Telefónica Tech

Security Status Report 2023 H2

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

telefonicatech.com

Index

EXECUTIVE SUMMARY

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

2023 ends with more than 29,000 documented vulnerabilities (CVEs). The record of 2022 is broken again, with more than 22,000 and 2021 with more than 20,000. Is the software more insecure? Is there more software to attack? Is more research being done to find the flaws? Probably the answer is a combination of all these factors. What is certain is that it is more important than ever to create secure software because more and more activities depend on flaw-free programming so that society can develop in confidence. It is precisely to improve the assessment of these CVEs that a new version of the CVSS metric, version 4, has been released in the last semester, which will allow us to better calibrate the danger of these flaws.

Following this thread, there are also some worrying data. For example, Chrome (and its Chromium engine) continues to be successfully attacked despite being designed with more than reasonable security. This year it has suffered 8 0day vulnerabilities, exploited by attackers. Attackers have been investing in this software as an attack vector for some time now, which shows once again that with motivation, few programs are secure. There are also two other news items of concern that have appeared in the last six months. The Terrapin vulnerability, which allowed man in the middle attacks in the SSH protocol and impacted dozens of implementations in different ways. The problem with this vulnerability was not so much its complexity as the discoverers' final recommendation: the protocol needs a major overhaul. This is not the first time that serious flaws in fundamental protocols have put the entire industry at risk. In the last semester, Marvin, the cryptographic flaw that can never be corrected because it pushed to the limit the exploitation of a known flaw, but which was thought to be impossible to exploit, was unveiled. Researchers fine-tuned the measurements to take advantage of this problem in encryption.

As I mentioned earlier, it's not just attackers: researchers can also improve security if they set their minds to it.

In the second quarter of 2023, a lot of news stands out. We are left to finish with the sad farewell of Kevin Mitnick in July, one of the pioneers of the industry.

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 going on? What is the current landscape? This report will provide the reader with a tool to understand the state of security from different perspectives and will be able to understand its current state and project possible short-term trends. The information gathered is based in large part on the compilation and synthesis of internal data, contrasted with public information from sources we consider to be of quality.

Here we go!

HIGHLIGHTS OF THE SECOND HALF OF 2023

The following are some of the news items that have had the greatest impact during the second half of 2023.

JULY

- Extortion of users by email is common, frequent, and well known. The potential victim receives an email claiming to have compromising images of them (related to the consumption of pornography) and different amounts of money are requested in order not to disseminate them. A joint study by Barracuda Networks and Columbia University analyzed 300,000 mails over a year finding that 80% of the attacks (analyzing the cryptocurrency wallets used) come from only 100 individuals or groups.

- 0-days in 2022: Google's Project Zero team observed that 41 0-day vulnerabilities were exploited in 2022, a considerably lower number than the 69 detected in the previous year. The main trends observed: they look like a move towards less secure platforms than browsers; on Android attackers don't need 0-days because patching is very heterogeneous across vendors; and finally, that almost half of the attacks are variants of older bugs which denotes a root-cause identification problem in patching.

- TeamsPhisher: A RedTeam member from the U.S. Navy published a tool that exploits an unresolved security issue in Microsoft Teams to bypass restrictions on incoming files from users outside a target organization. It was possible to treat an external user as an internal user simply by changing the ID in the POST request of a message.

- Deactivating WhatsApp accounts: A security researcher discovered that the process of deactivating an account on WhatsApp does not have enough identity checks or linking the request to the account to be deactivated, meaning that anyone could actually request the deactivation of any account with a simple email and the associated phone number.

- Kevin Mitnick passes away. Mitnick is considered a reference in the hacking world, in his beginnings he was included in the most wanted people by the FBI and after some time in prison, he worked as an ethical hacker for the rest of his professional career.
-

  The website of the "Bazan" group, operator of Israel's largest oil refinery, was attacked with a DDoS that took it offline. After a while, Bazan enabled access from Israel but filtered access attempts from the rest of the world. Meanwhile, an Iranian hacktivist group called "Cyber Avengers" claimed responsibility for the attack, indicating a major intrusion and leaking on its Telegram channel alleged screenshots of the SCADA systems of several industrial processes. However, the business group's spokesperson called these screenshots “completely made up”.

AUGUT

- **Spyware WebDetetive Dismantled**: Attackers claimed to have penetrated the infrastructure of the Portuguese-language WebDetetive spyware and removed the spyware from victims' devices. They also said they had downloaded data on those who had paid for the spyware and shared that data with the DDoSecrets leak archiving site. WebDetetive was used extensively in Brazil and was used to compromise more than 76,000 Android phones.

- CISA publishes the most exploited flaws of 2022: The most exploited vulnerability of 2022 was a 2018 Fortinet bug. This Fortinet bug (CVE-2018-13379) replaces the Log4Shell exploit, which topped the 2021 list. The other Top Five vulnerabilities are identical to the previous year, including three variants of the ProxyShell exploit affecting Microsoft Exchange servers and a Zoho ManageEngine remote code execution.

- Public vs. private sector: Cloudflare, the well-known internet infrastructure company published its own list of most commonly exploited vulnerabilities in 2022. The top vulnerability according to CISA is not on Cloudflare's list, which shows the different sets of bugs used to attack U.S. government entities compared to Cloudflare's worldwide private sector customer base.

- Following the philosophy of using transparency as a security element, initiated by Google with Certificate Transparency, Google launched Pixel Binary Transparency. Google will use the hash of the firmware installed on Pixel phones and publish all firmware hashes in a public Logs. If someone creates firmware that is not made public through them, the conclusion is that the phone has firmware that has not been entered into the logs and will therefore be suspect.

- Vulnerability in **WinRAR**: RARLAB released a security update for its WinRAR compression tool to fix a vulnerability that could be used to execute malicious code on user devices. The vulnerability could be triggered when performing common tasks such as unzipping a RAR archive crafted by an attacker. The vulnerability was in the WinRAR code responsible for processing RAR4 recovery volumes.

- **NightOwl** joins the already long list of legitimate applications abandoned and reused by attackers to install malware on victims' devices. In this case it is an application for MacOS, something not so usual, which became very popular to automatically switch between light/dark modes in the operating system, but once Apple integrated it natively into the operating system it fell into disuse, something that "TPE.FYI LLC" took advantage of to acquire the application at the end of 2021 with the aim of incorporating its users into a botnet without their consent.
- An APT group uses legitimate software (Cobra DocGuard) to attack companies in Hong Kong. The attackers were able to infect more than 2,000 computers with a backdoor using a downloader signed with a legitimate Microsoft certificate through a malicious update of the software, which was created for encryption and decryption tasks. However, malicious activity has only been observed on just over 100 computers, implying that these are targeted attacks.

SEPTEMBER

- **BlastPass**: Apple released an urgent patch for all its operating systems that fixed a critical issue. It is about two CVEs in particular, reported by the Citizen Lab organization following an investigation and forensic analysis on a victim's phone, in which they found traces of an infection and components related to the NSO Group and its Pegasus spyware. The exploit does not require user interaction, hence the criticality, the attacker could simply send via iMessage, a message containing a Passkit formatted attachment with images carefully crafted to trigger the attack.

- **BEC (business email compromise) scams, although technically not a major innovation, are still more than profitable**. In the USA, a Nigerian citizen pleaded guilty to attempting to swindle $6 million by this method. Of this, he succeeded in obtaining just over one million, which is a fairly high "success" rate. Regarding the BEC scam, Microsoft published an analysis showing that an attacker requires only two hours to execute the entire scam, from initial access to launching and deleting the scam email.

- 38TB of private information exposed by a misconfiguration: Microsoft's AI research team, in publishing an open-source training dataset on GitHub, accidentally exposed an additional 38 terabytes of private data, including a disk backup of two employees' computers. This copy contained private keys, passwords and internal Microsoft Teams messages. The researchers shared their files using an Azure feature called SAS tokens, but incorrectly configured the link to share the entire storage account, which included another 38TB of private files.

- Attacks disguised as Dependabot contributions: A cybercriminal exploited developers' reliance on Github dependency bot contributions to inject malicious code into their projects. Detected by Checmarx, the campaign has been running since July and has impacted hundreds of repositories. If project owners approve the contributions, the malicious code collects the victim project's secrets and secretly inserts an infostealer into the project.

- Cyber security market: Networking and cyber security giant Cisco acquires SIEM provider Splunk for $28 billion. Cisco plans to merge Splunk's threat detection and response capabilities with its threat prediction and prevention services to boost its cyber security offering.

- LastPass stings: Several security researchers believe that attackers who hit LastPass security last year are now cracking stolen password vaults, retrieving seed passphrases from cryptocurrency wallets, and stealing money from cryptocurrency accounts. It is estimated that the attackers have stolen more than $35 million in crypto assets from more than 150 victims. One of the largest thefts identified is a multi-million-dollar heist from an employee of blockchain tracking company Chainalysis.

- The CISA, FBI, and CNMF issued a security advisory detailing that a vulnerability in remote assistance application Zoho ServiceDesk Plus is being used to establish persistent access on infected devices and execute lateral network movements. This vulnerability, along with others related to Fortinet firewalls, allowed access to some companies in the aviation sector. These agencies reported that the intrusion could have taken place in January 2023 and, due to its dangerousness, issued this warning.

OCTOBER

- **HackerOne Anniversary**: Hackerone turned 10 years old and unveils some accumulated figures, as a reflection of a business, that of research and disclosure of vulnerabilities in a responsible way, which is in great shape and also helps to know the cybersecurity status of many products at different levels. It has doled out $300 million in such bounties in 10 years. A single researcher has earned $4 million and 30 of them more than $1 million. The median reward value is $500 this year. For critical bugs, $3,700 on average.

- Massive exploitation of vulnerability in Atlasian Confluence: The American cybersecurity agency (CISA) together with the FBI and other institutions jointly issued a security advisory on the widespread exploitation of the 0-day vulnerability CVE-2023-22515, CVSS of 9.8, as of September 14. The vulnerability affects Atlassian Confluence Data Center and Server versions 8.0.0.0 to 8.5.1 and allows privilege escalation, creation of unauthorized administrator accounts and changing critical server configurations.

- Cyber security regulation: Article 11 of the European Union's proposed Cyber Resilience Regulation (CRA) receives some pushback from the cybersecurity industry. A group of more than 50 technology experts and organizations have signed an open letter calling on the European Union to reconsider the article. The article focuses on the obligation for manufacturers to report any actively exploited vulnerabilities to competent national authorities within 24 hours of becoming aware of them. The signatories of the open letter argue that Article 11 of the CRA greatly expands the number of organizations that will have immediate knowledge of actively exploited vulnerabilities, which, in turn, increases the risks to manufacturers, their customers and the general public.

- VBScript End of Life: Microsoft announced this October that it would remove VBScript from future versions of Windows, although it will be available as an "On-Demand Feature" if needed. VBScript has been part of the Windows operating system since 1998 and was a popular tool among malware developers.

- The Spanish national police dismantled a criminal organization dedicated to computer scams, which had collected almost three million euros by carrying out various types of scams: smishing, phishing and vishing and which had personal data of more than 4 million people. The police have arrested 34 members of the criminal group and reported that the leaders of the scheme used false documentation, making use of spoofing techniques to hide their identity and invested their profits in cryptoassets.

- Ubiquiti releases a security update to fix a major vulnerability in UniFi, the management software for controlling the company's wireless gateways, switches, and access points. Identified as CVE-2023-41721, the vulnerability allows threat actors to access device configuration data and has received a severity rating of 10/10.

- Okta data leak: An attacker compromised the account of a support employee at Okta, a leading global identity and authentication provider, and gained access to some customer data. The attacker had access to the support network for more than two weeks, from Oct. 2 to Oct. 18. Okta indicates that the intruder only stole HTTP archive files that the company requires customers to upload to its customer support portal for debugging.

- Mass Exploitation of Vulnerabilities in Cisco IOS XE: CISA and its partners provide guidance for action upon detection of a mass exploitation of vulnerabilities in Cisco IOS XE Web UI (CVE-2023-20198 and CVE-2023-20273 affecting the Cisco Internetwork Operating System (IOS) XE Software Web User Interface. An unauthenticated remote actor could exploit these vulnerabilities to take control of an affected system, allowing them to create a privileged account that grants full control over the device.

