Telefónica Tech

Security Status Report 2024 H1

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

telefonicatech.com

Index

EXECUTIVE SUMMARY

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

The year 2024 begins with some very relevant news in the world of cyber security, although this has already become the norm. The previous semester we highlighted that Chrome suffered 8 0day vulnerabilities throughout 2023 and, so far in 2024, that number has already been reached. Undoubtedly, the “monoculture” of the Chromium engine has motivated attackers to exploit flaws in this software. The security bar is being raised as high as the attackers' skills.

We also highlight the attack on Microsoft by Midnight Blizzard, which stole information from Microsoft in an attack in January and used the data to gain unauthorized access to repositories and other internal systems. History repeats itself. In 2002 Microsoft launched an initiative called “Trustworthy Computing” that was a paradigm shift, prioritizing company-wide secure development and changing the more or less widespread view among Microsoft users that its software contained many bugs and design problems that made it unstable. At the end of 2023 Microsoft was once again forced to make a similar communication through its CEO Satya Nadella following a series of high-profile incidents that have again affected Microsoft's reputation and questioned its security culture and posture by many cyber security experts globally. The new Secure Future Initiative intends to work with security by design, by default and perform secure operations.

We will see the results of this initiative over the next few years. Attackers are putting us to the test. The enormous sophistication of the attack on Linux through the XZ library that occurred in the first half of the year makes it clear how complex the attacks are becoming.

Not only at the technical level or in the supply chain... This attack shows the importance and impact of trust as a new attack vector.Having gained the trust of a developer, actively collaborating with a project for years, all to, at the right time, modify the code so cleverly that it goes unnoticed and is only distributed in packages to avoid being seen in the repositories... A flawlessly patient strategy from the attacker's point of view, but which forces us to rethink even the collaboration and reputational model in open-source software.

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 important thing going on? 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 learn about 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 FIRST HALF OF 2024

The following are the news items that have had the greatest impact during the first half of 2024.

JANUARY

- **Midnight-blizzard attacks Microsoft:** Attackers, allegedly sponsored by the Russian state, breached Microsoft's internal network and stole emails from the company's leadership, legal, and cyber security team. **The intrusion began in late November 2023 and lasted until January 13**.
- **Ivanti connect secure:** On January 10, Ivanti issued a security advisory about two vulnerabilities in its Connect Secure (formerly Pulse Secure) VPN appliance that were being actively exploited. These two 0-days were identified as CVE-2023-46805 (Authentication bypass) and CVE-2024-21887 (command injection). **Ivanti's security advisory did not include firmware patches, but only temporary mitigations** in the form of an encrypted XML file that customers were required to run on their devices. Estimated impact on **more than 1,700 infected applications during the early stages of the attack**.
- **Critical vulnerability in Gitlab:** GitLab released security updates for the Community and Enterprise editions to fix two critical vulnerabilities (CVE-2023-7028, CVE- 2023-5356), one of them allowing **account hijacking without user interaction**.
- **23-and-me:** The company **attempted to blame its users for its January data breach, claiming they are responsible for using weak passwords.** The company was sued more than 30 times for its recent security breach and after the company **unilaterally changed its terms of service to force people into arbitration.**
- **Scraping for AI models:** The UK's privacy watchdog (ICO) launched a review of the legality of AI companies scraping web content to train generative models. **The initiative analyzes whether the practice infringes proprietary or contract laws and its compliance with existing data protection laws.**
- **Schneider Electric hit by "Cactus" ransomware:** According to BleepingComputer, the attack, carried out on January 17, affected the company's sustainability business division. This area offers consulting services to companies, primarily focusing on the renewable energy business. According to the media outlet, the attackers stole terabytes of data, including confidential information on the industrial infrastructure of the company's customers.

FEBRUARY

- **KeyTrap** (CVE-2023-50387): t is probably the worst DNS attack ever discovered. A denial-of-service on DNSSec servers (today used in 31% of resolutions) and precisely for processing cryptographic keys. The vulnerability can exhaust CPU resources on DNS servers and paralyze domain name lookups. **Exploitation requires only one malicious package, and some DNS servers can be down for up to 16 hours**. Microsoft, BIND, PowerDNS, and most major Linux distributions have released patches for KeyTrap.

- **LockBit breach dismantled:** The UK National Crime Agency (NCA), in collaboration with law enforcement agencies from 10 other countries including the FBI, have disrupted the infrastructure and services of the operators of the LockBit ransomware. The events took place on Monday, February 19, and according to Cyberscoop, the FBI has gained access to nearly 1,000 decryption keys, which would allow for the possible recovery or remediation of ongoing LockBit extortion operations. LockBit's managers have identified that they would have been compromised due to the exploitation of the PHP vulnerability registered as CVE-2023-3824.
- **Rhysida ransomware decrypted:** South Korean researchers have broken the encryption scheme used by the Rhysida ransomware and released a decryptor that allows victims to recover files without paying the ransom. **Launching any kind of decryption tool that exploits a vulnerability in the ransomware binaries is a dilemma.** This is because ransomware gangs will simply fix their code and eliminate a way for victims to recover files.
- **Novel fingerprinting technique in Spyware:** ENEA, a Swedish-based telecom security company, claims to have reproduced a previously unknown hack. Among the documentation in the court case between Whatsapp and NSO Group, the term **"MMS fingerprinting"** was used. This term is new in the industry and was not present on the internet except in a court case. **The attack reveals the target device and OS version through an MMS sent to the device without interaction, participation or message opening by the user.**
- **Controversial Reddit-Google deal:** Reddit and Google have concluded a $60 million agreement **that allows Google to Train AI Models with Reddit posts.** In addition, Google will also provide Reddit with tools to improve its internal search.
- **Varta Cyber Attack:** Well-known battery manufacturer Varta was forced to **shut down production at five factories as a result of a cyber-attack.** The incident took place on February 12, and also affected the company's administrative network. The company says it disconnected the affected networks from the internet while it investigated the incident.
- More than 100 Romanian hospitals hit by ransomware: Over the weekend of February 10-11, an attacker reached the widely used "Hippocrate" information system and encrypted data belonging to 26 hospitals across the country with the Backmydata ransomware. The first affected was a children's hospital on February 10. Another 74 medical facilities connected to this system were isolated for analysis and protected.

MARCH

- **Critical VMWare security patch:** VMware has been forced to patch a set of vulnerabilities **even in affected product versions that were no longer supported.** The reason is the severity of the flaws discovered, some of them with a 9.3 out of 10 on the CVSS standard scale. **The bugs are related to the USB driver that allows virtual machines to access guest hardware as if the guest were directly connected to the virtualized system.**
- **NIST NVD enrichment bottleneck:** NIST's NVD (National Vulnerability Database) released an announcement on February 15 that it is establishing a consortium to address resource challenges within the organization. Following that announcement over the subsequent weeks NIST only **enriched 59 CVE entries, leaving over 2,100 vulnerabilities without any**

description or context. The impact is considerable in the security community, as NIST is the primary publisher and enricher of CVEs and thus a central part of many current security systems.

- **EU AI Act:** The European Parliament passed the Artificial Intelligence Act in March, the world's first major act to regulate the use of AI. The law passed with 523 out of 618 votes. The new legislation **prohibits the use of AI applications that threaten citizens' rights. This includes biometric categorization, emotion recognition and predictive policing systems.** The EU's AI law includes exemptions, for the use of biometric identification systems by law enforcement agencies, under strict conditions.
- **Trello - Emails of 15 million users for sale:** An actor, using the pseudonym emo, put up for sale on a well-known hacking forum, data of 15 million Trello users with public and private user information: username, full names, and associated emails.
- **AWS - Denial of Wallet Attack:** A new attack method on AWS allows attackers to create several RANGE requests for parts of large files (>1GB) before quickly canceling the request. **This bills owners for the entire request, which can result in up to 50x cost amplification.**
- **Cryptocurrency thefts continue their steady trickle:** as an example, during March, an attacker **stole $6.5 million worth of cryptoassets from cryptocurrency trading platform Seneca.** The company confirmed and attributed the attack to a vulnerability in its smart contracts. Seneca recovered 80% of the stolen funds after allowing the attacker to keep 20% as a "white hat hacking effort," whatever that means.
- Researchers at the Georgia Institute of Technologies (Atlanta) published a study analyzing the possibilities of executing remote attacks similar to the Stuxnet malware against current systems. The researchers developed a malware designed to exploit PLC websites as an entry vector to prove their theory. After gaining access, the malware attempts to abuse PLC web APIs to disrupt running processes or modify them, causing damage to the hardware.

APRIL

- **Critical vulnerability found in XZ:** A critical vulnerability CVE-2024-3094, **CVSSv3 10 out of 10,** was detected in versions 5.6.0 and 5.6.1 of the XZ compression utility and its associated liblzma libraries. The malicious code, not present in the public Git repositories but hosted in the tarballs of the official releases, was intentionally inserted by a contributor to the project and **represents a significant threat against Linux systems by manipulating elementary authentication processes used.** Everything points to the preparation of a massive supply chain attack.
- **Chromium V8 Sandbox:** After three years of waiting, the V8 sandbox, Chromium's JavaScript engine or, in other words, that of almost all browsers except Firefox, is here. This is very relevant because it allows to extend the sandbox to a still vulnerable place in the browser. In fact, between 2021 and 2023, 60% of the vulnerabilities in Chrome that ended up in exploitation and code execution were caused by memory corruption in V8.
- **Malware distribution:** Cybercriminals are using **comments in GitHub issues to host**

malicious files in the official repositories of legitimate companies. The attack consists of creating an issue in an official project and uploading the malicious file as a comment, but not reporting the issue. The issue is never active or visible to the project owner. **The URL of the file will trick users into thinking it is an official file of that project,** even if it was uploaded by an attacker.

- **Chrome Incognito Mode:** Google settled a class action lawsuit and has agreed to delete user data it collected through the Chrome browser's private browsing mode. **The company was sued for violating user privacy in 2020** after users discovered that Google was tracking their movements even in private Chrome browsing sessions. **Google settled the lawsuit after the plaintiffs allegedly sought $5 billion in damages. As part of the settlement, Google will also redesign Chrome's private browsing mode.**
- **LastPass Deepfake Incident:** A threat actor used a deepfake recording of its CEO in an attempt to trick one of its employees. The employee did not fall for **the scam because the request came via WhatsApp, an unusual business channel.**
- OpenAI's Voice Engine technology, capable of cloning voices with just 15 seconds of audio, has been deemed too risky for widespread release due to disinformation concerns and also that the **UK has pledged to introduce laws making the creation of explicit deepfakes without consent a crime.**
- **Cryptographic flaw in PuTTY:** A team of German academics has discovered a cryptographic vulnerability in PuTTY, an extremely popular SSH and Telnet client for Windows users. The vulnerability allows attackers to observe cryptographic signatures and retrieve a user's private key. The **main impact of the vulnerability is on source code repositories if they have been managed through a client that integrates PuTTY.** Attackers can look at a project's past public signatures and then determine a developer's private key, this **opens the door to supply chain attacks where threat actors can send signed malicious code to legitimate projects**.
- CISA issued an emergency directive on April 11 requesting to look for signs (IoC) of compromise from the APT Group “Midnight Blizzard“, which managed to reach Microsoft's corporate network and accessed correspondence from several U.S. government agencies.

