is not, unfortunately, doing misdeeds in cyberspace. The difficult thing is to hide. Especially when they are of such dimensions that all eyes are on you.

More information: https://www.xataka.com/seguridad/se-acabo-fiesta-policia-londres-arresta-a-siete-presuntos-lideres-lapsus

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 are extracting all the information about the threats accessing the system. Aristeo uses the information from all the devices deployed in the different node-signposts to apply relations and intelligence to go beyond the data, being able to proactively detect campaigns, targeted or sectorised attacks, 0-day vulnerabilities, etc.

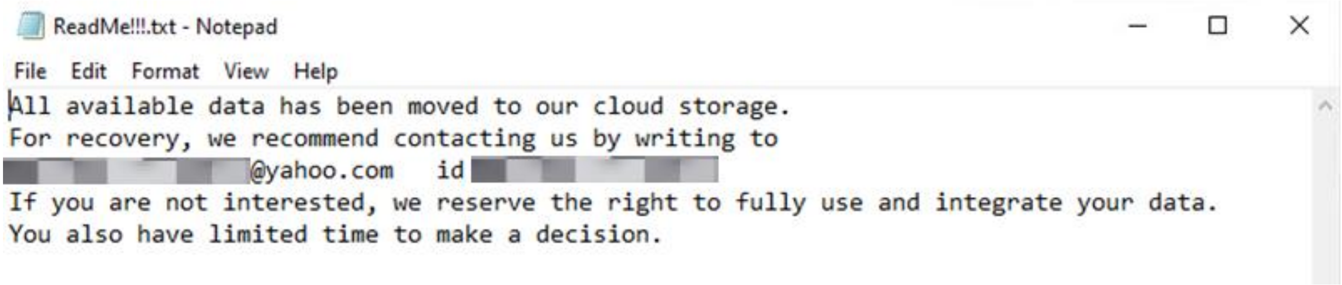
Each node-nested token has its own characteristics and reproduces a different process. Therefore, protocols, devices, productive sectors... change in each of them. Furthermore, the nodes are alive, which means that they can undergo alterations in their configuration to suit the taste of the team of researchers working with them, or 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

Analysis of the information

We are slowly moving away from SARS-COV2 and this semester we bring you a case that reflects the importance of recognising industrial cyber security as a distinct domain from information cyber security. Of course, the bad guys are clear about this and behave differently.

A few weeks ago, we had a guest in our system who showed that he knew where the industrial ecosystem was hurting the most. We found the system down, all values reset (including passwords) and a terse message that said:



```
All available data has been moved to our cloud storage.
For recovery, we recommend contacting us by writing to
[redacted]@yahoo.com  id [redacted]
If you are not interested, we reserve the right to fully use and integrate your data.
You also have limited time to make a decision.
```

Stopped, factory reset, "stolen" process... but what about the star of the party? What about the ramsonware? At no point does it talk about "encrypted information". Why didn't you deploy ransomware? For two reasons:

1. Laziness or inability (probably a mixture of both). Once inside, it would be easy to run some malware on the system, but... what for? This is answered in the next point.
2. The attacker stopped the whole system, reset all the values... stole the information from our process. And that's all he wanted.

The final explanation is simple, if we look at it with perspective and experience. The CIA is to blame. We are referring, obviously, to the three pillars of information security.

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

In an environment where everything is "information", the IT environment, stealing information can only affect confidentiality. Integrity and availability are affected by other manoeuvres (e.g. encryption). Of course, one of the most effective and fastest is to execute ransomware. Recovering the system is complicated, the files with the information that we may have in backup may not be up to date...

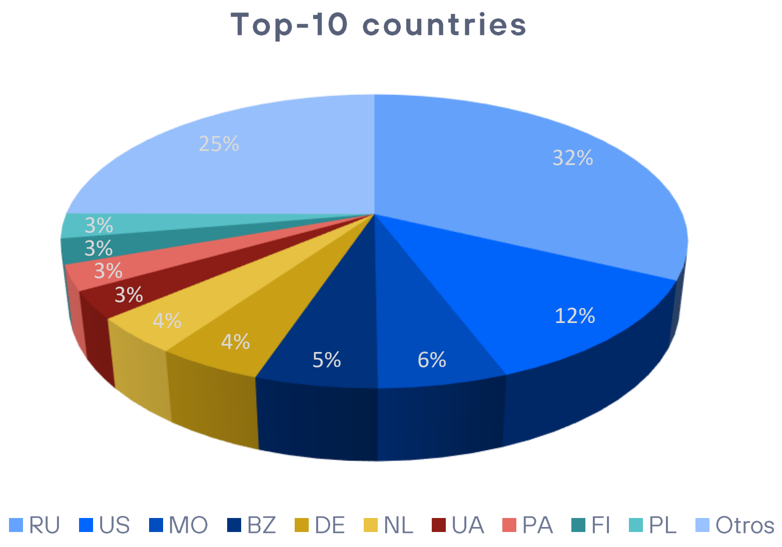
However, in the TO environment, the most effective way to affect the integrity and availability of the industrial environment is simply to delete (or reset) the values that govern the system. Ransomware, on the other hand, only half affects the actual industrial system, because there are devices in the industrial ecosystem where ransomware cannot run. In addition, the values of an industrial system do not usually change, so backup information is usually "up to date". Therefore, recovering information from an industrial system is easier than in a pure information system.