- Securelist publishes an analysis of a series of attacks against Russian companies in industrial and government sectors. Among other techniques and tools, the campaign uses a backdoor programmed in Go that has shown improvements over time as the security firm detected other targets under attack. One of the latest improvements detected prior to publication was the ability to steal passwords from various browsers.

NOVEMBER

- The ransomware industry is not only lucrative, but perfectly oiled to become more and more so. The FBI offered a specific piece of data at the end of 2022: Hive, one of the most active ransomware organizations, earned $100 million from 1300 victims from June 2021 to November 2022. An average of about $77,000 per victim. 81 victims per day every day.

- Apple's Find My to steal passwords: Positive Security has found that Apple's Find My location network can be used by attackers to leak information captured via keyloggers installed on keyboards. Analysts have even published their implementation on GitHub, called Send My, which others can leverage to upload arbitrary data to Apple's Find My network and retrieve it from any Internet-connected device anywhere in the world.

- Open letter eIDAS regulation: More than 300 cyber security experts, researchers and NGOs have signed an open letter calling on the European Union to abandon its new eIDAS (Electronic Identification, Authentication and Trust Services) regulations. The experts argue that the new articles would force web browsers to automatically trust certificate authorities and cryptographic keys imposed by EU governments, opening the door to mass surveillance and interception of encrypted web traffic across the Union. Signatories include Mozilla, the EFF, the Linux Foundation, Cloudflare, Fastly, etc.

- MOVEit, a file transfer platform of Progress Software Corporation, was attacked by a ransomware operation called Cl0p. The impact of the attack has affected more than 2000 organizations and 75 million individuals as of November 2023 according to information shared by EMSISoft.

- Malaysian authorities have dismantled phishing-as-a-service provider BulletProftLink in November and arrested eight suspects, including the platform's main administrator. Launched in 2015, BulletProftLink grew to become one of the largest known on-demand phishing platforms to date, offering for a monthly fee of $2,000 hosting for phishing sites, access to phishing kits, email templates and tutorials.

- CitrixBleed: CitrixBleed is a vulnerability affecting Citrix ADC and Gateway on premises products. It is characterized by allowing an attacker to gain unauthorized access to sensitive data, such as user session tokens. The vulnerability allows unauthorized access to memory through a simple, specially crafted request. A very dangerous feature of this vulnerability is that the manipulated attack leaves no logs in the logs, which makes it very difficult to detect. Several security companies have identified massive attempts to exploit this vulnerability with more than 100 unique IPs probing the network for unpatched systems and moving up.

- ownCloud vulnerability exploit: Several threat actors scanned the internet during November for ownCloud file sharing servers to exploit a recently patched vulnerability. Identified as CVE-2023-49103, this security flaw has a severity rating of 10 out of 10 and can be used to leak administrator passwords and mail server credentials from ownCloud installations. Exploitation has been independently detected and confirmed by GreyNoise, SANS ISC and Shadowserver Foundation.

According to the latter, there are more than 11,000 ownCloud servers currently connected to the Internet.

- A water treatment facility in Pennsylvania was attacked by a group linked to Iran: Cyber Av3ngers. This group managed to gain access to the facility's PLCs that regulated the water pressure. As soon as the company became aware of the intrusion, they overrode the remote operation and switched to manual operation, so that the attackers were no longer able to continue their operations.

DECEMBER

- End default passwords: The Cybersecurity Agency CISA issued an advisory requesting technology manufacturer to stop using default passwords on their devices and software. Instead of using a single default password, it recommends manufacturers provide unique, tailored configuration passwords for each product. It also suggests implementing temporary passwords that are disabled after initial configuration, as well as promoting the use of MFA authentication.

- Part of the BlackCat ransomware infrastructure disarmed: An FBI operation, together with authorities in Spain and Germany, among others, reportedly managed to shut down the BlackCat ransomware infrastructure. According to authorities, the FBI remained undercover for months while they extracted the public and private decryption keys that helped 500 victims and also managed to seize the ransomware's website with the aim of shutting it down.

- LeaksMas, massive data exposure on the Dark Web: Resecurity detected multiple actors on the Dark Web releasing more than 50 million records containing personally identifiable information (PII) of consumers around the world on Christmas Eve. This massive data exfiltration, released under the label "Free Leaksmas," could result in account takeovers, corporate email breaches, identity theft and significant financial damage. Moreover, it was not only limited to the United States, but also affected companies and organizations from different sectors in countries such as France, Peru, Vietnam, Russia, the Philippines, Australia, India, South Africa, and others.

- Major operation to arrest drug mules used by cybercrime groups: Europol, Interpol and law enforcement agencies from 26 countries have arrested 1,103 "financial mules" in one of the largest actions against money laundering operations. In addition, they identified nearly 11,000 mules and their recruiters. More than 2,800 banks and financial institutions assisted law enforcement in the tracking.

- 23andme: After the attack received by the well-known genetic analysis company 23AndMe, and after several disturbing movements, they have finally acknowledged that an attack had affected almost 50% of their users (6.9 million). In the immediate aftermath of the attack, they downplayed the severity of the attack and modified the terms and conditions to impose mediation for the resolution of legal disputes with their users. The company began moving in the right direction and is enabling two-factor authentication (2FA) for all of its customer accounts in an effort to protect its users from brute force attacks and account hijacking.

- CISA suggested that the paradigm of rapid patching for rapid incident remediation was a failed model. In December alone, there were media reports of: Russian state-sponsored actors actively exploiting an Outlook bug fixed in March 2023; Citrix Netscaler vulnerabilities being used in ransomware attacks despite a patch being issued in October; and CISA itself recently warned about the exploitation of an Adobe ColdFusion bug that was fixed in March.

- Spanish police arrested one of the leaders of the cybercriminal group "Kelvin Security". This group, active since 2013, is linked to attacks on critical infrastructure and government institutions. Their motivation was to obtain information to sell it on specialized forums. They are also suspected to be the architects of the ARES platform, dedicated to the buying and selling of stolen databases. The detainee, in particular, was in charge of money laundering.

- Forescout researchers revealed 21 vulnerabilities in "Sierra Wireless Airlink" OT/IoT routers. Some of these vulnerabilities are easy to exploit and can have disastrous effects on industrial processes: stealing credentials, hijacking control of a router by injecting malicious code, generating persistence on the device and using it as an initial access point to critical networks... Researchers found more than 86,000 such routers exposed. These devices were related to sectors such as energy distribution, a national healthcare system, waste management, retail, and vehicle tracking.

MOBILE

Apple iOS

iOS 17 and the new security and privacy features.

The second half of the year undoubtedly brings us the most important news of the year regarding Apple's mobile terminals: the renewal of its operating system.

This year it was the seventeenth iteration, iOS 17, which, as usual, was made public in September. Let's take a closer look at the improvements in the security and privacy chapter.

- Los Messages with one-time use codes will be automatically deleted. Now, when a single-use code (characteristic as a second authentication factor) is received and used, it will be deleted once we make use of it, something that is detected since the operating system itself offers to complete the form with this code. Once it has completed its task, it will be discarded. This is more functional than a security measure, since if the server implementation is correct, single-use codes, as they are called, should not be reused.

- Mute non-contact calls. It is possible to select that FaceTime calls from non-contacts do not ring the device.

- Safari. Private browsing (incognito mode) can be blocked if not in use, preventing anyone with access to the browser from viewing content loaded in incognito mode. Re-access will require user authentication.
  Browsing has been improved in the sense of privacy by enhancing the blocking of trackers and preserving our digital footprint.
  Safari in private browsing will detect links with tracking information and filter that content from the URL. This allows you to bypass this tracking technique that tries to counteract the "non-acceptance" of third-party cookies.
  As with SMS messages with one-time use codes, if they arrive via the Mail (email) application and we use them in Safari, the email will be automatically deleted.
  Safari now allows you to share passwords with a group of users. We create the group; assign passwords and they will be synchronized between them.

- Sensitive content. Specially designed and useful for children. It is now possible to tell the system to blur images and videos with explicit content.
  The photo selector that applications use when they want to access the photo gallery has been improved. We can now select a group of photos instead of a folder or the entire gallery.

- Calendar now has a new permission that only allows applications to write to calendars, preventing them from also having read access and obtaining calendar information.
  Lockdown mode has been improved in the aspects of networking, media file handling and sandboxing.

- AppleID. Some functionality of this service has been extended. It is currently possible to authenticate to another Apple device by simply bringing your phone close to it.
  In addition, during authentication on a service where we use Apple ID as a mechanism, we can use both email and phone number. Obviously, hiding this information from the third party.

Vulnerabilities and released versions

We review the security updates of the iOS operating system that the second half of 2023 has brought us.

At the beginning of the first half of the year, iOS 15 and 16, in their respective revisions, released urgent patches: 15.7.7 and 16.5.1. They also do so through Apple's rapid response mechanism. The bugs fixed are critical and are being actively exploited. This is a trend that will be repeated throughout the remainder of the year.

15.7.8 and 16.6.1 are released on September 7 due to a vulnerability that is being actively exploited, "BLASTPASS", to infect cell phones of persons of interest. Exploitation occurs via message without the need for user interaction.

Days later, on September 18, the new major update of iOS, version 17, was released, with the new security features we have discussed.

This version also comes with more than 60 security patches, many of them related to arbitrary code execution.

A new set of patches must be urgently released on September 21 to mitigate infection by the "Predator" malware that has been observed to be actively exploiting the now-fixed vulnerabilities.

The newly released version 17 sees its first three patches with 17.0.1, while for version 16 we move up to 16.7 with almost a score of fixes including those mentioned above.

On the same September 21 iOS 17.0.2 is released but it does not contain any security fixes, it is a functionality fix affecting iPhone 15 handsets.

An urgent security patch is released again on October 4: iOS 16.7.1 and 17.0.3 are released. We've had a half-year of scares with 0-day vulnerabilities being exploited in high-level operations. These releases fix a remote execution of arbitrary code and, once inside the system, an escalation of privileges affecting the kernel.

October 25. iOS 15 receives its latest update. Version 15.8 containing an important security patch, a 0-day exploit related to the malware campaign known for the "Triangulation" trojan.

On the same day the usual set of security patches was also released with more than twenty bugs fixed in the versions: iOS 16.7.2 and 17.1.

iOS 17.1.1 was released on November 7 with no security fixes.

November was not going end with no surprise and, once again, a dangerous and actively exploited vulnerability. iOS 17.1.2 was released. Another new 0-day for the first half of the year. Interestingly, they would not release for iOS 16 until December 11, with iOS 16.7.3 and an additional set of patches.

Speaking of December 11, a new set of security patches appeared for iOS 17. Version 17.2 was released with nearly twenty fixes.

On December 19, iOS 17.2.1 was released with no security fixes, closing out a 2023 that was characterized by a large number of actively exploited vulnerabilities.

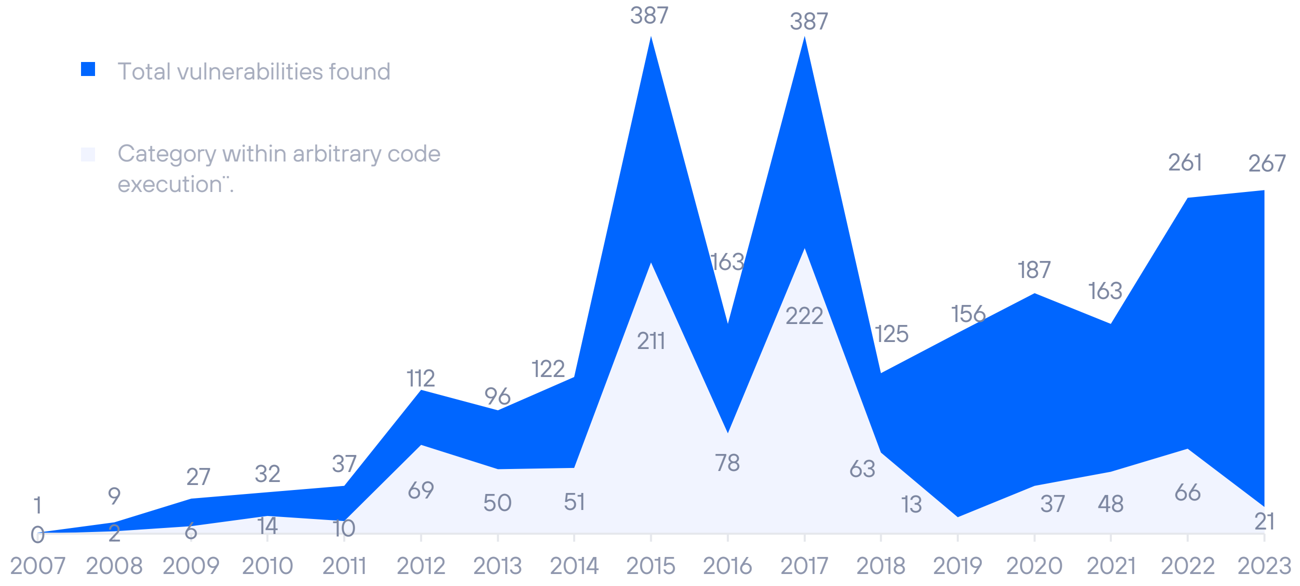
Evolution of vulnerabilities in iOS in the second half of 2023

The second half of 2023 closed with 154 unique vulnerabilities patched, around a dozen considered high-risk, with the possibility of executing arbitrary code. Many of them affecting the operating system kernel itself and, as we have seen, involved in very specific attacks or as part of APT infection campaigns.