MAY

- **Microsoft Secure Future Initiative:** Following the incidents related to Midnight Blizzard earlier this year, Microsoft, in an article published this May, details the acceleration and extension of the SFI (Secure Future Initiative) within the company following recommendations received by the U.S. State Department's cybersecurity committee. An important detail is that Microsoft is willing to make a strong commitment to ensure its proper execution through a **modulation of Microsoft's leadership compensation**
- **Malware on Android:** Malware keeps coming to Google Play. **90 apps** were **found that had managed to install themselves on 5.5 million Androids.** All of them resulted in infection with Anatsa (or Teabot), an Android banking Trojan that can steal information from 650 banks worldwide. Since the end of 2023, this campaign has reached 150,000 apps on Google Play.

Moreover, almost all of them disguised as "productivity".

- **Massive attack on Wordpress plugin:** A 9.9 severity vulnerability was disclosed in the WordPress Automatic plugin. The vulnerability is a SQL injection that could allow unauthenticated attackers to create administrator accounts and take control of a WordPress site. WPScan has logged more than 5 million attempts to exploit the vulnerability since its disclosure.
- **Ticketmaster is facing a class action lawsuit over a massive data breach:** Live Nation Entertainment acknowledged a data breach in a regulatory filing after an individual claimed to be selling data on 560 million Ticketmaster customers on hacking forums for $500,000. **It took Live Nation 11 days to confirm the massive Ticketmaster data breach.** The breach involved **unauthorized access to a third-party cloud database containing customer data such as names, addresses and credit card details**.
- **Ban apostrophes to avoid SQL injections:** A local government in the United Kingdom has banned the use of apostrophes in city street names to avoid problems with its computer systems. The best SQL injection protection we have heard of.
- **Cyber security education in the EU:** The EU's cyber security agency, ENISA, has published **guidance** on how member states can assess the **maturity of their cyber security training at primary and secondary school levels.** More information.
- Rockwell issued an advisory reiterating to their customers the advice to disconnect devices that are not specifically designed for public internet connectivity from the internet. In their advisory they explicitly cite "increased geopolitical tensions and adverse cyber activity globally" as the reason."
- The FBI announced the dismantling of the world's largest botnet, "911 S5". The US bureau arrested its creator, a 35-year-old Chinese national, who had infected more than 19 million devices. These devices were used to commit various crimes, including harassment, threats, fraud, and child pornography. The operation was coordinated by the U.S. DoD and the FBI but it also involved several law enforcement agencies around the world.

JUNE

- **Critical vulnerability in PHP for Windows:** The security flaw was registered as CVE- 2024-4577, CVSSv3 of 9.8 according to vendor, and is due to a flaw in the handling of character encoding conversions, specifically the "Best-Fit" function on Windows when PHP is used in CGI mode. The vulnerability affects all versions since 5.x and Shadowserver warns that **malicious actors are already starting to exploit the security flaw and that a PoC has already been published**.
- **Attacks on VIP TikTok users:** A cybercriminal appears to be using a 0-day exploit to hack into and take control of high-profile TikTok accounts. The malicious code is sent to victims via TikTok direct messages and **requires no user interaction except opening the message. Some of the larger hacked accounts include CNN, Sony and Paris Hilton**. TikTok announces that it has now fixed the zero-day vulnerability that allowed attackers to take control of accounts, so it is **highly recommended to make sure to update to the latest version**.

- **Controversial change in Adobe Photoshop's Terms of Service (ToS):** Adobe has been blocking access to its Photoshop application unless users **accept new terms of service that give the company full access to its content, the right to use it freely and even sublicense it to others**. After the wave of criticism received from some of the world's top creators, **the company is now implementing a new ToS that specifically clarifies that it will not use any customer data to train its AI**.
- **Information leak of the New York Times and its famous Wordle game:** An attacker posted a source code file and stolen data belonging to the New York Times on 4chan. **The leaker claims to have accessed the source code through a compromised GitHub token**, which was confirmed by the media outlet. **The leaked data allegedly includes source code for the company's public website, mobile apps and even its Wordle game**, the leak contains 270 GB of data, most of it unencrypted.
- **Microsoft's Recall feature:** Security researchers have proven how cybercriminals could steal data collected by Microsoft's Recall feature. **Recall, enabled by default in new Copilot+ PCs, allows Windows users to easily find previously viewed information on their PC through periodic screenshots**. Following the controversy **Microsoft has bowed to public pressure and is implementing changes to its Recall feature** in Windows 11. The feature will be shipped **disabled by** default for all Windows 11-compatible systems.
- CISA has notified participants in the Chemical Facility Anti-Terrorism Standards (CFATS) program that information including personal information and user accounts **may have been compromised following illegal access to the Chemical Security Assessment Tool (CSAT).** This access was possible thanks to the exploitation of a 0-day vulnerability found in an Ivanti Connect Secure device in January 2024. The incident could affect more than 100,000 people.

MOBILES

Apple iOS

The new iOS 17 security improvements

New iOS versions are traditionally released in the second half of the year. Still, that doesn't mean Apple is resting on its laurels. In this first half of the year, two major versions of iOS 17 have been released: 17.4 and 17.5 with little more than a month between them. Let's see what they bring us in the security section.

Note that version 17.4 prepares the operating system for the opening to third-party stores, promoted by European legislation (Digital Markets Act), which is designed to promote free competition. This constitutes an important turning point whose nuances in the security aspect remain to be seen.

17.4 brings us an improvement in the stolen device protection feature. In particular, when the iPhone enters this mode it will subject various actions,

such as accessing passwords and data, to authentication with biometrics. That is, if someone knows our passcode to the iPhone, this will not be enough and will request an additional biometric check to ensure that it is the rightful owner who is accessing the device.

Another curiosity is that if you try to change the AppleID of the device, you will have to wait up to an hour. During that time, the system will ask again for biometric authentication to ensure that the operation is lawful.

This technique is known as Security Delay. 17.5 brings us a curious functionality regarding privacy. If we remember, Apple Tags are devices which are quite useful for legitimate use. They allow us to easily find things like key rings, wallets, backpacks, etc. Even leaving them in a vehicle allows us to monitor its position in case of theft. The problem with these devices is that they cannot discern if the use they are being put to is ethical or if they are being used for illegal and questionable tracking.

From 17.5 onwards the system will warn us in case we are near an Apple Tag that is not known. The idea is that if we spend some time near that device (we move with it) it will warn us of the proximity and that it is active.

Next semester, iOS 18 will be published, foreseeably, since its development versions are already being tested and we will see what new features will bring us.

Vulnerabilities and versions released in the first half of 2024

We will review the security updates of the iOS operating system that the first half of 2024 has brought us. Let's remember that we left the previous semester with iOS versions 17.2.1, 16.7.4 and 15.8.

The release of new versions was extended until January 22. The year opened with 15.8.1, 16.7.5 and 17.3 versions.

Correspondingly, two, nine and twenty patches, of which nine fix vulnerabilities that allowed the execution of arbitrary code. It should be noted that the star component (most affected) is WebKit (Safari).

On February 8 we found 17.3.1, but it did not bring security patches. It was a set of bug fixes and improvements in the functionality of the systems.

On March 5, 15.8.2 was released with no security fixes. On the same day users of version 16 woke up to a group of security patches, and not a small one. Up to 19 vulnerabilities were fixed in 16.7.6, although only one of them was serious.

However, the highlight of the day was the release of the eagerly awaited version 17.4 with a fairly extensive list of security patches: up to 39 fixes. Four of them addressed the execution of arbitrary code.

March did not end without patches. On the 21st of that month, 17.4.1 and 16.7.7 were released with identical and serious fixes: patches for the WebRTC and CoreMedia components that allowed arbitrary code to be executed. March did not end without patches. On the 21st, 17.4.1 and 16.7.7 were released with identical and major fixes: patches for the WebRTC and CoreMedia components that allowed arbitrary code execution.

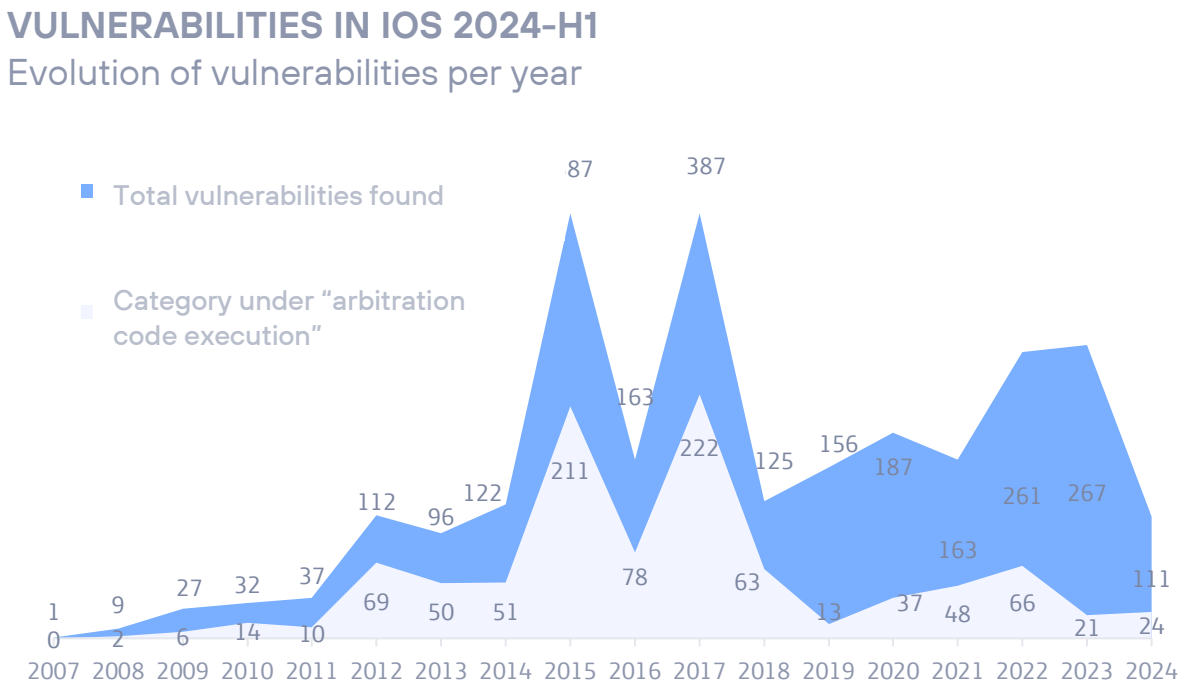
April was a quiet month, but May 13 brought a major update, no less than iOS 17.5, with 42 patches, 13 of them associated with arbitrary code execution.

Meanwhile, 16.7.8 was released with half of the patches, 21, seven of which were critical.

We closed the semester with the release of 17.5.1 on May 20, but it brought no security updates.

Evolution of vulnerabilities in iOS during the first half of 2024

The first half of 2024 has closed with 111 unique vulnerabilities patched, about two dozen considered high-risk, with the possibility of executing arbitrary code. It is already more than all the high-risk vulnerabilities found in 2023.