It is important not to lose sight of the business: while in an IT ecosystem, what you pay the most money for is to recover the files with the most up-to-date information (and if you pay, everything is "as before"), in the TO ecosystem what is worth the most money is the process itself, the operation. Stealing the process and selling it to the competition, publishing its details... that is what is most valuable (economically and operationally). Stopping the system, rendering it unusable... is more or less important, but it is damage that is done beforehand and that cannot be undone, so cybercriminals can no longer profit from it. In short, in an OT environment, recovering the information is relatively easy because of its stability (a backup solves it even if it is not extremely recent) and therefore encrypting the information in an OT environment, paradoxically, is not so harmful. The damage is stopping the operation or selling it to a third party, and this cannot be recovered.

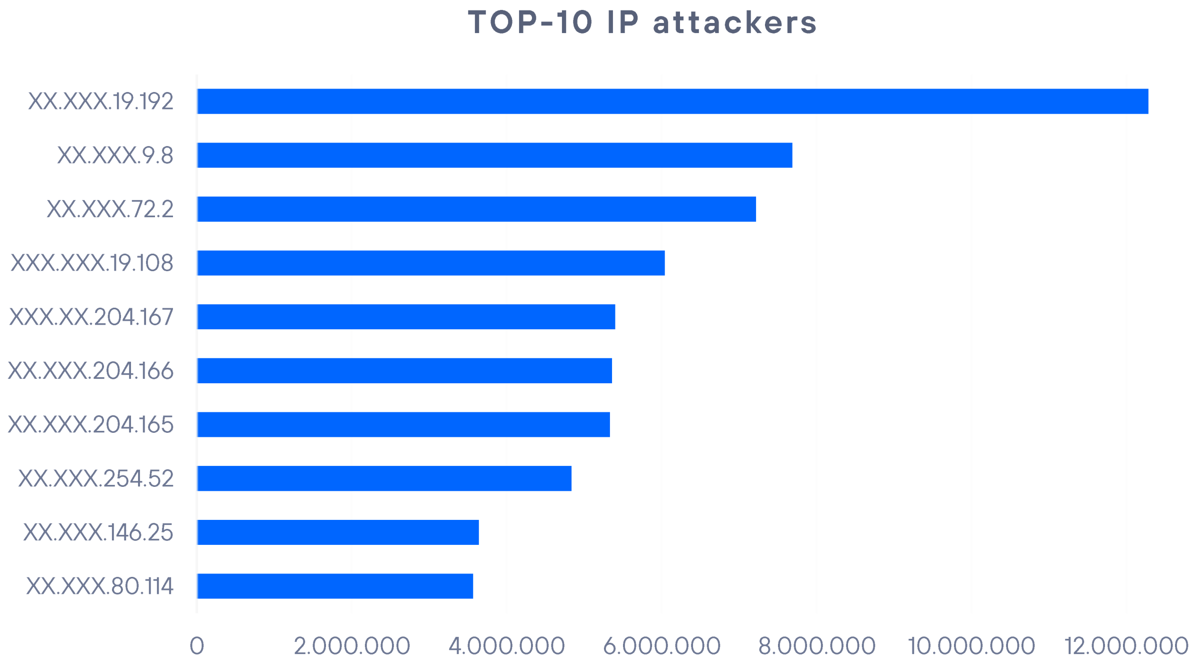
And now we come to the generic statistics of the information recorded. In the first half of 2022, more than 415 million cyber security events were detected. This represents an increase of more than 160% compared to the data recorded in the first half of 2021 and 3% compared to the previous half.

However, the number of events has been decreasing month by month, from a January in which 105 million events were recorded and ending with a June in which just over 50 million were detected.