In short, 2023 closed with 267 unique vulnerabilities fixed, slightly more than the previous year, which closed with 261.

VULNERABILITIES IN IOS 2023-H2

Evolution of vulnerabilities per year



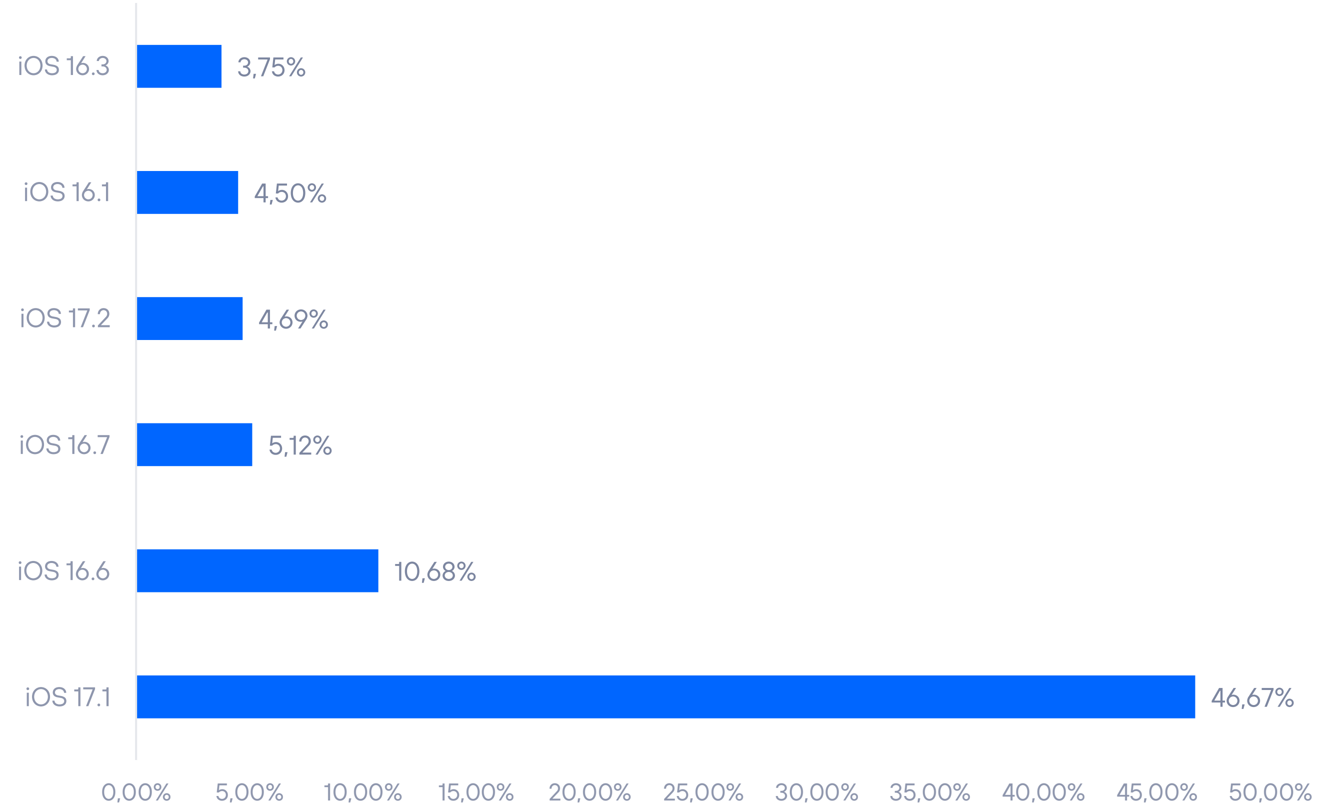
Fragmentation of versions during the second half of 2023

Fragmentation, traditionally, has never been an issue for iOS developers. The advantage of having a homogeneous platform is undisputed and continues to yield near-identical numbers every time we review iPhone user adoption of a new version of the operating system.

No version fragmentation data was available from Apple at the time of going to press, so the figures below are from StatCounter.

As usual in Apple's version cycle, iOS 15 has practically disappeared, with versions 16 and 17 being the most popular. Only the various sub-branches persist, from handsets whose users have not yet upgraded to higher branch versions.

FRAGMENTATION IN APPLE 2023-H2



Apple Transparency Report

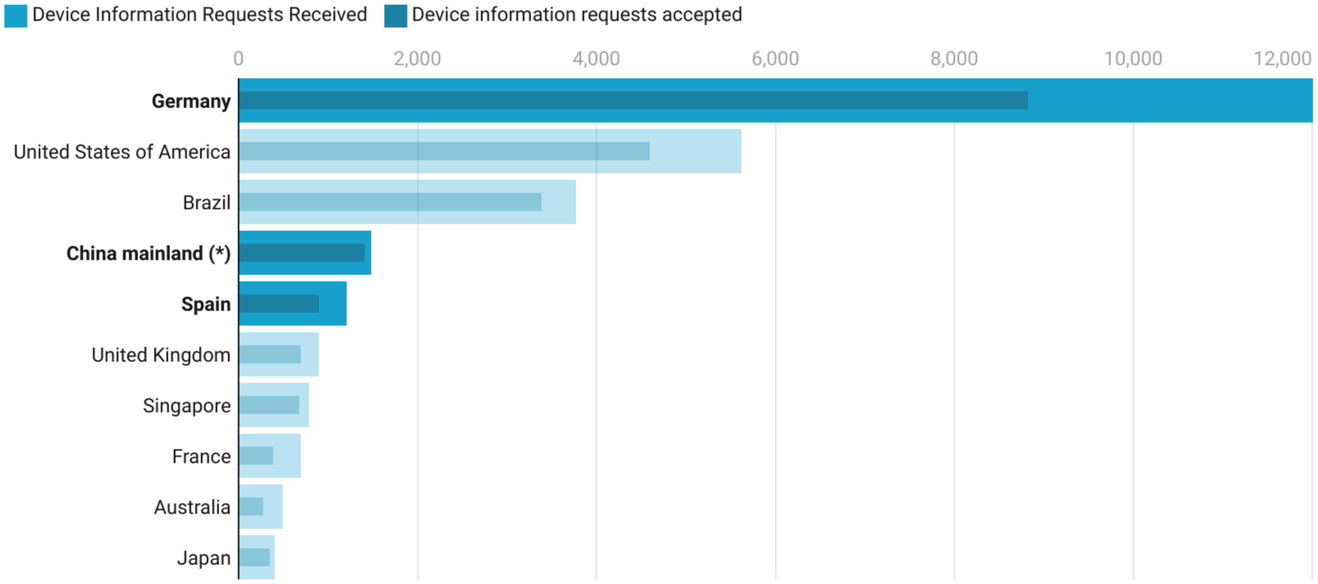
Governments sometimes need to rely on large corporations to help them do their jobs. When a threat involves knowing the identity or having access to the data of a potential attacker or a victim in danger, the digital information stored by these companies can prove vital to the investigation and avert a catastrophe. Apple publishes a comprehensive report every six months on what data governments request from it, which data and to what extent the requests are fulfilled. We update here some data we have extracted from the information published by Apple for the first half of the year 2022 (the last published by Apple as of the second half of 2023) on the activities and requests from governments to the company.

Device-based requests

This represents requests from government agencies requesting Apple device information, such as serial number or IMEI number. When law enforcement agencies are acting on behalf of customers whose devices have been lost or stolen, for example. It also receives requests related to fraud investigations: they typically request details of Apple customers associated with Apple devices or connections to Apple services.

Germany is the country with more device information requests in the first half of 2022

The total number of requests made and those accepted by apple are displayed.



In this Top 10, the degree of acceptance varies from 55% for requests from Australia to 95% for those corresponding to China. China leads by a wide margin, however, in the number of devices it requests information on, with more than 165,000 devices.

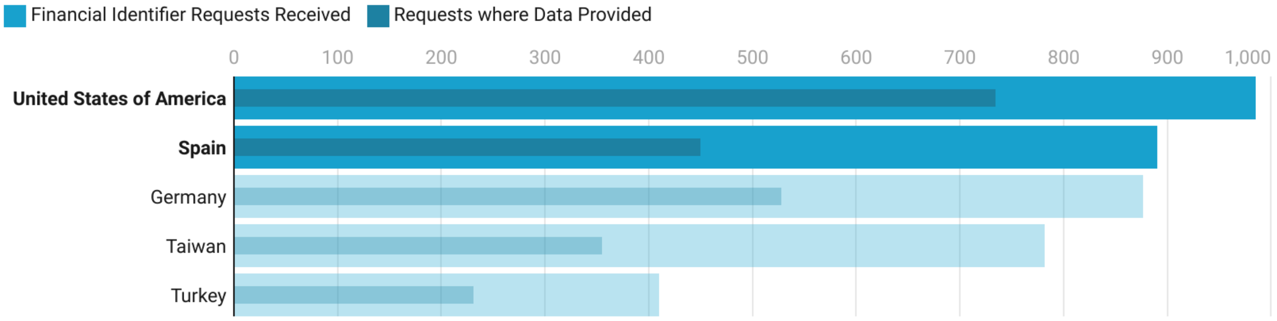
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Requests based on financial data

These requests are made when law enforcement acts on behalf of customers who require assistance related to fraudulent credit card or gift card activity that has been used to purchase Apple products.

USA leads fraud requests made in the first half of 2022, with Spain in a surprising second position.

The total number of requests made and those accepted by Apple are displayed.



The degree of acceptance among the 5 countries with the highest volume varies from 45% for requests from Taiwan to 75% for those corresponding to the USA.

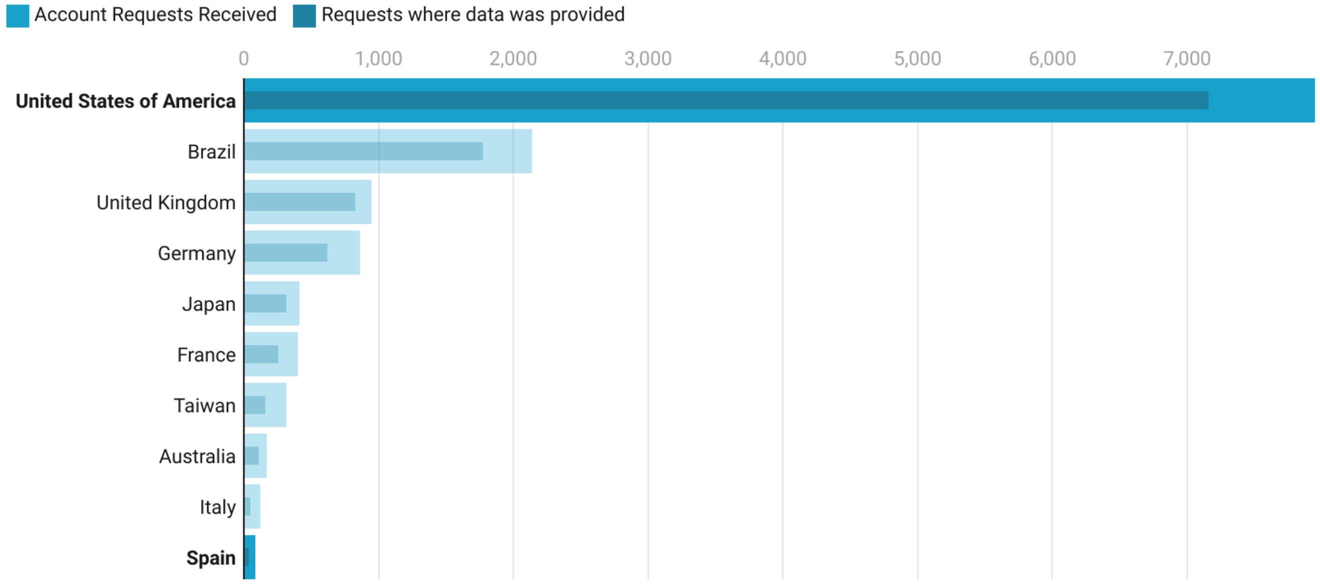
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Account-based requests

Requests are made, from governments, to Apple related to accounts that may have been used against the law and Apple's terms of use. These are iCloud or iTunes accounts and their name, address and even cloud content (backup, photos, contacts...).