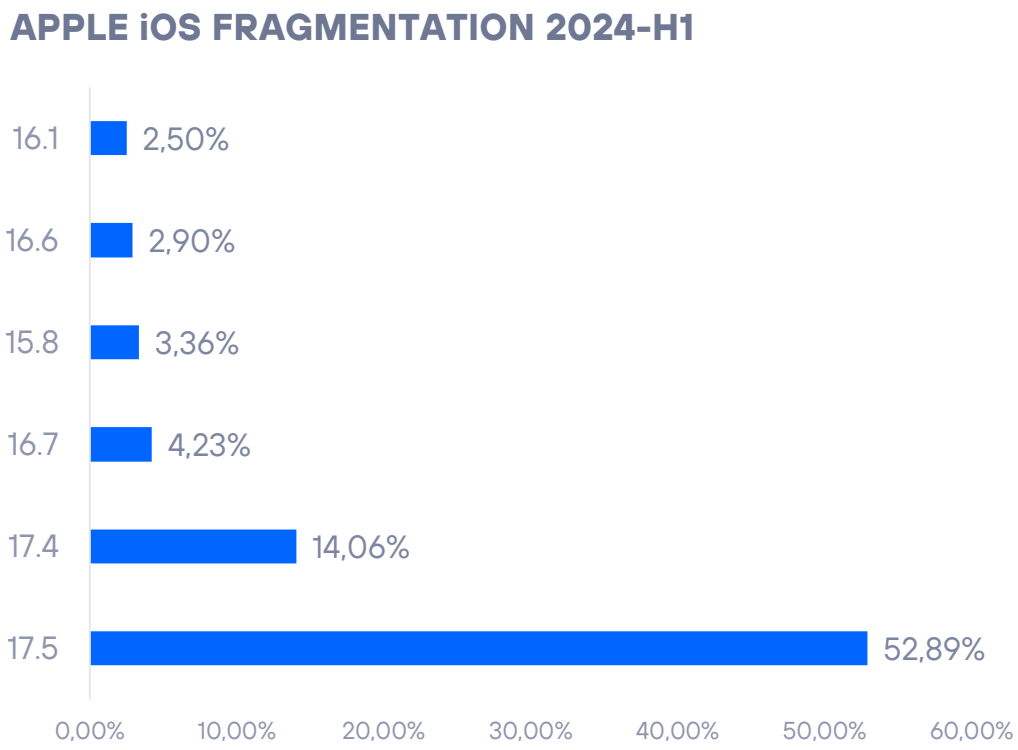
Version fragmentation during the first half of 2024.

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 publication time, so the figures below are from StatCounter.

As usual in Apple's release cycle, iOS 15 has practically disappeared with only a high of just over 3%, with versions 17 and 16 beginning to eclipse it, with 17.5 and 17.4 being the bulk of the iOS ecosystem.

Only the various sub-branches persist, coming from terminals from users who have not yet upgraded to higher branch versions.



Apple Transparency Report

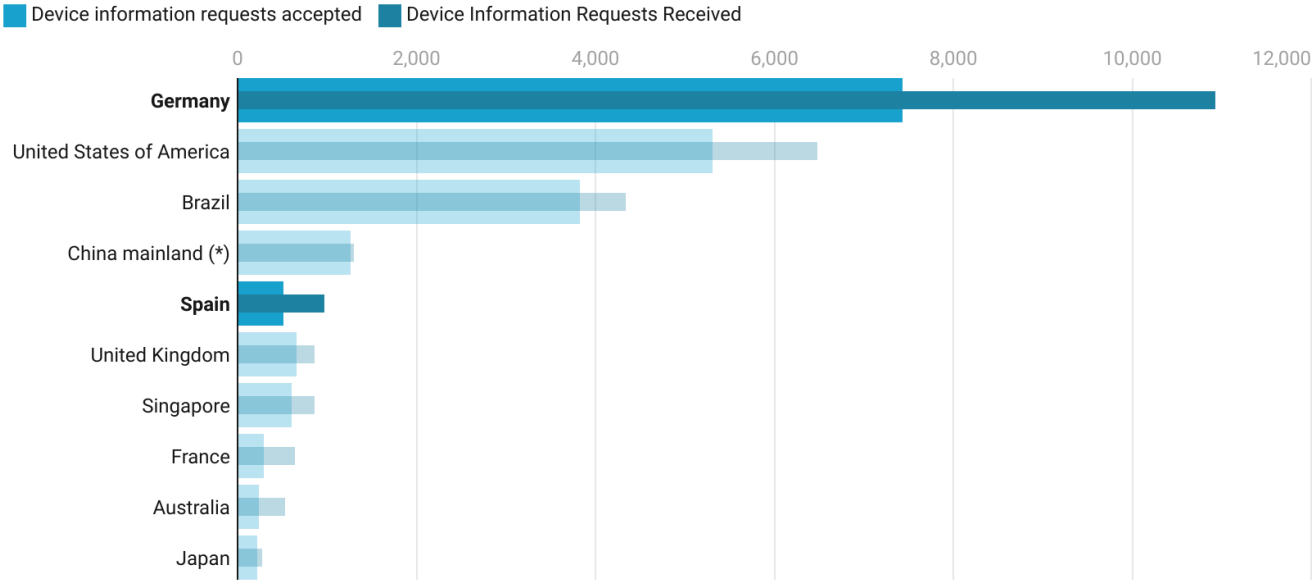
Governments sometimes need to rely on large corporations to do their job. When a threat involves knowing the identity or having access to the data of a potential attacker or a victim at risk, the digital information stored by these companies can prove vital to the investigation and avert a catastrophe. 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 provide here an update on some data we have extracted from the information published by Apple for the **second half of 2022 (the last published by Apple as of the first half of 2024)** 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. Requests may arise, for example, when law enforcement agencies act on behalf of customers whose devices have been lost or stolen. 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 continues to lead prominently in device information requests made in the second half of 2022.

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



Within this Top 10, the acceptance rate varies from 45% for Australia's requests to 97% for those corresponding to China. This leadership of Germany is also transferred for the first time to the number of devices on which it requests information, with more than 100,000 devices.

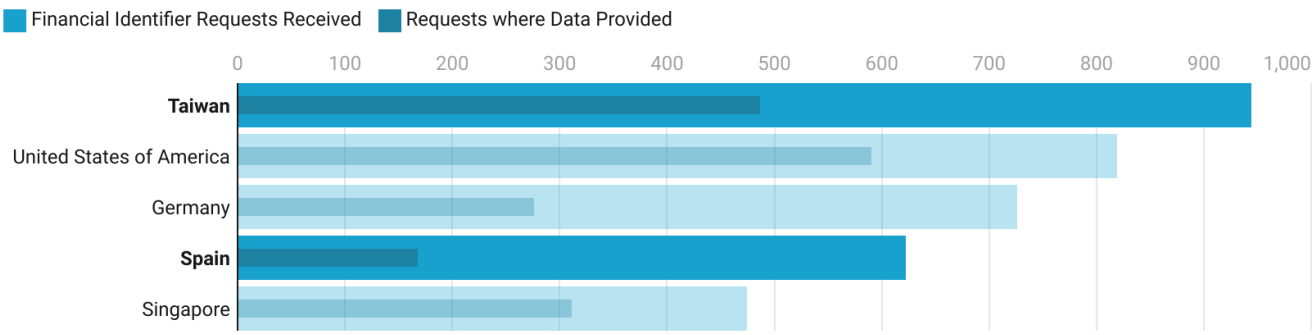
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Requests base don financial data

These requests occur 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.

Taiwan surpasses the United States in fraud information requests in the second half of 2022. Spain ranks fourth in the number of requests.

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



The acceptance rate among the top 5 countries with the highest volume varies from 27% for Spain's requests to 72% for those corresponding to the USA.

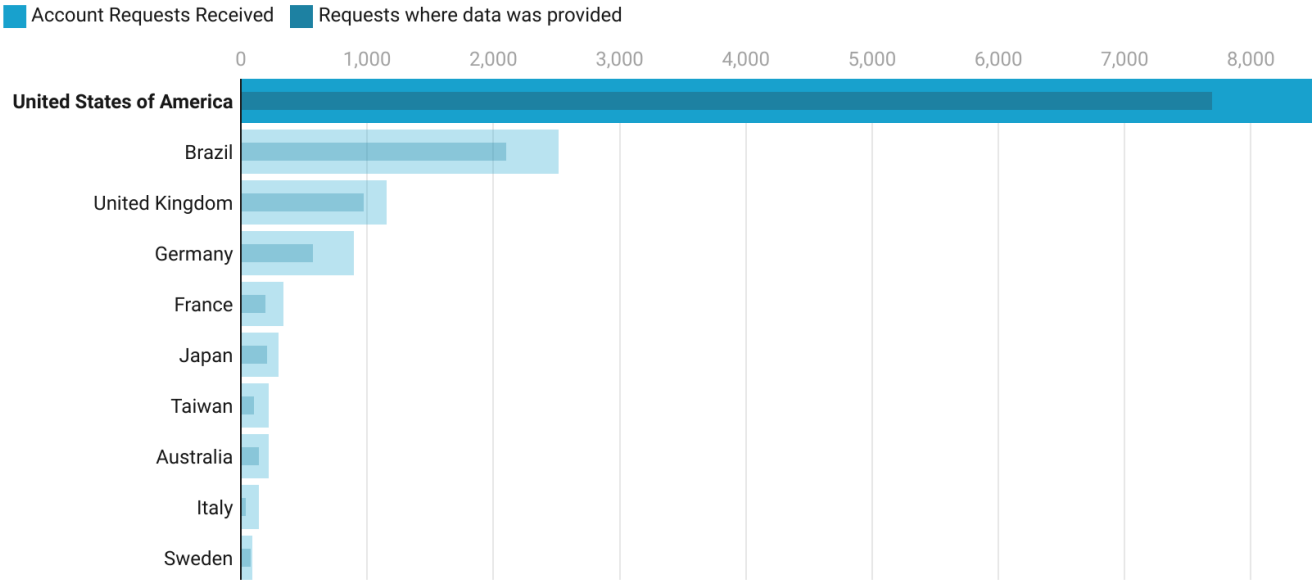
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Account-based requests

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

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

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



Of the 76 requests made by Spain, the eleventh country with the highest number of requests, only 33 were accepted (43%).