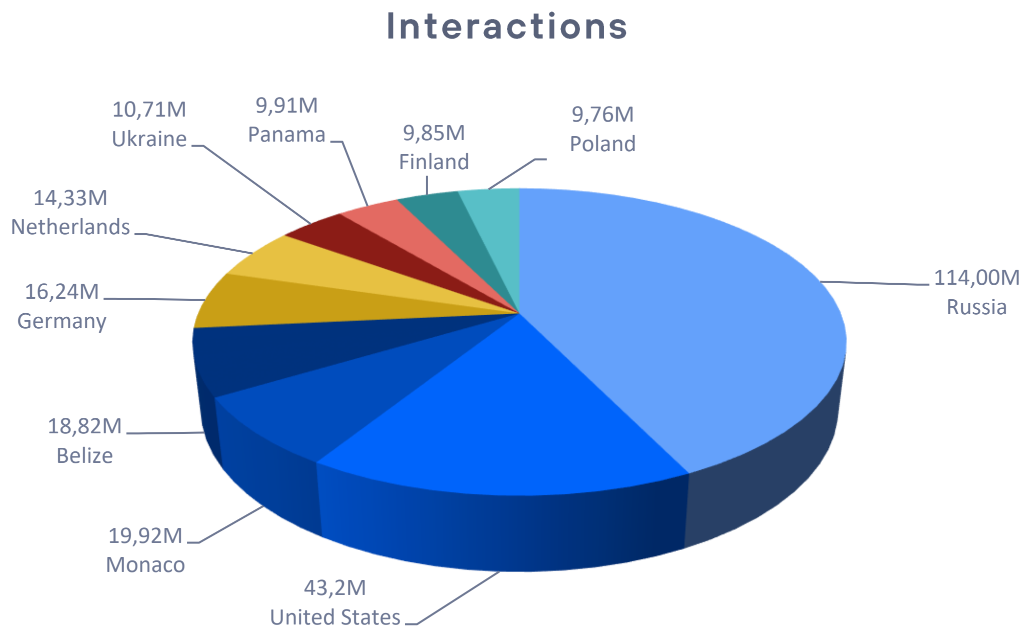
The distribution by country would be as follows:



Now let's take a look at the Top-10 IP addresses with the most interaction with the Aristeo system. Of the TOP-10, 30% belong to the same service provider in an Eastern European country, and it has delegated the administration of these IPs, a /24, to an entity located almost 10,000 km away from that country.



Below, we find the distribution of activity among the countries with the largest presence in our Aristeo. The entry of Belize (a country with less than 400,000 inhabitants) in this exclusive list is particularly striking.


Interactions
10,71M Ukraine
9,91M Panama
9,85M Finland
9,76M Poland
14,33M Netherlands
16,24M Germany
114,00M Russia
18,82M Belize
19,92M Monaco
43,2M United States

RECAP

The number of flaws fixed on both iPhone and Android has fallen for the second half of the year in a row. While in 2017 both operating systems reached a record high in vulnerabilities fixed with several hundred issues, both have dropped considerably in recent years and set records downwards not seen since 2014.

Microsoft, Google and Oracle are the companies with the most bugs fixed, as usual. Jenkins comes in fourth for the first time and enters the ranking strong.

Google detects far fewer vulnerabilities in Microsoft systems, while ZDI remains the broker of choice for discoverers. Some independents continue to find dozens of flaws.

Regarding OT security, the world of ransomware shows that it knows how to economise on resources when it enters one of these systems. It does not encrypt, it only destroys, because that is where the value of the operation lies.

USEFUL LINKS

Don't just stay in 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 interest to you. Here are our most relevant articles.

IDENTIDAD

Cuatro años de la RGPD: cómo mejorar la gestión de la privacidad

El nuevo final de las contraseñas

Digital Identity Wallets contra el fraude en identidad

Web3 y la evolución de la Identidad en Internet

CRIPTOGRAFÍA

Comprendiendo los certificados digitales

Google da un paso para mejorar el ecosistema de Certificate Transparency: No depender de Google

MALWARE

La hipocresía del doble lenguaje entre las bandas de ransomware

The information contained in this document is the property of Telefónica Cyber security & Cloud Tech S.L.U. (hereinafter "Telefónica Tech") and/or any other entity within the Telefónica Group or its licensors.

Telefónica Tech and/or any Telefónica Group company or Telefónica Tech's licensors reserve all intellectual property rights (including any patents or copyrights) arising from or pertaining to this document, including the rights to design, produce, reproduce, use and sell this document, except to the extent that such rights are expressly granted to third parties in writing. The information contained in this document may be modified at any time without prior notice.

Telefónica Tech shall not be liable for any loss or damage arising from the use of the information contained herein.

Telefónica Tech and its brands (as well as any brand belonging to the Telefónica Group) are registered brands. Telefónica Tech and its subsidiaries reserve all rights therein.