USA once again leads by a wide margin in the requests for account information sent to Apple during the first six months of 2022.

The total number of requests made and those where data (content or metadata) was provided by Apple are displayed.



Out of 79 requests made by Spain, the tenth country with the highest number of requests, only 34 were accepted (43%).

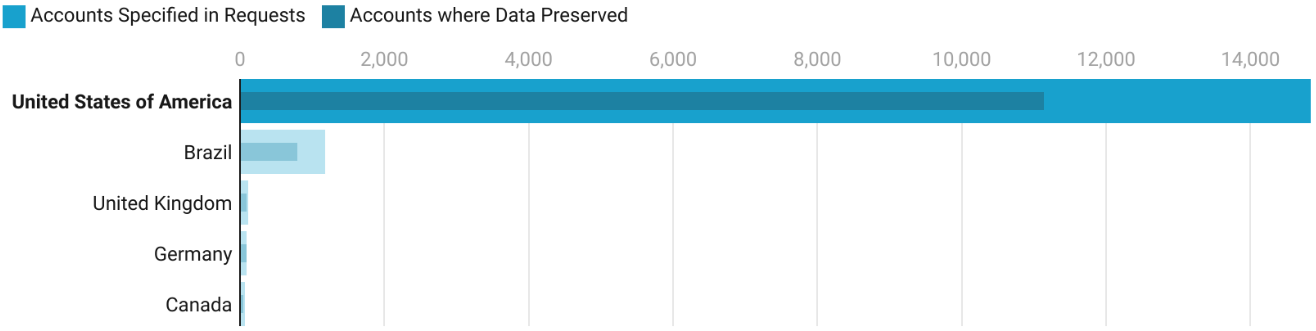
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Account Preservation Requests

Under the context of the U.S. Electronic Communications Privacy Act (ECPA), Apple may be requested to "freeze" an account's data and hold it for 90 to 180 days. This is a preliminary step to requesting access to the account, pending legal permission to request data and to prevent the account from being deleted by the respondent.

USA outnumbers any other country by tenfold in requests for account preservation to Apple during the first six months of 2022.

The total number of accounts whose preservation was requested and those preserved by Apple are displayed.



Spain did not issue a single requests during this period.

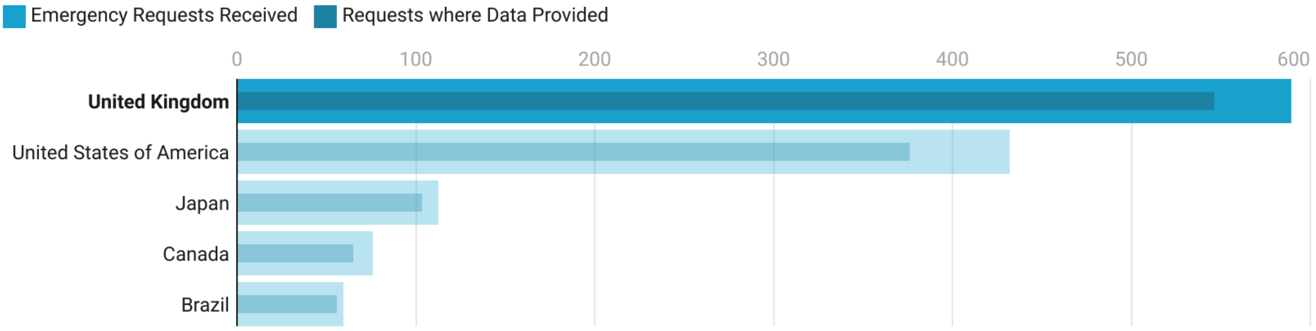
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Emergency Requests

Also, under the U.S. Electronic Communications Privacy Act (ECPA), it is possible to request Apple to provide private account data if in emergency situations it is believed that this could avert a danger of death or serious harm to individuals.

UK is the country that made the most requests for emergency access to accounts in the first half of 2022.

The total number of requests made and those accepted by Apple due to emergencies are displayed.



Spain, ranking 18th in the list, issued 3 requests for emergency account access, of which only 1 was accepted (33%).

Chart: Juan Elosua • Source: Apple • Created with Datawrapper

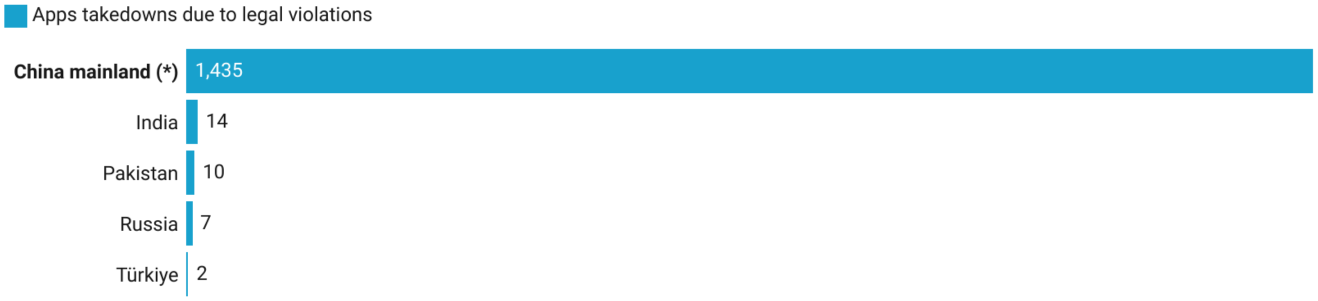
Requests related to the removal of apps from the market

In mid-2023 Apple has published its commitment to generate a specific transparency report for its App Store in which it has expanded the information related to the removal of apps from the market by making available to the public some interesting information that we will analyze below.

Following on from other semi-annual reports, we begin by exploring app recalls that violate the sovereign law of the requesting country/region.

China requested 1,435 app removals from the market for legal reasons in the first half of 2022, outnumbering the next country in the ranking by 100 times.

Apps whose removal from the respective market has been carried out due to legal requirements of the government are shown.



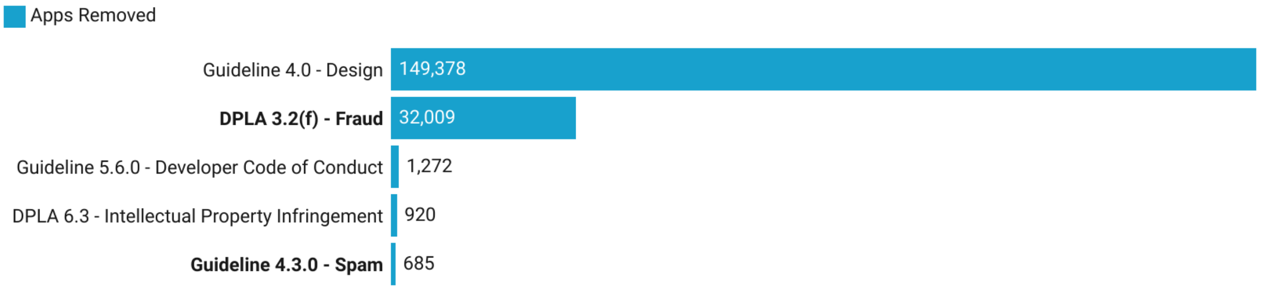
(*) 1,276 of those apps removed by China are games that do not have the GRN license (More info about GRN licenses: https://appinchina.co/how-to-get-a-game-license-in-china/)

Chart: Juan Elosua • Source: Apple • Created with Datawrapper

The following is an interesting summary of application withdrawals for non-compliance with Apple's internal regulations within the review process to reach the market as well as for non-compliance with Apple's application developer agreement.

Fraud and Spam are among the top 5 reasons for app removal from the 2022 market for non-compliance with Apple's regulations or development policies.

Apps that have been removed and the specific regulations that have been breached are shown.



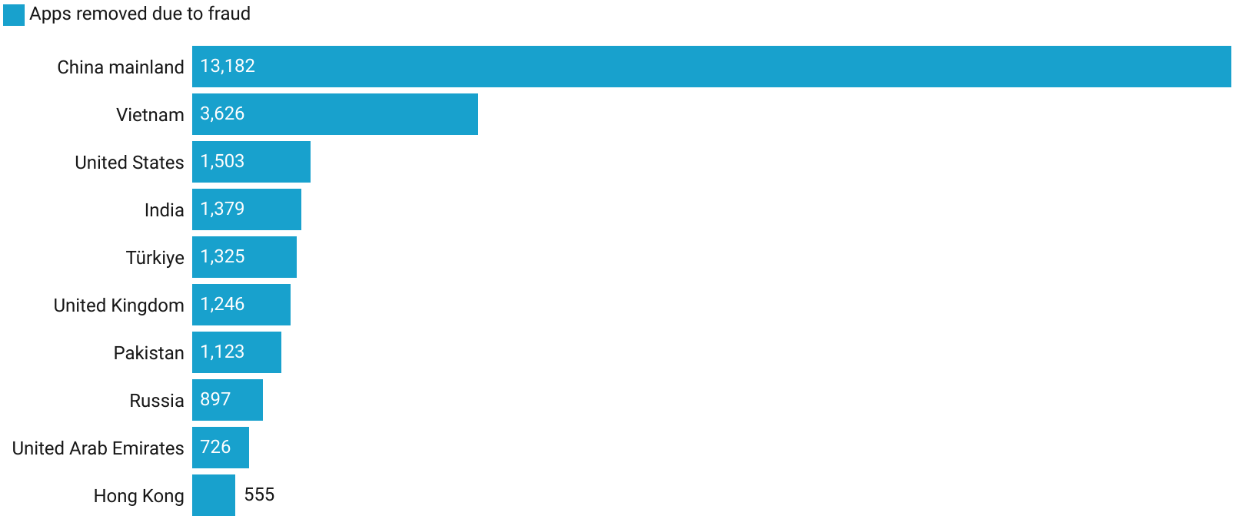
More info at: https://developer.apple.com/support/terms/apple-developer-program-license-agreement/ and https://developer.apple.com/app-store/review/guidelines/

Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Focusing on the more cyber security-related categories, we can see a detailed ranking of the top 10 countries with developments with the most spam and fraud breaches.

Top 10 countries with apps removed from the Apple Store due to fraud in the year 2022.

Apps removed by country or region are shown.