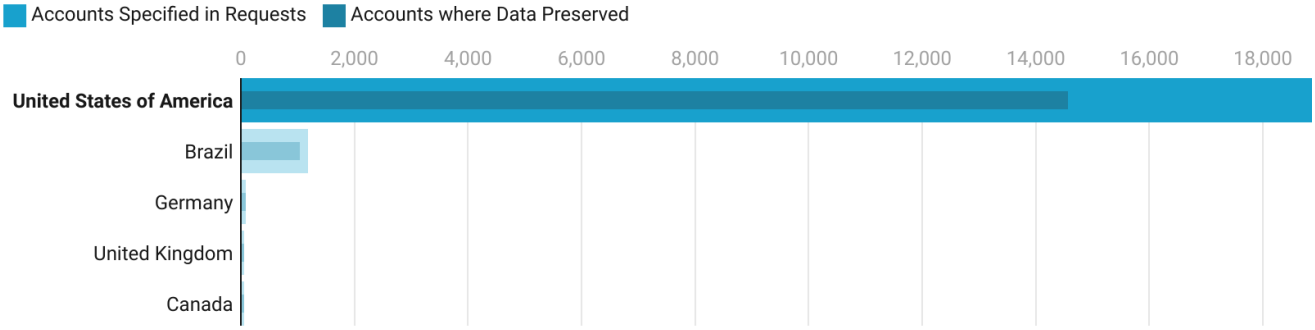
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Requests Related to Account Preservation

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 multiplies by more than 20 the 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 any account preservation request throughout 2022. Only the USA seems to use this capability effectively.

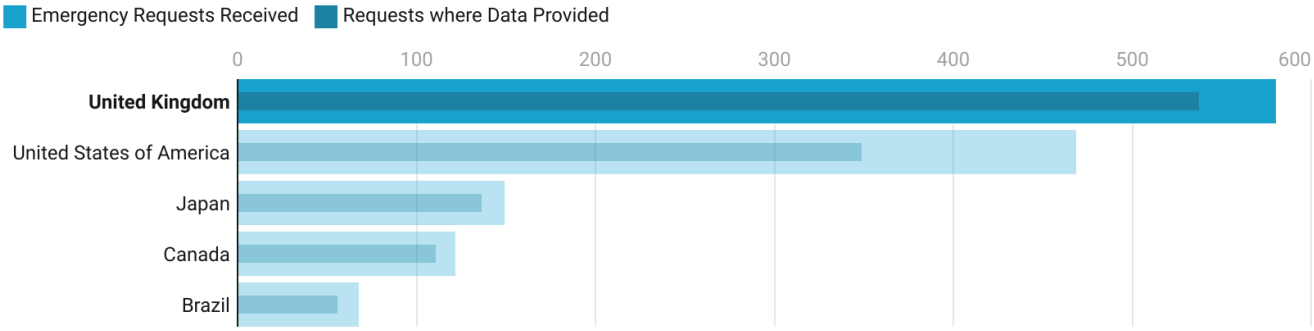
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Emergency Requests

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

UK once again becomes the country with the most emergency account access requests in the second half of 2022, closely followed by the USA.

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



Spain, which ranks 25th, issued 2 emergency account access requests and all were accepted (100%).

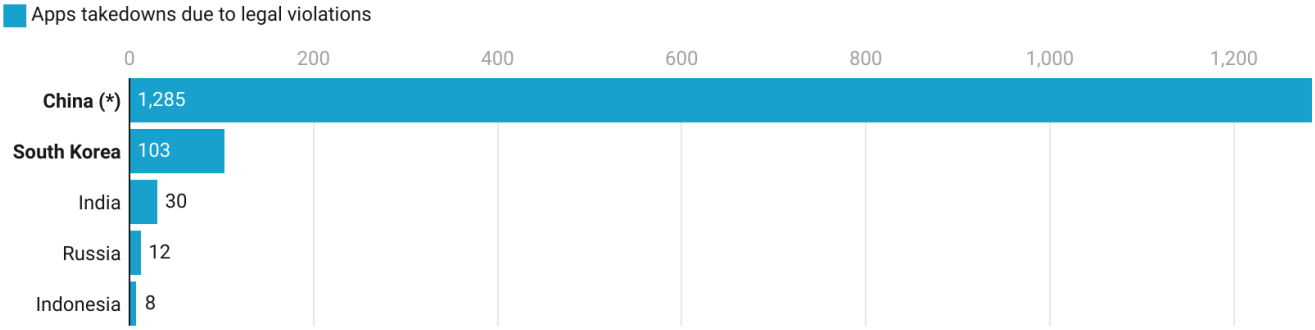
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Requests related to the removal of apps from the market

In mid-2024 Apple 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 interesting information, in this case on an annual basis (2023), which we will analyze below. In line with what has been analyzed in other biannual reports, we will begin by exploring the removal of apps that violate the sovereign law of the requesting country/region.Dando continuidad a lo analizado en otros informes semestrales, comenzamos por explorar las retiradas de aplicaciones que violan la ley soberana del país/región solicitante.

China requested 1,285 app removals from the market for legal reasons in 2023. South Korea has multiplied its requests by 10 compared to 2022.

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



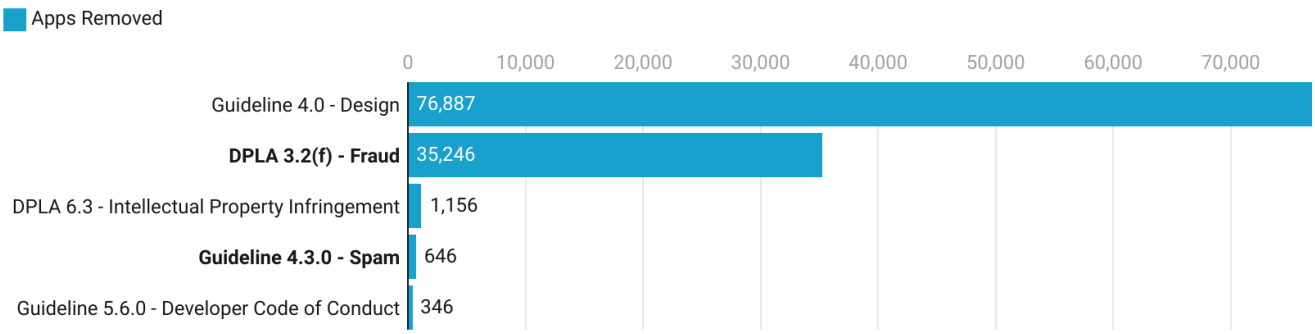
(*) 1,067 of those apps withdrawn by China are games that do not have the GRN license. (More info about GRN licenses: https://appinchina.co/how-to-get-a-game-license-in-china/)

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

The following is an interesting breakdown of app recalls both for non-compliance with Apple's internal regulations as part of the review process to reach the market and for non-compliance with Apple's app developer agreement.

Fraud and spam continue to be among the top five causes of app removal from the 2023 market for non-compliance with Apple's regulatory or development policies.

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



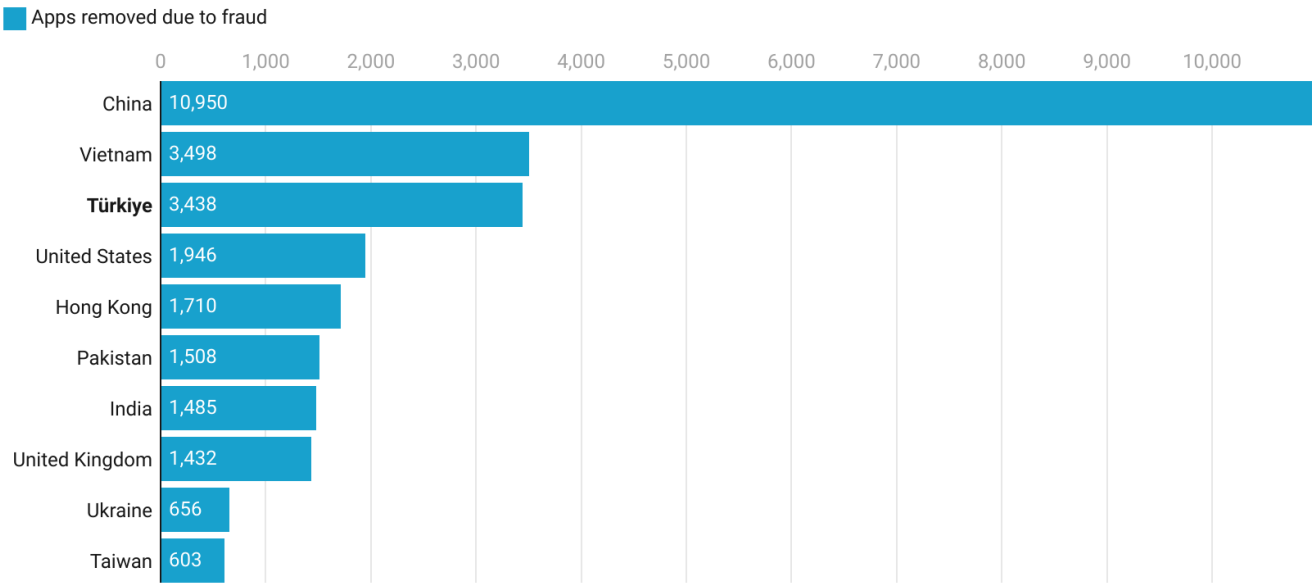
It is noteworthy that there has been a nearly 50% reduction in removals due to design issues compared to 2022. More info at: https://developer.apple.com/support/terms/apple-developer-program-license-agreement/ and https://developer.apple.com/app-store/review/guidelines/.

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

Focusing on the more cybersecurity-related categories, we can see a breakdown of the top 10 countries with the most spam and fraud breaches.

Top 10 countries with apps removed from the Apple Store due to fraud in 2023. Turkey has doubled its numbers compared to 2022.

Apps removed by country or region are shown.

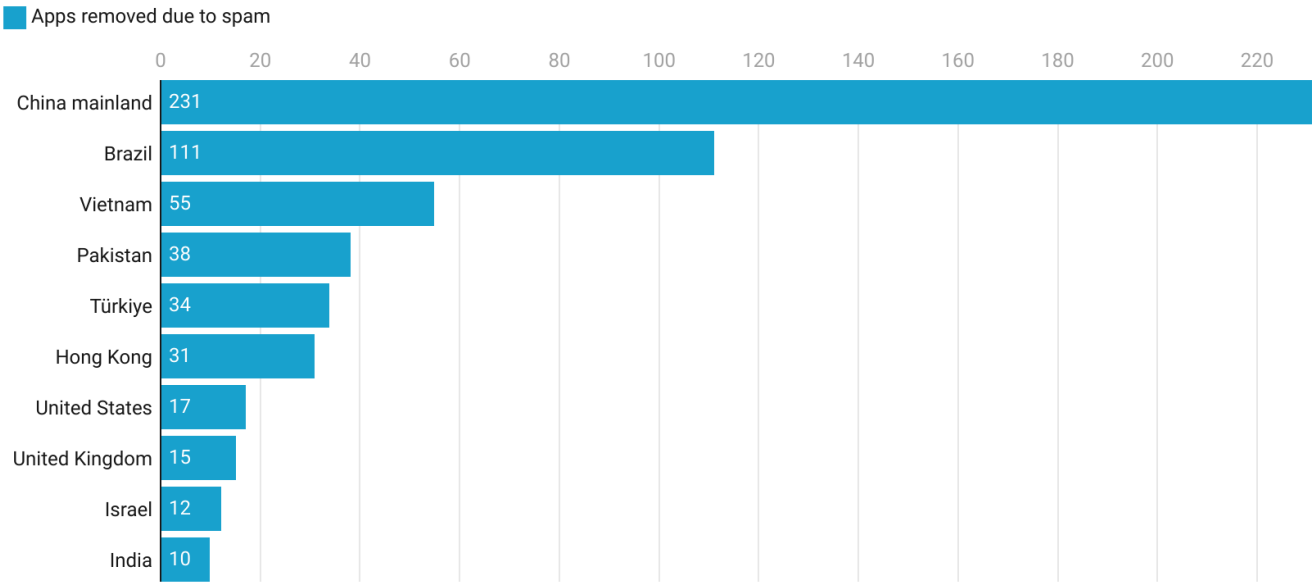


More info at: https://developer.apple.com/support/terms/apple-developer-program-license-agreement/#ADPLA3.2

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

Top 10 countries with apps removed from the Apple Store due to spam in 2023. No changes in the Top 3 compared to 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 we could also argue that it may be the case that justice works more swiftly there, or that there is more fraud 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 since we started tracking it. **This leadership extends for the first time in 2H2022 to the specific number of devices included in the requests.**

- **Taiwan overtakes the United States for the first time in requests for account information by fraud** in 2H2022. **Spain ranks fourth, albeit with a very low acceptance rate by Apple (27%).**

- The U.S. requests by far more than any other country for account preservation and access to the data housed therein. 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 given the volumes of account access in the U.S. This reinforces the theory that there is a procedure in place for launching such requests by the U.S. foreign department.

- China continues to be the country that requests the most app recalls 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 1,067 of the total of 1,285 apps withdrawn are due to games that do not have the approval of the Chinese regulatory body. **South Korea now occupies a prominent second position.** We will see if this is a trend or something merely incidental with Apple's next data.

- We see that, within the apps removed from the Apple App Store, **fraud and spam continue to be part of the "Top 5" categories of violations committed by developers in 2023 following the line of what was seen in 2022.** The decrease in violations related to design issues is striking, falling by almost half compared to 2022.

- It should also be noted that **Turkey has seen a 2-fold increase in the number of apps eliminated by Apple** for fraud, as in the case of South Korea, we will have to wait for the 2024 data to review its relevance.

***Note**: In this exercise we have graphed 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. Apple, for example, counts the number of requests for device information, and in turn each request can contain an undetermined number of devices in them. Same 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. For 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

We are still continuing with Android 14, which as of the time of writing this report has 54 revisions in total since its release on October 4, 2023.

Android 15 only exists in its beta form for development and is not expected to be released until after the summer, as per usual.

We don't have many updates on the security side beyond the released patches, but we can peek into the window of new features that Android 15 will bring soon in advanced.

The star feature is the new **privacy sandbox.** Google's bid to safeguard user privacy with tracking with restrictions on third-party cookies, etc., which is also intended for the web browser.

As it says on the Google website dedicated to this technology: "Our proposal is to bring Privacy Sandbox to Android and provide a clear path to enhance user privacy without compromising access to content and services free of charge...".

In the development section, the file integrity API (FileIntegrityManager) is made available to developers to protect the integrity of the files we choose via cryptographic signature.

In the next report, we will describe these new improvements and those that will come with the foreseeable release of Android 15.

Vulnerabilities

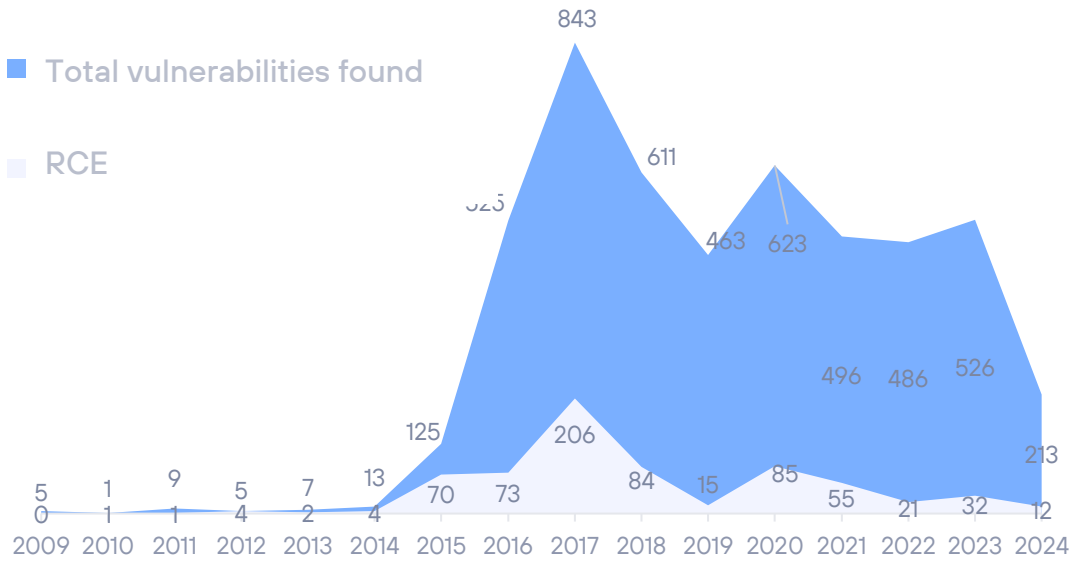
Android releases a set of patches every month, usually during the first week. In this first half of 2024 six bulletins had been released with a distribution of 59, 46, 38, 28, 29 and 13 unique patches or CVEs fixed per month.

In total, 213 patches (297 in the previous six months); 12 of them are considered critical (32 in the previous year).

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

ANDROID VULNERABILITIES 2024 H1

Evolution of vulnerabilities per year



Fragmentation on Android systems

Statcounter's latest release at the time of publication, indicates that the most deployed version of Android is Android 14, with a share of 25.64%, followed by 13 with a share of 22.29%.

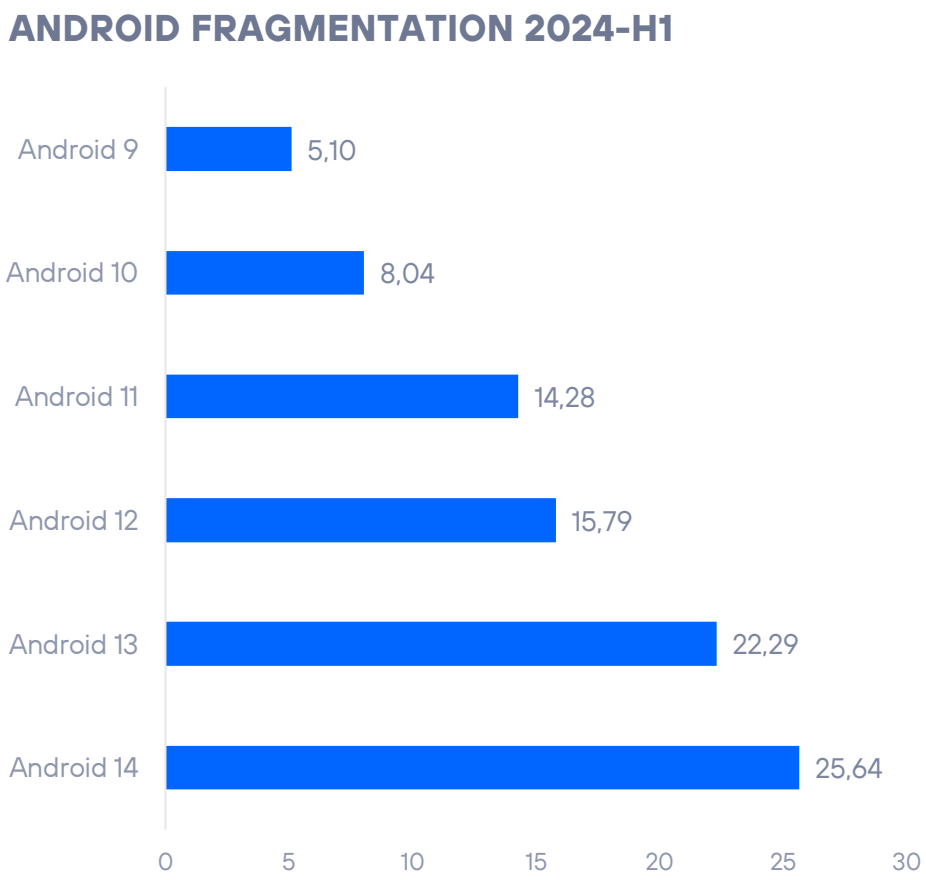
This is typically the peak of the current version, 14, released in October, which will begin to decline as soon as 15 is released, something that is happening to Android 13 which has dropped by just under 14 market share points.

Android versions prior to version 12 (including, system that appeared in September 2020) are no longer supported for updates.

This is a significant negative aspect: the existence of systems with no support at all but which continue to be in active operation without receiving security updates.

For instance, Android 12 still accounts for 15.79% of the pie (a good chunk) as does Android 11 with 14.28%. Between these two systems, which are, we repeat, unsupported, they represent 30% of the population with Android phones.

What's more, versions 10 and 9 still appear with 8.04% and 5.1% respectively. The rest of the unrepresented share (just under a not inconsiderable 10%) is held by even older versions, such as 8.0 and 8.1 Oreo and even 7.0 Nougat.



SIGNIFICANT VULNERABILITIES

Below are some of the key vulnerabilities of the first half of 2024.

CVE ID	TARGET	DESCRIPTION	SCORING
CVE-2024-4577	PHP on Windows	The 'Best-Fit' functionality in Windows when using PHP in CGI mode allows code execution.	9.8
CVE-2024-21764	Rapid Scada	An attacker could read sensitive files from the server, write files to the Rapid Scada directory (thus achieving code execution), gain access to sensitive systems and data, etc.	9.8
CVE-2024-21767	Access control system WS203VICM	This critical vulnerability could allow a remote attacker to bypass Commend WS203VICM access control by creating a malicious request.	9.4