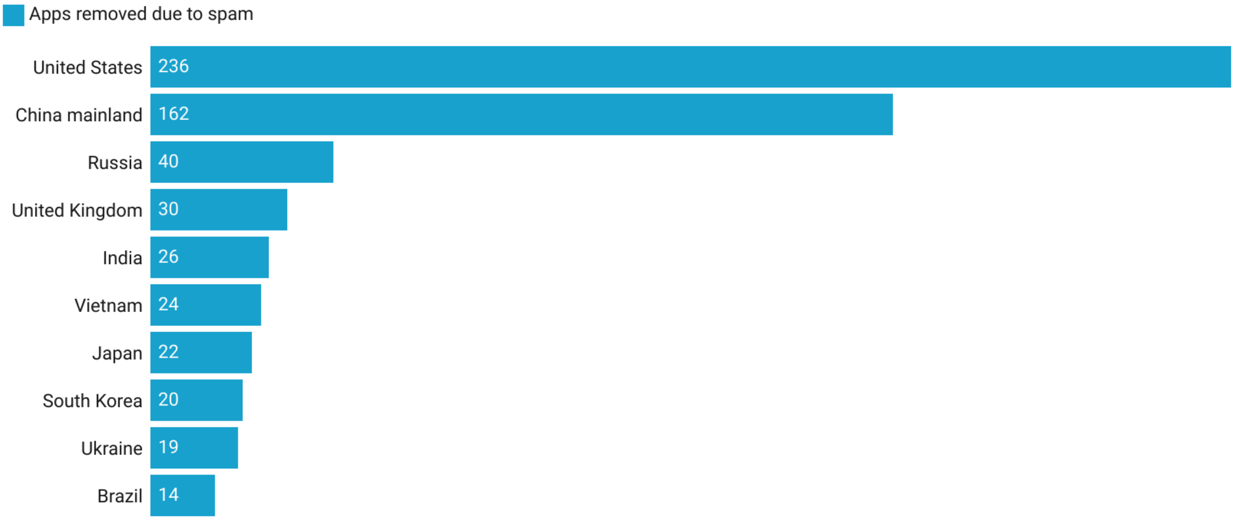


More info at: https://developer.apple.com/support/terms/apple-developer-program-license-agreement/#ADPLA3.2

Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Top 10 countries with apps removed from the Apple Store due to spam in the year 2022.

Apps removed by country or region are shown.



More info at: https://developer.apple.com/app-store/review/guidelines/#spam

Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Conclusions

We could conclude that certain governments "too often" request access to data, but also argue that it may be the case that justice works more smoothly there, or that there is more fraud more in these locations, the interpretation is free. Here are some conclusions based on our analysis:

- The German government has generated the most requests for device information.
- Spain ranks a surprising second in requests for account information by fraud in the first half of 2022, although only half have been accepted by Apple.
- The United States requests by far more than any other country for account preservation and access to the data hosted on it. What continues to stand out from our analysis is that Brazil remains in a strong second place with requests doubling from third place.
- The UK continues to lead in requests for access to account information for emergency situations, those where danger to life or serious harm to individuals can be averted. This is surprising in light of the volumes of US account access. This reinforces the theory that there is a procedure for launching such requests by its foreign department.
- Unsurprisingly, China continues to be the country that requests the most app takedowns in the App Store. The difference is huge with the rest of the world. This year, thanks to the new App Store transparency report, we know that 1,276 of the total 1,435 apps removed are due to games that do not have the approval of the Chinese regulatory body. From the nearly 300 apps whose removal has been requested by China in the last half of 2021 we go to only 6 for Russia which occupies the second place in this list.
- Finally, we see that among the apps removed from the Apple App Store, fraud and spam are part of the "Top 5" categories of violations committed by developers in 2022.

Clarification: In this exercise we have charted the tables published by Apple itself. It is important to specify that requests are made in batches that may include more than one account or device. For example, Apple counts the number of requests for device information, and in turn each request can contain an undetermined number of devices in them. Same thing with account requests and the number of accounts in each request. When Apple talks about the percentage of fulfilled requests, it is talking about requests, but not about specific accounts. As an example: Apple receives 10 requests, with 100 devices among all the requests and then says it has satisfied 90% of the requests, we don't know how many individual devices have been provided. So this is an exercise that can give us a rough idea of the actual number of devices provided for the example given.

Android

New security features

As usual, we released Android 14 in the month of October, specifically it was released on the 4th. Version 14 is known internally as "Upside down cake".

We already mentioned in the previous report that one of the new security measures was to prevent the installation of applications considered outdated. Starting with Android 14, it will not be easy for the user to install applications designed for SDKs lower than version 23. This is because a lot of malware uses older SDK functions that put it at an advantage with respect to the system's modern protections. In other words, in order to be able to run "old" applications, Android allows a level of backward compatibility that leads to a loss of protection.

Another interesting measure is the requirement that code dynamically loaded by an application can only be read (read permission) and not executed. In addition, the Android project expressly discourages developers from using the dynamic code loading feature, due to the insecurity it entails.

Regarding privacy, Android allows (finally) to give permission photo by photo (or video) if an application requests access to the media. Previously the permission to access the gallery was either all or nothing, something that did not convince users. From this version onwards we can give permission in a more granular way.

Vulnerabilities

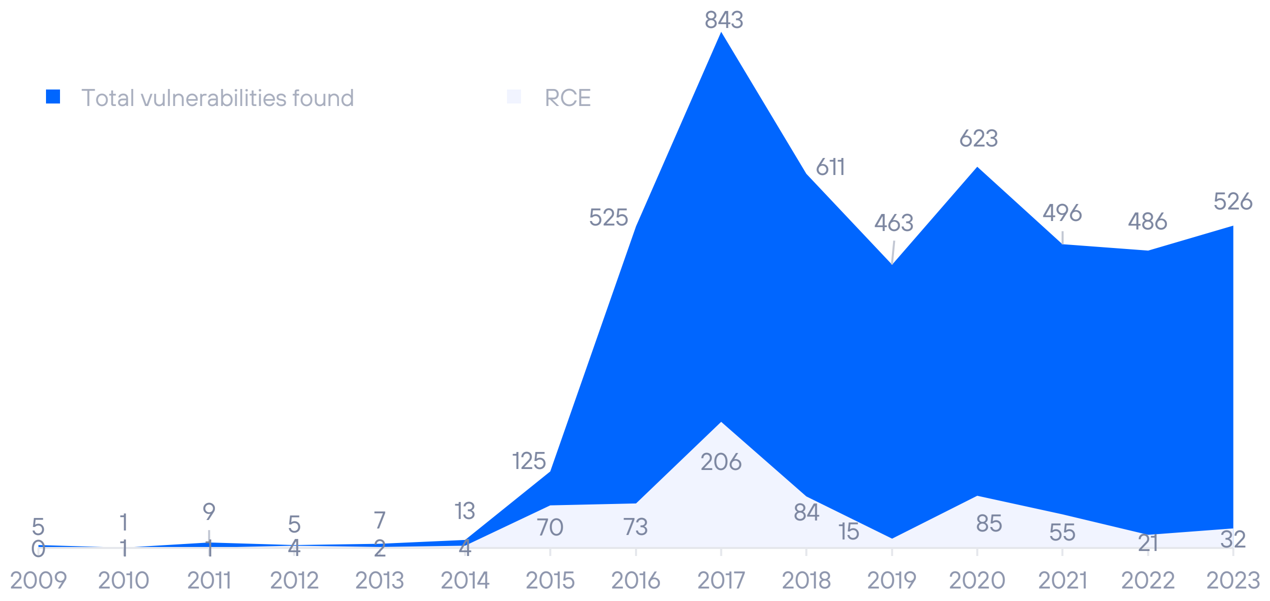
Android releases a set of patches every month, usually during the first week. In this second half of 2023, six bulletins have been published with a distribution of 43, 40, 32, 51, 37, 94 patches or CVEs fixed per month. Likewise, by monthly appearance, critical bugs are distributed as 2, 3, 3, 3, 2, 0, 1 respectively.

In total, 297 patches (the previous six-month period was 229); 11 of them are considered critical (21 in the previous six-month period).

It should be noted that many of these bugs affect the software or firmware of certain manufacturers in particular, which means that the same vulnerability does not necessarily affect the entire stock of Android devices, but only those with the affected components.

VULNERABILITIES IN ANDROID 2023-H2

Evolution of vulnerabilities per year



Fragmentation in Android systems

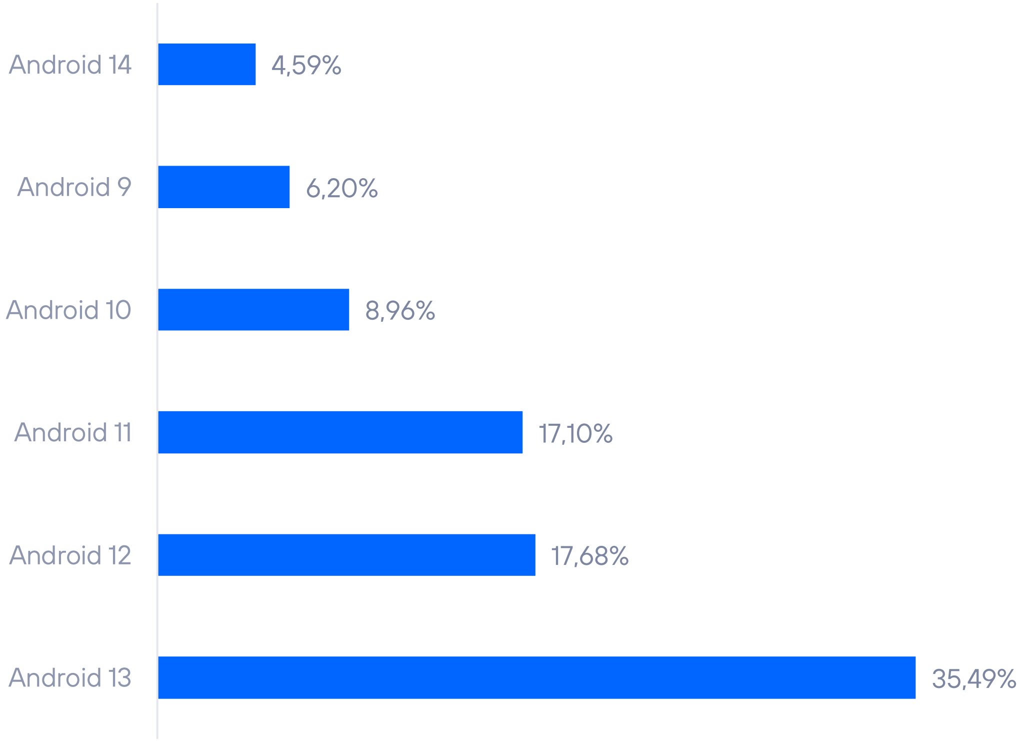
The latest publication of *Statcounter* at the date of this report indicates that the most widely deployed version of Android is version 13, with a share of 35.49%, followed by version 12 with a share of 17.68%.

It is typical in Android that new versions of the operating system take a long time to be adopted, mainly because each manufacturer must customize and adapt the changes to the particularities of the device and idiosyncrasies of the brand.

The new version, Android 14, has only 4.59%. This is normal in Android; new versions take a long time to catch on with the public, mainly due to the relative aging of the operating system terminals, in which the systems see how in a little more than two or three years they stop receiving updates.

Another negative aspect is the continued existence of unsupported systems, which continue in active operation without receiving security updates. For example, the most extreme case is Android version 9, which has 6.2% of the market and ceased to be supported in January 2022. Android 10, whose share is 8.96%, is also no longer supported in 2023.

FRAGMENTATION IN ANDROID 2023-H2



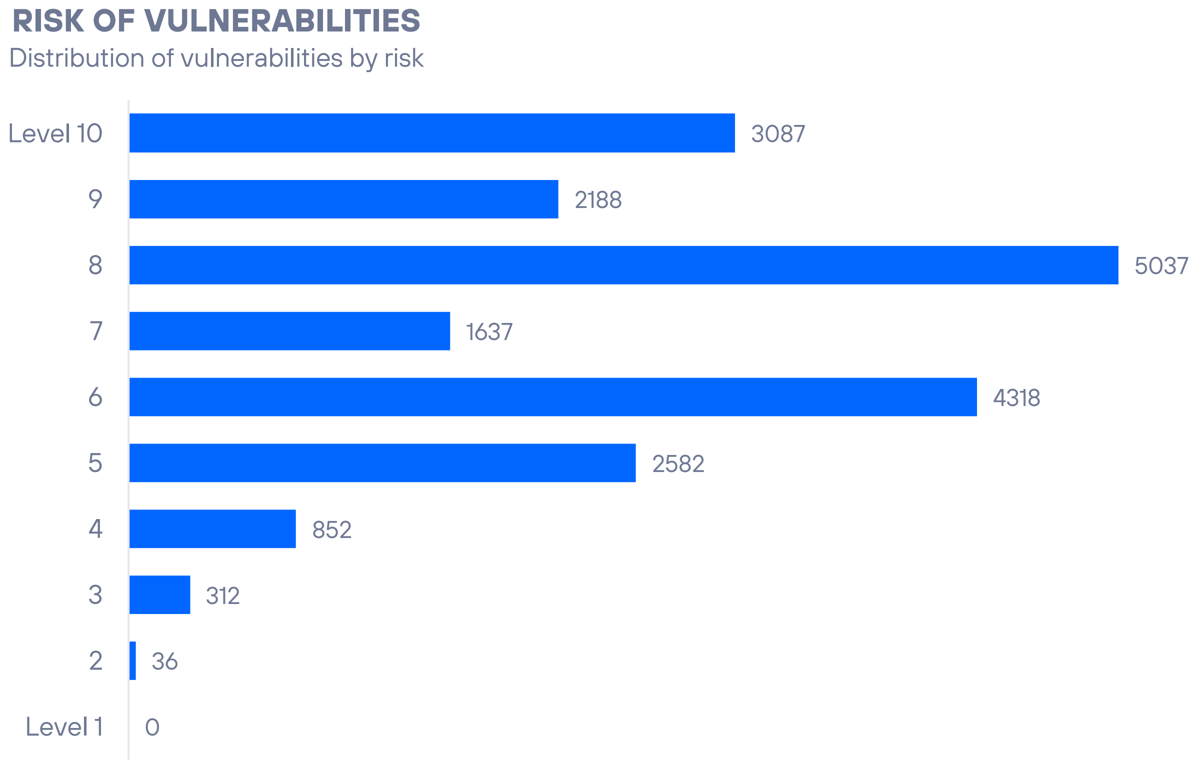
SIGNIFICANT VULNERABILITIES

In this section we will discuss some of the key vulnerabilities of the second half of 2023.

CVE ID	TARGET	DESCRIPTION	SCORING
CVE-2023-3638	GV-ADR2701 Geovision Cameras	An attacker could edit the login response to access the vulnerable camera web application. Identifier CVE-2023-3638 has been assigned for this vulnerability.	9.8
CVE-2023-1935	RTU Emerson controllers	These devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a DoS condition.	9.4
CVE-2023-4523	Real Time Automation Gateways 460	This series of gateways with versions prior to 8.9.8 are vulnerable to Cross-Site Scripting, which could allow an attacker to execute any JavaScript reference from the URL string.	9.4
CVE-2023-5642	Monitoring software for industrial routers	An attacker could access sensitive information, including database access credentials and a default SNMP string (a string similar to a user ID or password that allows access to a device's statistics).	9.8
CVE-2023-20198	Cisco IOS XE software Web user interface	The attacker could additionally log into the product database, create an application-level SuperAdmin user, and log into the product's web user interface with that user.	10

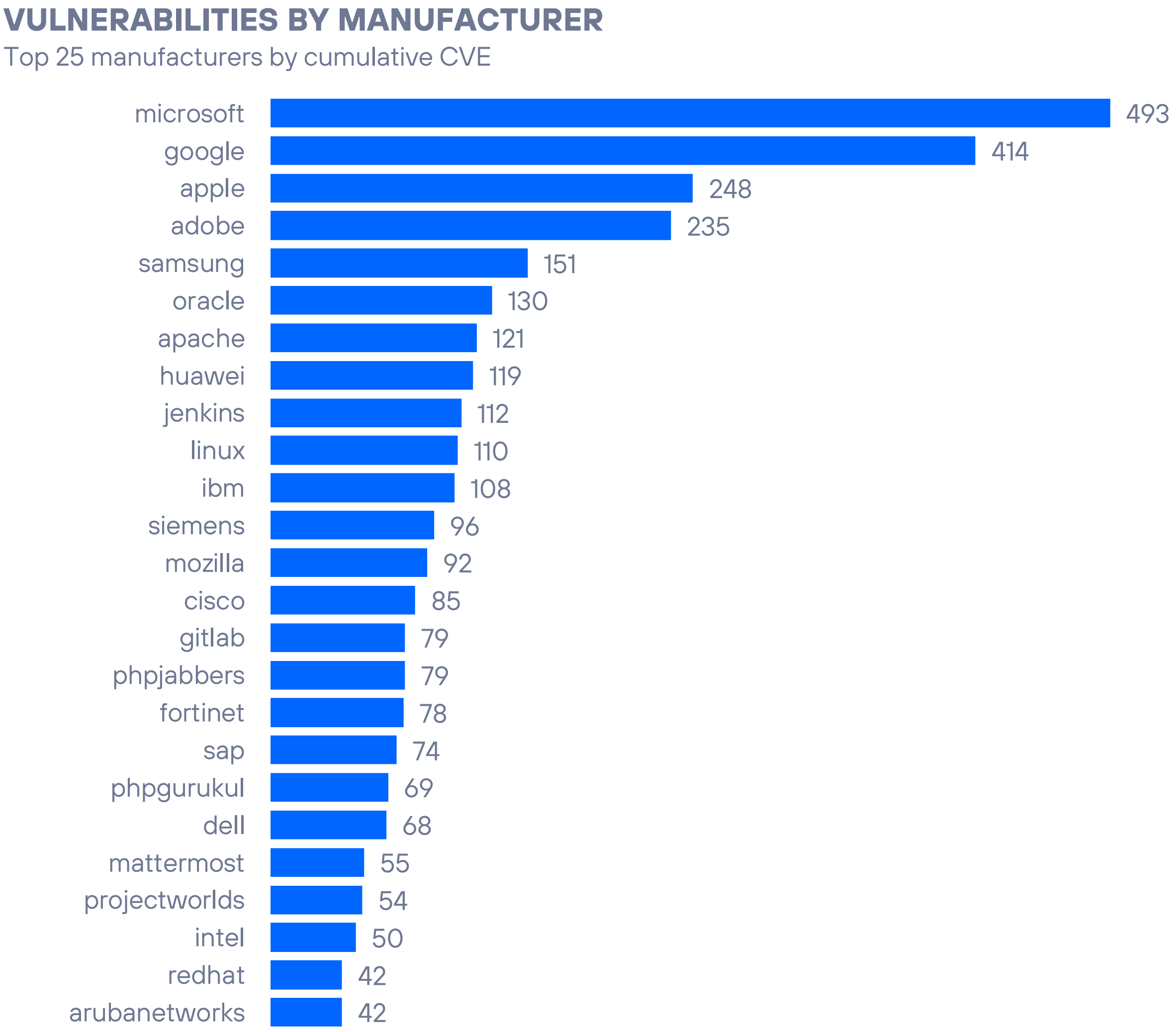
Vulnerabilities in figures

The distribution of CVEs published by risk level (scoring based on CVSSv3), in terms of the number of vulnerabilities discovered, was as follows.



Top 25 companies with the most accumulated CVEs

During the first half of 2023, Microsoft has led by far in terms of number of known vulnerabilities, followed by Google. In general, it is usual for the big three, along with Oracle, to always be among the first in terms of number of vulnerabilities. This half year, Apple has also been among the top three, with a significant increase in the number of vulnerabilities fixed compared to the first half of the year.



APT OPERATIONS, ORGANIZED GROUPS AND ASSOCIATED MALWARE

We review the activity of the various groups attributed with the authorship of APT operations or major campaigns.

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

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

Significant APT activity, detected during the first half of 2023

STORM 0558 – Category 5 storm

This group, originally from China, has gained fame thanks to an attack against the U.S. State Department. According to the investigation, it was able to steal 60,000 emails from 10 accounts, as well as a list of all the contacts of this agency.

According to Microsoft researchers, Storm stole an MSA account after successfully compromising the corporate account of a Microsoft engineer. They forged Outlook access tokens via OWA and Outlook.com with this account.

It was not only the US DoD that was affected. Other institutions, such as the US ambassador to China, were also affected.

More information: https://www.infosecurity-magazine.com/news/microsoft-breach-60000-state/

Multiplayer: the era of global conflict

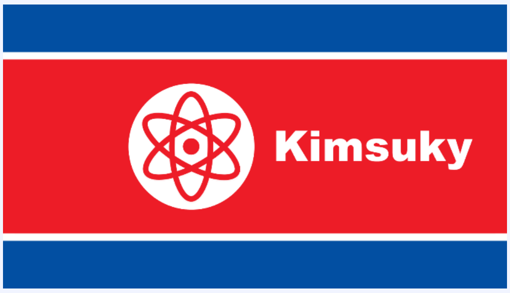
This case is proof of the unstoppable global chessboard on which we all move.
Several APT groups of Indonesian origin attacked Indian government services with several DDoS to the point of rendering them unserviceable. The justification of these groups was that other groups of Indian origin, namely "Indian Cyber Force" had attacked the official website of the terrorist group Hamas.
The Indonesian groups responsible for this attack were Ganosec, Garnesia, and Sylhet, among others.

All the information of these actions (both Indian and Indonesian) was published by the groups themselves on their Telegram channels.

More information: https://business.outlookindia.com/news/israel-hamas-war-indian-cyber-space-caught-in-the-crossfire-as-threat-groups-escalate-online-conflict

APT43 – Kimsuky: de grupo APT a parte del estado

This group, which we discussed in 2020, has been sanctioned by OFAC, the US Treasury Department's Office of Foreign Assets Control.
Although it may seem absurd to "sanction" such a group, in practice it means recognizing it as part of the North Korean government and linking it directly to its financing and intelligence work. OFAC specifically recognizes it as "the main foreign intelligence service" of North Korea.



Be that as it may, the fact remains that Kimsuky's activity has been long and prosperous (for them). They have been active since before 2010 and their attacks are usually directed at high-profile targets. Initially, they focused on South Korea (operation "Kabar Cobra", for example), but over time they expanded their scope, with deception campaigns using SARS-COV-2 and attacking international institutions such as the UN.

More information: https://www.bleepingcomputer.com/news/security/us-govt-sanctions-north-koreas-kimsuky-hacking-group/

APT28 – Fancy bear: A very fit old bear

The long career of the Fancy bear group seems to have no end. In fact, it was already in its prime when we talked about it back in 2020.
In this case, the group has been discovered using exploits based on Outlook 0-day vulnerabilities against several NATO targets, including the Rapid Reaction Corps (NRDC), although it is not known from which country.

Having analyzed the vulnerability, researchers in Palo Alto detected activity as early as March 2022, and other European authorities have been warning of more activity this year. In an attempt to continue its success, Fancy bear has been mixing in several other vulnerabilities, which could imply an above-average interest in these targets during this time.

More information: https://www.bleepingcomputer.com/news/security/russian-military-hackers-target-nato-fast-reaction-corps/

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 appear to be industrial systems in real production, and behave as such, but are extracting all the information about the threats accessing the system. With the information from all the devices deployed in the different node-signposts, Aristeo applies relationships and intelligence to go beyond the data, being able to proactively detect campaigns, targeted or sectorized 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. Moreover, the nodes are alive, which means that they can undergo alterations in their configuration at the discretion of the team of researchers working with them, or of the client who has temporary or permanent use of them. This variability may generate slight discrepancies in the data shown in this section when compared between semesters.

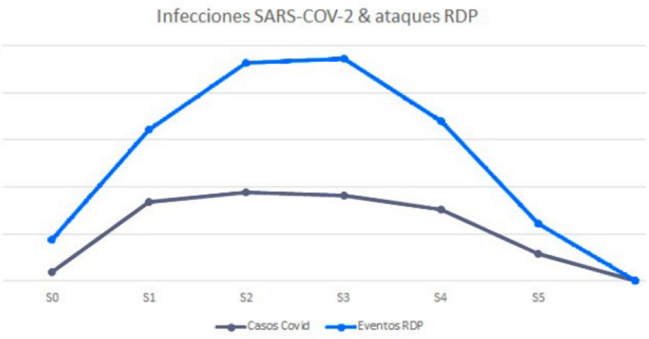
More information: https://aristeo.elevenlabs.tech

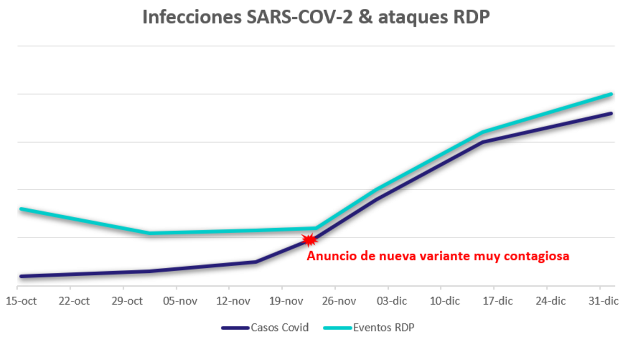
Data analysis

The Aristeo system has been with us long enough to be able to do the following analysis. This semester we are going to talk about how the threat landscape has evolved over this time.