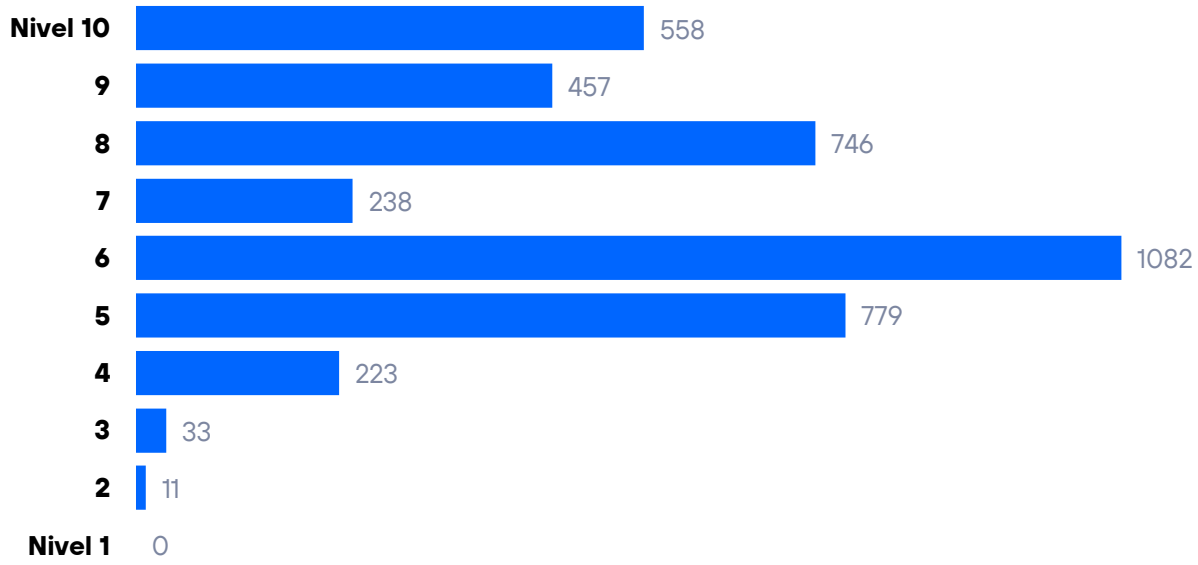
CVE-2024-21899	QNAP OS	Exploitation of this vulnerability allows an unauthenticated attacker to remotely access a NAS device.	9.8
CVE-2024-22252 y CVE-2024-22253	VMware Workstation/Fusion and ESXi	Exploitation requires local administrative privileges on a virtual machine but could allow an attacker to execute code as the VMX process of the virtual machine on the host. On Workstation and Fusion, this could result in code execution on the host machine.	9.3
CVE-2024-23897	Jenkins	A bug in args4j allows arbitrary file reads and thus code execution. A proof of concept was released.	9.8
CVE-2024-24691	Zoom - Windows	A flaw in the validation of input parameters in the Zoom for Windows application allows an unauthenticated remote user to escalate privileges on the host system.	9.6
CVE-2024-26305	ArubaOS	Buffer Overflow vulnerability on the "Utility" daemon that allows an unauthenticated attacker to execute arbitrary code remotely on the protocol used by Aruba to manage access points and wireless network monitoring systems.	9.8
CVE-2024-27322	Programming language R	It allows arbitrary code execution through specially crafted RDS and RDX files. R is a language widely used in critical sectors because of its ease of use for statistical analysis and data mining.	8.8
CVE-2024-27956	Wordpress Valvepress	The authentication mechanism of this plugin can be circumvented in versions prior to 3.9.2.0 to perform SQLi attacks that could lead to the creation of administrator accounts on the website.	9.9
CVE-2024-3094	Xz Utils	Versions 5.6.0 and 5.6.1 of this data compression library contain malicious code that can authorize unauthorized remote access via SSH using a payload that modified the OpenSSH server decryption routines to allow a remote attacker to authenticate.	10.0
CVE-2024-36266	PowerSys, controller of teleprotection systems for high voltage lines SWT 3000 Siemens	The affected application does not protect responses to authentication requests adequately. This could allow a local attacker to bypass authentication and thus gain administrative privileges for remote managed devices.	9.3
CVE-2024-37036	RTU Schneider Electric	An out-of-bounds writing vulnerability exists that could cause an authentication bypass when sending an incorrectly formatted POST request and particular configuration parameters are set.	9.8

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.

VULNERABILITIES RISK

Distribution of vulnerabilities by risk

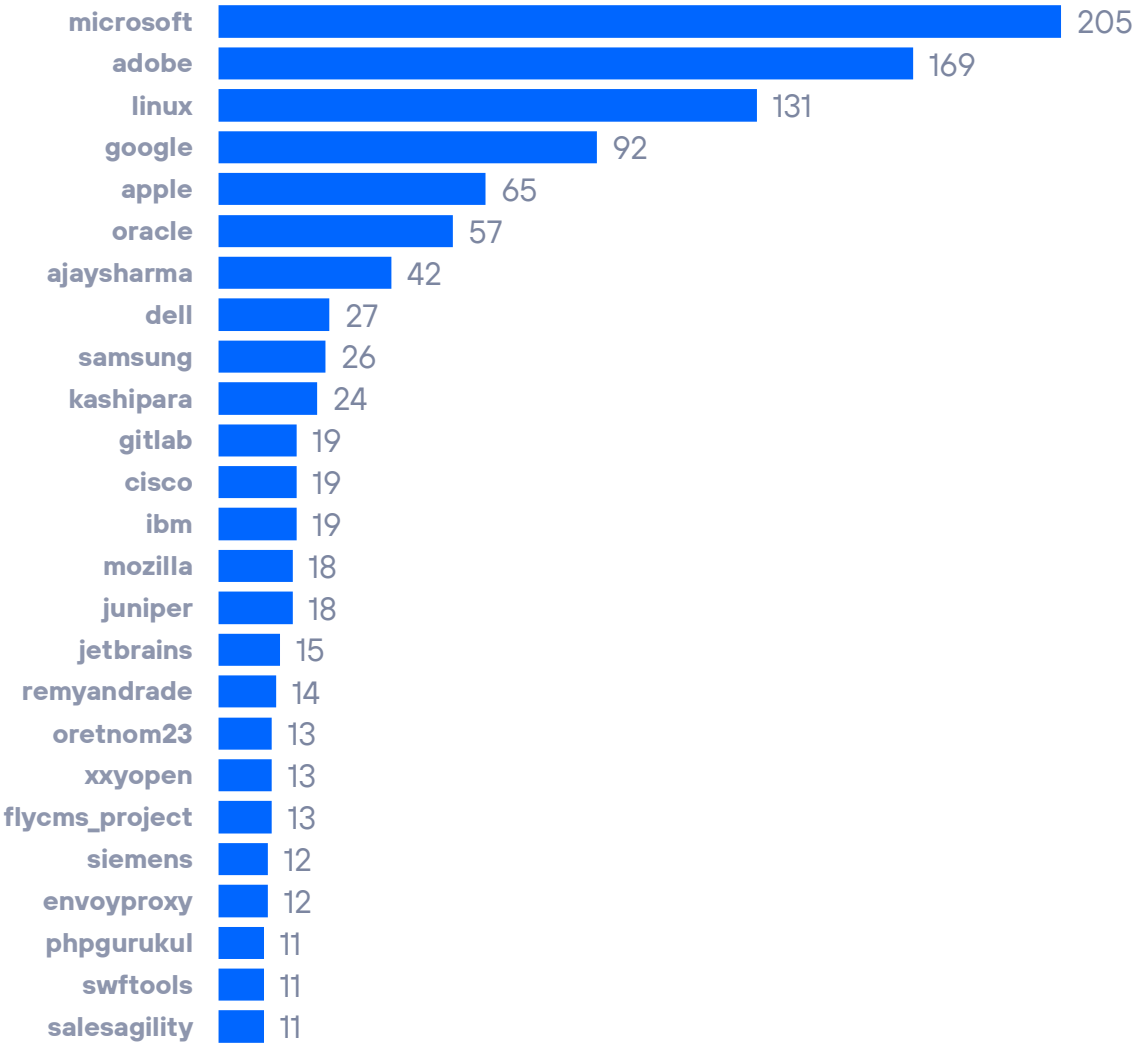


Top 25 companies with most accumulated CVEs

During the first half of 2023, Microsoft has led by far in terms of number of known vulnerabilities, followed by Adobe y Linux (in a generic way). Overall, it is usual that Microsoft, Google and Oracle are always among the first in number of vulnerabilities, but this semester we found that Adobe had a large number of bugs.

VULNERABILITIES BY MANUFACTURER

Top 25 manufacturers by accumulated CVE



APT OPERATIONS, ORGANISED GROUPS, AND ASSOCIATED MALWARE

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

We warn that the attribution of 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 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 in order to divert attention or harm them.

Significant APT activity detected during the first half of 2024

Sea Turtle - is dedicated to chewing on internet cables

This group, also known as "Teal Kurma" and "Cosmic Wolf") backed by the Turkish government, has been detected conducting multiple espionage campaigns in the Netherlands, targeting telecommunications companies, media outlets, Internet Service Providers (ISPs) and Kurdish websites.

Prior to this target shift, the group focused on the Middle East, Sweden, and the United States, using TTPs related to DNS hijacking and traffic redirects to conduct MiM attacks.

In its journey along Dutch shores, the turtle has shown particular interest in economic and political intelligence and specifically Kurdish interests and information.

Its TTPs are not particularly complex or novel. Initial access in the observed attacks is achieved by using compromised cPanel accounts to establish an SSH tunnel into the target infrastructure. They then use an open source shell for a reverse TCP connection to gain Command & Control capabilities.

More information https://www.huntandhackett.com/blog/turkish-espionage-campaigns

Cozy bear – Politically incorrect

Also known as "APT29", this group has been observed by Mandiant researchers using a new backdoor called "Wineloader". This backdoor was detected at the end of January 2024, but its use could not be associated with any known APT group. However, the target of the campaign in which it was used suggested that it could be APT29, which specializes in diplomatic targets and embassies.

A month later, this backdoor (a new version) was detected again in a phishing campaign against political targets. The messages posed as an invitation from the German CDU party to a dinner party in particular. The backdoor has features and functions commonly used in other APT29 tools, which ended up associating the campaign and the backdoor to this group.

Incidentally, Cozy Bear was the group behind the Solarwinds attack.

More information: https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties

Sandworm – Under the sand

The worm is back. The creators of Black Energy have been caught doing evil under the mask of hacktivism. In this case, the group has been detected employing several Telegram channels to amplify the communication of their actions through narratives close to state propaganda. However, we all make mistakes. The Telegram channels were sharing actions of the group that had already been carried out... until, at one point, one of the Telegram channels communicated an action that had not yet been carried out. At that point it became clear that Telegram channels and APT44 were the same (or very similar).

But why do it this way and not announce it directly? Mandiant's researchers explain that it looks like a test transmission of information to fake popular support for this type of action by APT groups sponsored by states and their intelligence services. We are social animals. Something contrary to our way of thinking but supported by an important part of society generates less rejection

or more doubts than that same “something” supported by nobody or almost nobody.

Welcome to the hybrid strategies of narrative control.

More information: https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-pose-as-hacktivists-in-water-utility-breaches/

Unfading Sea Haze - Terror in the mist

It has taken six years, for the cyber security ecosystem to detect this group. Since 2018, it has been responsible for “visiting” military and government entities in the South China Sea area.

And how they have managed to stay hidden for so long, two concepts:

On the one hand, this group shares characteristics with APT41, but has differences that clearly distinguish it from our already known “Double Dragon”. This sharing is, on the other hand, something common in state-sponsored groups.

On the other hand, they work fine. They start with well-prepared spear-phishing campaigns, abuse legitimate services (installing malware without a downloaded file, compiling from memory with MSBuild) and use proprietary tools. Combine that with patience and the ability to improve what already works, and you have a group that has been evading controls for a long time.

More information: https://www.bleepingcomputer.com/news/security/unfading-sea-haze-hackers-hide-on-military-and-govt-networks-for-6-years/

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 threats accessing the system.

Aristeo applies relationships and intelligence to go beyond the data, being able to proactively detect campaigns, targeted or sectorized attacks, 0-day vulnerabilities, etc., thanks to the information from all the devices deployed in the different node-signature.

Each node-signature has its own characteristics and reproduces a different process. Therefore, protocols, devices, productive sectors... change in each of them.

In addition, 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.