2021-Pandemic Year II

The year 2021 is the first year in which Aristeo is considered stable enough and accurate enough to provide data for the report. What we are experiencing at this time is a pandemic that does not leave us and the need to set up remote connection services every time the incidence of the virus rises. Although we had already been living with the pandemic for some time, the temporary nature of these services meant that many companies did not devote sufficient time to their proper securitization. Criminals, aware of this, acted ferociously on these services.





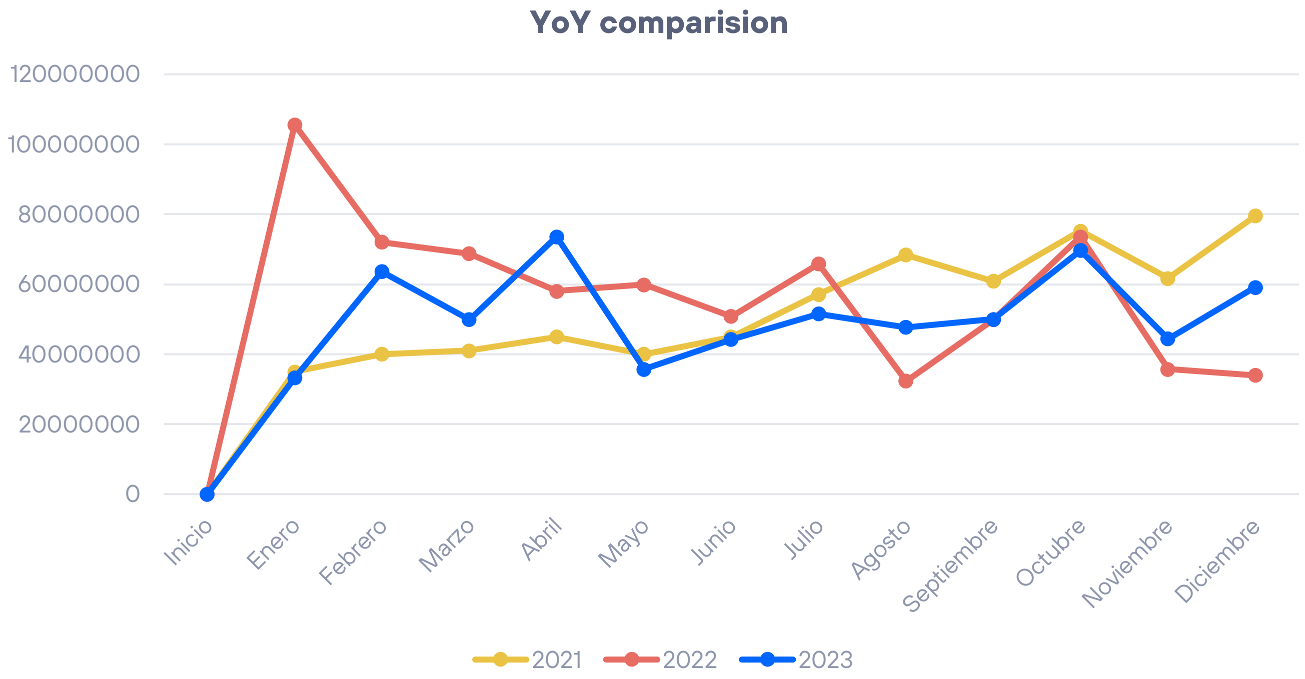
2022-Old European ghosts

The situation in Europe changed in 2022, resulting in some peculiar data. The beginning of the year was frenetic, until a certain stabilization began (within a pattern we will see later). With this activity on our minds, we took Aristeo out to see Europe. The results were the discovery and reaffirmation of trends and patterns we had seen previously. In addition, we demonstrated that our approach of using only real industrial hardware is valid for roaming systems (because yes, real systems work "really in reality") and that, although it seems obvious, it is more efficient than virtual systems.

2023-Reaffirmation and New Horizons

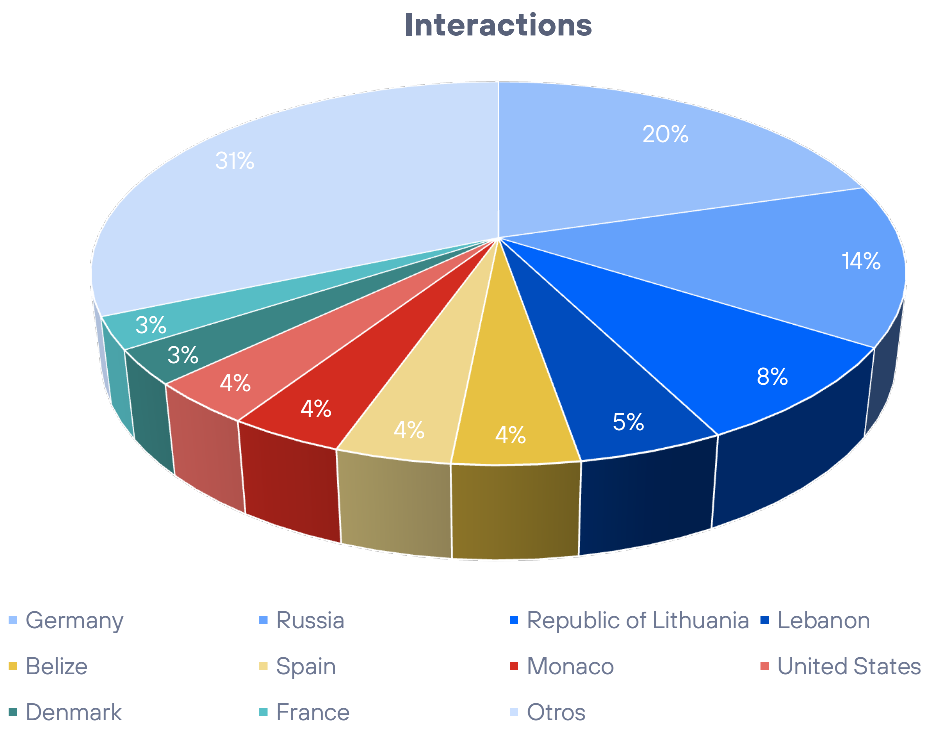
After the 2022 excursions, 2023 was the year to confirm what we had seen after a pandemic that had made a lot of noise and a lot of changes in attack and defense in the cyber domain. There are clear patterns that make sense the more data collection time we have, but we also start to see sense in the changes within those patterns, which helps us serve even better predictive intelligence to our customers.

To conclude, we show a monthly threat capture graph over these three years:



We now turn to the overall statistics of the recorded information. In the second half of 2023, more than 322 million cyber security events were detected. This represents a small rise compared to the data recorded in the first quarter of 2023, approximately 7% more, also compared to the same period last year. Despite all this, the final number of events for 2023 was 622 million. Almost 22% less than last year (706M). The difference between 2022 and 2023 was mainly the first half of 2022, which recorded more than 400 million events.

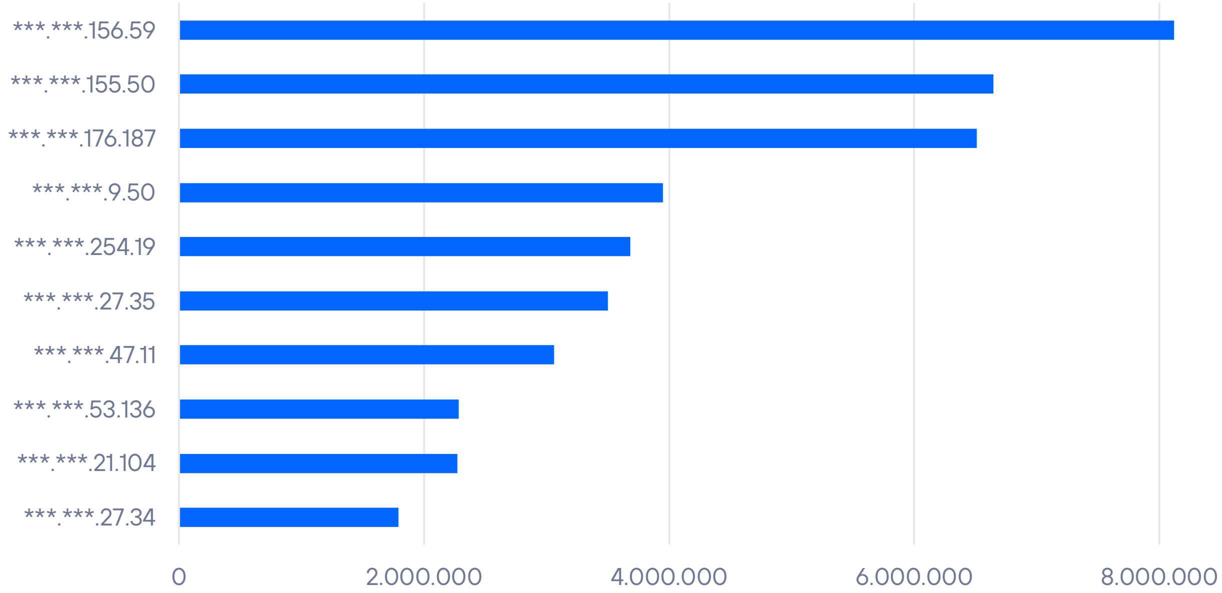
The distribution by country would be as follows:



The dispersion of previous years is generally maintained. This is something we have been witnessing since the beginning of the year and demonstrates the stability of our platform and of the global threat landscape in general numbers. Furthermore, not only does it remain the same between the top 10 and the other countries of origin of the recorded threats, but among the top 10 it also remains approximately the same weight. Panama's increase in weight is also striking, but we will talk about that in two graphs.

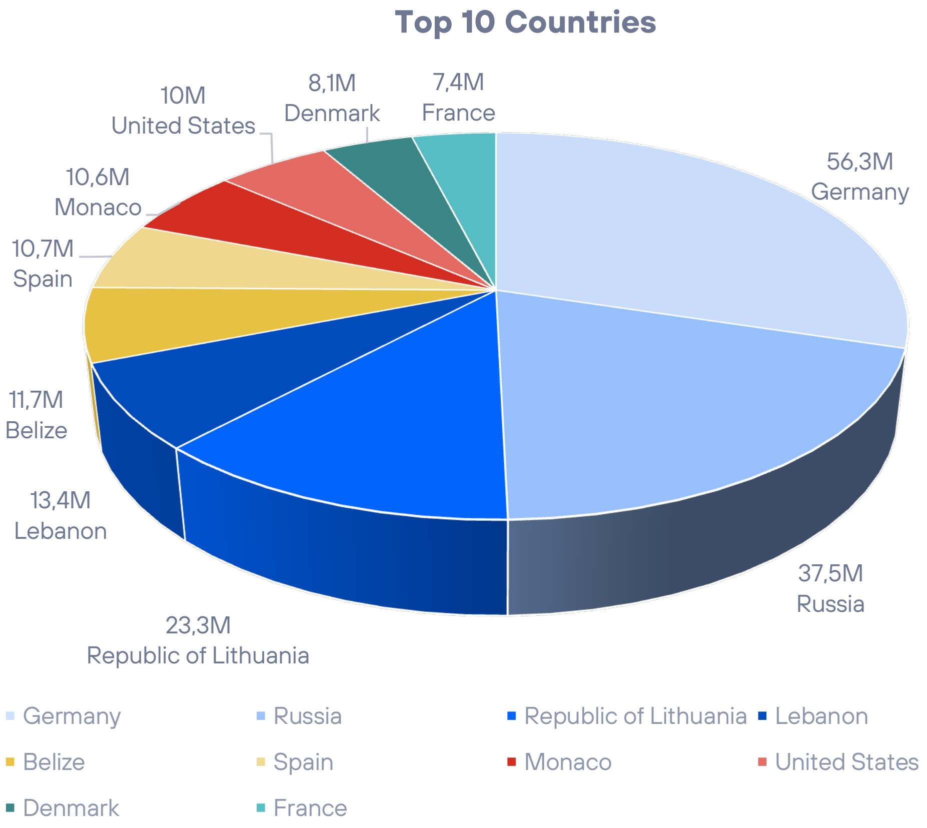
Now let's take a look at the top ten IP addresses with the most interaction with the Aristeo system. In this semester, 95% of the top 10 IP addresses registered in our system come from Central Europe. The attentive reader will have done the quick calculation: 95% of 10 is 9.5 How do you explain that half of the IPs are European, and the other half are not? Because sometimes there are IP addresses geolocated in a physical point, but which are delegated or managed from other sites in the interest of their owner.