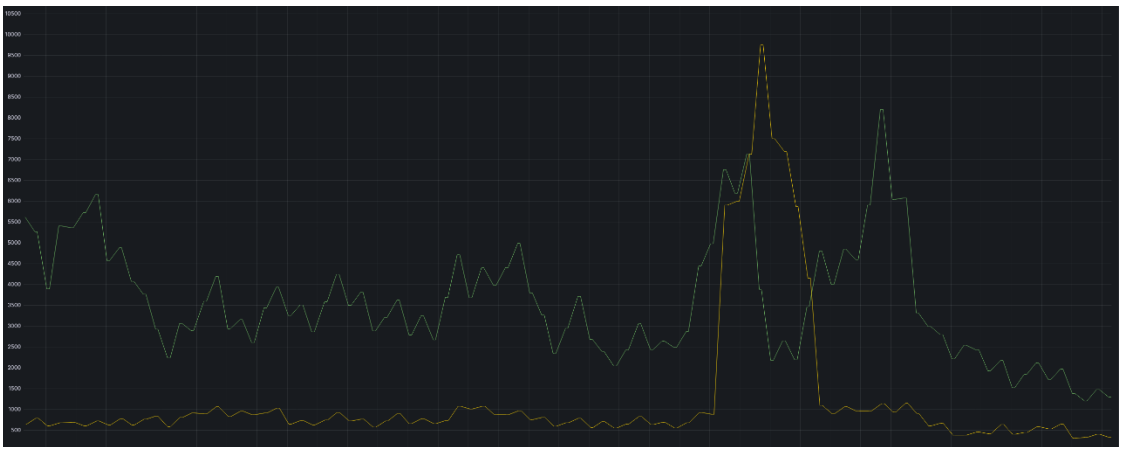
This variability may generate slight discrepancies in the data shown in this section when compared between semesters.

Information analysis

We will now comment on a campaign that we found particularly interesting, focusing this brief analysis on the country with the highest number of registered actions: Bulgaria.

Discovery campaign

Aristeo detected an unusual behavior within its decoy network on May 22nd:



The activity seen in the graph is an extension of Aristeo on the first two decoys where the activity anomaly was detected. We will not give more data on both decoys, but let's just say that each was receiving interactions as one would expect. Increases, decreases... all within the "normal" that can be the landscape of cyberattacks globally. However, from May 22 onwards, there was an anomalous increase in activity. In one of

them, the campaign has two distinct peaks, while in the other, with much less activity, the increase is more than appreciable. The campaign ended on July 3.

The origin of the campaign? The epicenter was detected in Bulgaria, but countries further east also increased their activity.

Ranking	Before		Campaign		After	
#	Country	%	Country	%	Country	%
1	The Netherlands	36.58	Bulgaria	30.28	USA	39.16
2	USA	27.55	USA	19.91	China	9.90
3	Bulgaria	8.57	Russia	14.27	The Netherlands	8.92
4	India	5.70	The Netherlands	11.31	Russia	8.27
5	China	5.69	Brazil	6.65	UK	6.50
6	UK	4.59	India	3.94	India	6.45
7	Russia	3.69	China	3.87	Bulgaria	6.22
8	Ireland	2.80	Hong Kong	3.65	Ireland	5.03
9	Germany	2.40	UK	3.56	Singapour	5.00
10	Vietnam	2.30	Ireland	2.57	Bahrain	4.54
AVERAGE	186.376,50		294.319,38		172.225,44	

It can be seen that the average number of events before and after the campaign was similar, but during the campaign it increased by 58%. If we look at the countries that most increase their representativeness in the Top-10 countries with the most events, we see that Bulgaria far exceeds the limits of what was expected. The fact that the average number of events increased by 58% and its representativeness rose from 8.57% to 30.28% indicates the magnitude of the campaign. Another country that has significantly increased its representativeness is Russia, although not in the way that Bulgaria has done.

Targets and type of activity? All of the above. Although the pattern of detection in both decoys is different, there is no apparent reason for this to have happened, beyond the fact that the type of exposure of each decoy (because they are not very similar) has determined the way of arrival of the registered origins.

Port of destination	Counting	Servicio-Exploit
8728	4.485	MikroTik Router - CVE-2023-30799
445	3.169	Samba
1900	1.284	SSDP
27017	1.049	MongoDB
23	658	Telnet
3306	501	MySQL
8443	448	Apache Tomcat
80	376	Http
22	345	SSH
3389	318	RDP
53	262	DNS
5432	239	PostgreSQL
443	220	TLS
2222	214	Cognex In-Signt
222	202	Miscellaneous
22222	195	Miscellaneous
8080	181	Web proxy server
3128	173	Web proxy server
8888	171	Miscellaneous
8088	165	Miscellaneous

These are the ports and services that aroused the most interest, but not the only ones. They searched for everything in all the Aristeo lures that were active. By the way, when we say “everything” it's because they didn't do an intelligent analysis of the targets beforehand. Some of the services and/or vulnerabilities they

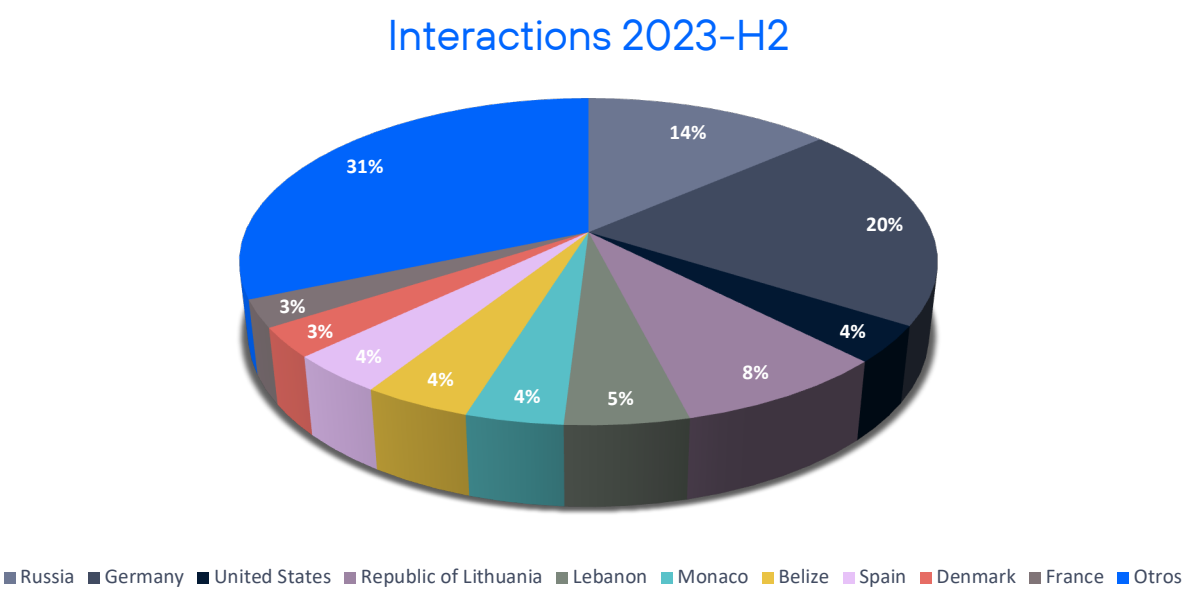
tried to exploit did not make sense for the simple reason that **the technology was NOT present in the decoys**.

Although we cannot know reliably what intentions the organizers of the campaign had, relatively short interactions and looking for any service that may be of interest, without having done prior footprinting or fingerprinting, could indicate a campaign to make a survey of opportunities that can be exploited later.

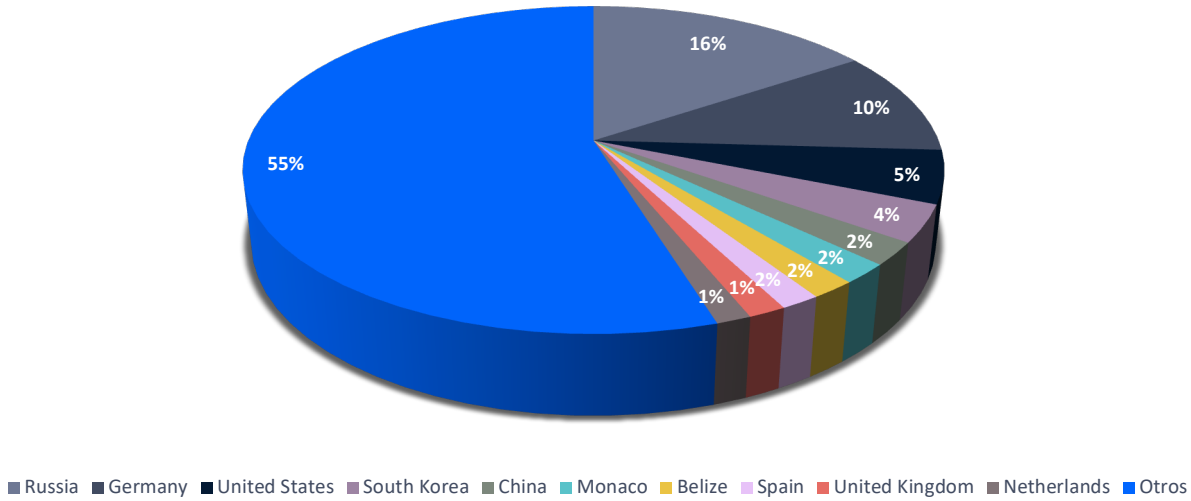
We will see.

And now, let's move on to the general statistics of the information recorded. In the first half of 2024, **more than 313 million cyber security events** were detected. This is down slightly from the data recorded in 2H2023, 322 million, and up from 2Q2023, when just over 300 million events were recorded. However, the figures remain in very similar ranges.

The distribution by country is as follows:



Interactions 2024-H1



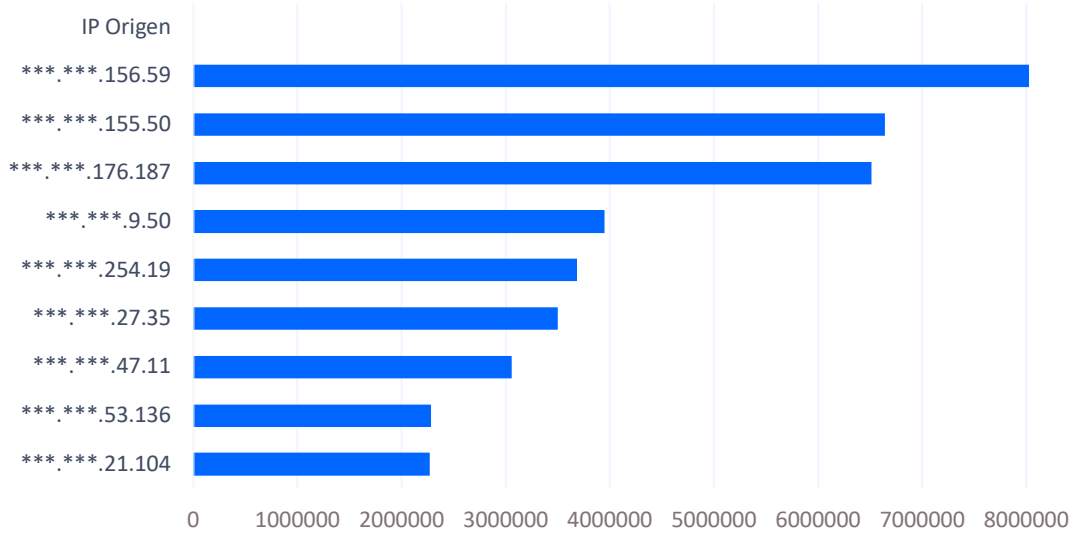
Although the dispersion of previous years is generally maintained, something curious has happened: there has been a clear loss of representation of the Top-10 in the total number of registered events. While in the last semester they agglutinated 183 million events, in this semester the Top-10 has registered 141 million events. This decrease, 23% less taking into account the total number of events in each semester, is quite significant. The Top-10 is usually a fairly representative scale of the total number of events (which is why we select it and show it in the half-yearly reports). It is a significant change that the Top-10 has lost 23% of its representativeness from one semester to the next and must be interpreted correctly.