TOP-10 IP attackers



Below is a summary of the distribution of the top 10 registered countries. In this half-year, the most striking figure is that of Panama in terms of the number of detections. After rising to second place in the first quarter, it has gradually declined in recent months until it has returned to more normal terms of its historical presence. This should imply that the campaign we were following in the previous half-year may be over.

Also, in the report for the previous semester we also drew attention to the decrease in detections from the USA and, in the light of the data, it is fair to point out that this has become the trend. Moreover, the first country of origin this time is Germany, which reinforces our view that the majority of origins detected this half-year have come from Europe, as we mentioned earlier.


Top 10 Countries
56,3M
Germany
37,5M
Russia
23,3M
Republic of Lithuania
13,4M
Lebanon
11,7M
Belize
10,7M
Spain
10,6M
Monaco
10M
United States
8,1M
Denmark
7,4M
France
Germany
Russia
Republic of Lithuania
Lebanon
Belize
Spain
Monaco
United States
Denmark
France

THREAT ANALYSIS BY INDICATOR

In collaboration with Maltiverse, we have conducted a ranking study of the indicators of compromise detected on their platform. That is, to indicate interesting attributes of maliciousness detected in IP addresses, domain names and URLs over the last six months. In total, for the different IOCs involved we have studied: 294,321 IP addresses, 99,792 domains and 303,225 URLs.

What kind of maliciousness do the URLs studied involve?

As we know, URLs allow us to access resources, they describe a protocol, a machine on the Internet (either directly through an IP or indirectly from a domain) and within that machine a resource is specified through a path.

In the end, in the context of malware, every IP and domain will be part of a URL to request a resource. Whether it is a URL that directs us to a phishing site and has a domain very similar to the original or it may be that the URL serves as a download point for malware.

It is important to determine what is at the end of the URL and categorize it properly to know what type of threat we are dealing with. This is precisely what we have asked in the Maltiverse database, and the following results have been found:

TYPE	QUANTITY	PERCENTAGE
Phishing	189884	62,62%
Malware Download	68138	22,47%
Malicious URL	42173	13,91%
Cobalt Strike	6262	2,07%
DBatLoader	1621	0,53%
IRATA	1514	0,50%
RecordBreaker	907	0,30%
Meterpreter	710	0,23%
GootLoader	496	0,16%
Lumma Stealer	475	0,16%

There are no surprises regarding the two categories with the highest number of indicators: phishing and malware download. Because if there is a classic in cyber security regarding what awaits us at the end of a URL, it is precisely these two major categories. Another generous figure, with 13.91%, is the generic category of "Malicious URL".

However, these are categories that group or assimilate a large part of what we find in the long tail. The rest of the categories are more explicit and even indicate to which malware family they belong.

The now classic "Cobalt Strike", for example, has a record number within its specialty: more than 2% of all URLs are related to this executable which, although it belongs to a tool used in pentesting, the malware industry has been able to take advantage of it in its operations. Another similar component (with 0.23%) is "meterpreter", included in the popular exploit suite: Metasploit.

Which domains are most frequently used by URLs flagged as malicious?

We consulted Maltiverse this year to find out which domains appear most frequently in the URLs studied. It is interesting to note which services, mostly legitimate, are the most used by malware authors and their associated campaigns.

In the end, a URL will have a host or redirect and needs an executable web space or application that at some point it will use for its purposes. It is the domain that will "tell us" where it has been hosted and what service it has used (illegitimately, for example).

DOMAIN	QUANTITY	PERCENTAGE
workers.dev	15086	4,98%
duckdns.org	4008	1,32%
weeblysite.com	3621	1,19%
web.app	3518	1,16%
github.io	3496	1,15%
blogspot.com	3183	1,05%
firebaseapp.com	3020	1,00%
r2.dev	2723	0,90%
pages.dev	2531	0,83%
000webhostapp.com	2378	0,78%

Very interesting. "workers.dev" is a "serverless" service from Cloudflare. Like almost all of those listed in the ranking, they are free to some extent. Malware writers take advantage of free account features to deposit their function and exploit them until they are reported or discovered.

Among the results are several Google services: "blogspot.com" and "firebaseapp.com". The former is Google's free blogging platform, while the latter relates to mobile applications.

Other services include dynamic IP resolvers "duckdns.org". These are used to dynamically point to IP addresses without the need to register a domain. Widely used when hosting malicious material on infected personal computers.

The rest are sites known to provide free hosting or hosting for code repositories that also allow publishing web pages and some dynamic functionality.

Which countries are the IP addresses from which malicious activity has been detected?

Before answering the question, it should be made clear that just because a country appears in this ranking does not mean that there is malicious intent towards that country. Many countries stand out from the rest because they have more services and hosting companies, which translates directly into greater fraudulent use. A server can be hosted in a country and the criminal organization that uses it can come from another nationality.

COUNTRY	QUANTITY	PERCENTAGE
United States	55984	19,02%
China	41498	14,10%
India	24507	8,33%
Russia	16436	5,58%
Vietnam	11249	3,82%
Germany	10333	3,51%
Indonesia	8368	2,84%
Pakistan	8295	2,82%
United Kingdom	7776	2,64%
South Corea	5148	1,75%

There are no major variations in this aspect in recent years. These are countries with large technological infrastructures and therefore, as mentioned above, have proportionally greater potential for use by cybercrime.

What type of maliciousness do IP addresses engage in?

TYPE	QUANTITY	PERCENTAGE
Mail Spammer	283188	96,22%
HTTP Spammer	106524	36,19%
Malicious host	54501	18,52%
Proxy	48225	16,39%
SSH Attacker	36513	12,41%
HTTP Flood	17968	6,10%
Poor IP reputation on UDP traffic	12772	4,34%
Poor IP reputation on TCP traffic	12767	4,34%
DDOS Attack	8849	3,01%
Brute force	6863	2,33%

We find the undisputed winner at the top of the ranking: SPAM. It has been the ranking par excellence for decades now. SPAM marking rules are very sensitive to this activity.

We could practically say that almost every public IP address will have been marked as SPAM at some point.

The rest, except for the generalist categorization of "Malicious host", is similarly divided and almost evenly distributed. There are, for example, IP addresses that act as open proxies, attacks focused on creating SSH sessions (almost always: dictionary or brute force attacks) or port scanning, which would include both scanners that take a census of the Internet and those whose activity is more inclined to find open and vulnerable services.

What are the top-level domains (TLDs) with the most malicious domains?

As we know, a domain refers to an IP address. In the world of cybercrime, domains are of paramount importance because they allow them to make use of this and to change the IP address if the currently active server ceases its malicious activity.

A domain is composed of several levels. If you look at them, they are stretches of strings separated by dots. If we get these groups from right to left, they form a hierarchy. The rightmost one is the highest-level domain.

We ca therefore group the domains categorized as malicious by their highest-level domain. The result is this:

TLD	QUANTITY	PERCENTAGE
com	33427	33,50%
org	8360	8,38%
net	6616	6,63%
top	5172	5,18%
app	4849	4,86%
link	2582	2,59%
xyz	2222	2,23%
my.id	2019	2,02%
biz	2003	2,01%
dev	1859	1,86%

It is no surprise that ".com" dominates the ranking, it is the TLD with the highest number of domains. However, there are some TLDs in the table that deserve an additional observation, for example the TLDs ".app" and ".xyz". In addition, we have a new guest in the ranking with the newcomer domain "my.id", which even manages to overtake "biz" and "dev".

The ".xyz" TLD is widely used in malicious domains used by malware, in particular and very much, by randomly generated domains or better known by its acronym: DGAs.

Regarding ".app" it is especially curious as it is a TLD for which Google paid more than $25 million to ICANN in February 2015 to take control of it. Moreover, it is a TLD for which HTTPS traffic is mandatory.

What malicious categorization do the studied domains possess?

Domains are closely linked to URLs (of which they are part) and also, of course, of the IP addresses to which a domain resolves.

Let’s see, finally, how these have been categorized over the last six months.

CATEGORY	QUANTITY	PERCENTAGE
Phishing	64322	64,46%
Malware download	8542	8,56%
NjRAT	3634	3,64%
Prometei	2880	2,89%
Cybergate	2574	2,58%
Cobalt Strike	1708	1,71%
Remcos	1648	1,65%
nanocore RAT	1618	1,62%
AsyncRAT	1346	1,35%
IRATA	1132	1,13%

As we have already mentioned, there is a very close relationship between domains and URLs, and this can be seen in the top 10 categories: phishing and malware. This month the RATs (trojans) NjRAT, and AsyncRAT appear strongly.

RECAP

As predicted, vulnerabilities fixed in iPhone have reached their highest number since 2017, although the number of bugs allowing code execution has at least dropped. A record not seen since 2017 was reached in 2022 and 2023 has beaten it again. On Android, the downward trend has been broken, although in the average with respect to previous years and far from the 2017 record.

Regarding Apple's transparency report, this edition (from the second half of 2021 but published recently) gains in granularity. China continues to be the country that requests the most app recalls in the App Store far behind the figures for the rest of the world. 1,276 of the total 1,435 apps withdrawn are due to games that do not have the approval of the Chinese regulatory body. And of the nearly 300 apps whose removal has been requested by China in the last half of 2021 we pass to only 6 for Russia which occupies the second place. We also see that within the apps removed from the Apple App Store, fraud and spam are part of the "Top 5" categories of violations committed by developers.

Microsoft, Google are the companies with the highest number of fixed bugs, as usual, although this semester Apple slips into third place overall.

In the second half of 2023, more than 322 million cyber security events were detected in Aristeo. This is a small increase compared to the data recorded in Q1 2023, approximately 7% more, also compared to the same period last year. Nevertheless, the final number of events for 2023 was 622 million. Almost 22% less than last year (706M). The difference between 2022 and 2023 was mainly the first half of 2022, which recorded more than 400 million events.

We can conclude from the analysis of the data in Maltiverse that many legitimate domains are being used for downloading and redirection in the fraud world. Workers.dev and duckdns.org stand out as domains that account for more than 5% of the malicious scans studied.

USEFUL LINKS

Do not just stay in the top layer of cyber security analysis, the semi-annual reports are both cumulative and summarized. Telefónica Tech's cyber security blog has much more information and news which may be interesting for you. Here are our most relevant articles.

IDENTITY

OSINT: un arma infrautilizada por el periodismo para combatir las fake news

Fallo en la privacidad: los dispositivos de Apple enviaban la MAC real del dispositivo junto a la aleatoria

La CIA publica un informe sobre deepfakes y cómo manejar esta amenaza

Remedios populares contra la fatiga de contraseña

CIBER SECURITY OT

La (llámala 'x') revolución industrial: La introducción de las nuevas tendencias en Ciberseguridad industrial

MALWARE

CitrixBleed, una vulnerabilidad en fase de explotación masiva

Escondiendo malware en Blockchain: Hosting gratuito y a prueba de takedowns

Las amistades peligrosas (o cómo una colaboración disfrazada en Github puede arruinarte el día)

ARTIFICIAL INTELLIGENCE Y CRYPTOGRAPHY

Riesgos en la Inteligencia Artificial: inyección de prompts en chatbots

Ciberseguridad en la era de la IA: por qué los ataques de phishing son ahora más peligrosos

El CNI publica un informe sobre la intersección entre IA y Ciberseguridad

Marvin, el fallo criptográfico que nunca se arreglará

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. ("Telefónica Tech") 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, service or technology 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, service or technology. The use of the product, service or technology 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 Telefónica Group) are registered service marks.