Where have the missing 36 million or so events gone (we will see them in the last graph)? Obviously, distributed among the rest of the countries. 88 this semester, out of the Top-10. Moreover, there is no country or small group of countries picking up these events, indicating that this is not a specific campaign, but a clear **increase in activity at a general level worldwide**.

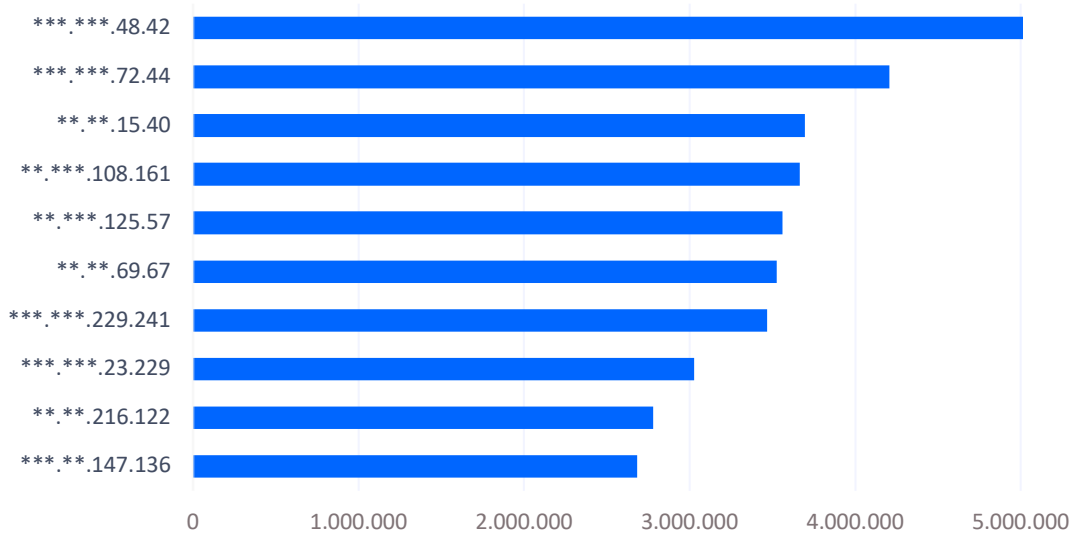
While we have stated that 9 million fewer events were registered this half year, that is a decrease of about 3% among all registered countries (98 countries this half year), which is a very low figure and almost non-representative of event registration in half a year. There are many reasons for this small variation. However, the fact that the Top-10 countries with the most events have lost a whopping 23% of representation from one semester to the next and that, in addition, the overall activity has not decreased significantly, surely has a lot to do with more or less notorious activity such as the discovery campaign that we discussed earlier in the document.

Now let's take a look at the top ten IP addresses with the most interaction with the Aristeo system. In this half year, 85% of the top 10 IPs registered in our system come from central-north-eastern Europe. Those who have read the previous report will already know why, but let's explain it. How can we 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. This has been the case in 70% of the Top-10 this semester, with several European service providers managing IPs located in other European countries than the provider's own. However, one of these Top-10 IP addresses is located in a European country but managed from a Caribbean country.

TOP-10 IP attackers 2023-H2



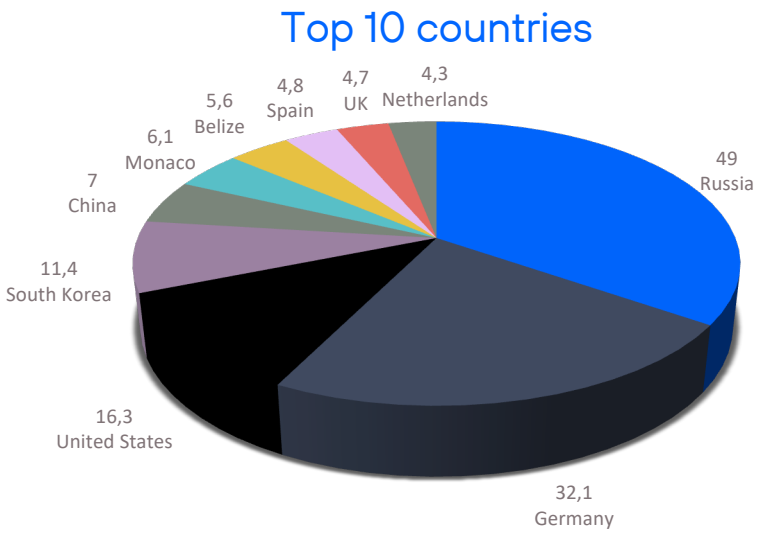
TOP-10 IP attackers 2024-H1



If we look at the data, as in the analysis of the Top-10 countries, the Top-10 IP addresses with the most activity lose representativeness compared to the previous semester. We are talking about a less significant percentage a priori than in the case of the analysis by country, but we must bear in mind that the results analyzed by country are normally distributed among approximately 100 countries (98 this semester) and if we analyze them by attacking IP, we are talking about thousands (and thousands, and thousands...).

In the IP analysis we have observed these movements before, but, together with what we have already seen, the data reinforces the analysis we are talking about. The more "equitable" distribution of hits on the Aristeo network together with an insignificant decrease in the total number of events indicates an overall increase in interest.

Below, we can see how the top 10 registered countries are distributed. Asian influence has increased this semester, with South Korea and China (which dropped out of the Top 10 last semester) as the top representatives.



Let's take a different approach to the representativeness of the Top-10 countries. In this case we can see that the total decrease of events from one semester to the other has been 47.7 million events. If we take into account that the overall decrease was only 9 million, as we indicated above, the other 36 million lost must have gone somewhere.

Answer: to the rest of the countries outside the Top-10.

#	2023H2	2024H1	Difference
1	56,3M	49 M	-7,3 M
2	37,5 M	32,1 M	-5,4 M
3	23,3 M	16,3 M	-7 M
4	13,4 M	11,4 M	-2 M
5	11,7 M	7 M	-4,7 M

6	10,7 M	6,1 M	-4,6 M
7	10,6 M	5,6 M	-5 M
8	10 M	4,8 M	-5,2 M
9	8,1 M	4,7 M	-3,4 M
10	7,4 M	4,3 M	-3,1 M
Total descrease			47,7 M

The decrease reinforces, once again, the idea of increased activity at the global level. A decrease of 9 million events in the entire network cannot justify the loss of representativeness of the Top-10 of 47 million, almost the same number of events recorded by the country with the highest presence in the Aristeo network.

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: 261.447 IP addresses, 62.740 domains y 346.811 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:

Malware Download	206081	59,99%
Phishing	129165	37,60%
Cobalt Strike	4148	1,21%
FAKEUPDATES	848	0,25%
GootLoader	759	0,22%
Coper	718	0,21%
DCRat	543	0,16%
Vidar	469	0,14%
Lumma Stealer	434	0,13%
Poseidon	387	0,11%

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.

However, they 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 1% 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.

Which domains are most commonly used by URLs marked as malicious?

We consulted Maltiverse this year to find out which domains appear most frequently in the URLs studied.

It is interesting to observe which services, mostly legitimate, are the most used by malware writers 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).

pages.dev	14465	30,84%
workers.dev	7816	16,66%
github.io	5371	11,45%
r2.dev	4559	9,72%
weeblysite.com	3735	7,96%
cprapid.com	3136	6,69%
vercel.app	2512	5,35%
vacationstoremiamibeach.com	1791	3,82%
blogspot.com	1773	3,78%
wordbracer.shop	1752	3,73%

Very interesting. "pages.dev" and 'workers.dev' are part of 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.

As can be seen and is the norm, sites related to free application development or infrastructure abound.

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

Before answering the question, it should be clarified that just because a country appears in this ranking does not mean that there is malicious intent with respect to 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.

USA	44607	25,69%
India	39523	22,76%
China	35095	20,21%
Russia	12509	7,20%
Germany	8663	4,99%
Venezuela	8375	4,82%
Pakistan	6789	3,91%
UK	6518	3,75%
Brazil	6466	3,72%
Singapour	5114	2,94%

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

What kind of maliciousness do IP addresses engage in?

Mail Spammer	124717	71,82%
HTTP Spammer	107102	61,67%
Malicious host	54875	31,60%
SSH Attacker	34800	20,04%
Malware download	26485	15,25%
Proxy	25002	14,40%
Suspicious host	16205	9,33%
Bruteforce	13879	7,99%
HTTP Attacker	13479	7,76%
Port Scanner	13205	7,60%

Crowning the top 10 ranking is the undisputed top 10: 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. These are also classic activities, such as 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 resolves 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.

This allows us to group the domains categorized as malicious by their highest level domain. The result of the top 10 is as follows:

com	16511	40,46%
dev	5997	14,70%
top	3613	8,85%
app	3350	8,21%
io	2782	6,82%
my.id	2292	5,62%
org	1852	4,54%
net	1578	3,87%
xyz	1438	3,52%
sn	1394	3,42%

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”. There is also 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 a part) and also, of course, to the IP addresses to which a domain resolves.

Finally, let's see how the top 10 of these have been categorized over the last six months.

Phishing	55113	92,06%
Malware download	1274	2,13%
Cobalt Strike	1003	1,68%
Cybergate	999	1,67%
CryptBot	387	0,65%
Poseidon	304	0,51%
Hydra	254	0,42%
AsyncRAT	200	0,33%
Lumma Stealer	167	0,28%
Hook	166	0,28%

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.

CONCLUSIONS

If in 2023 the vulnerabilities fixed on iPhone had reached their highest number since 2017, in the middle of 2024 they have already exceeded the number of those allowing code execution. **Android, on the contrary, seems to be on the path of reducing serious vulnerabilities**. If in 2023 there were 32, in the first six months of 2024 they have only 12 critical ones.

Regarding Apple's transparency report, this edition, **the German government has generated the most requests for device information** since we have been doing this monitoring. This leadership extends for the first time, in the second half of 2022, to the specific number of devices included in the requests. **Taiwan overtakes the United States for the first time in requests for account information by fraud in 2H2022**, Spain ranks fourth, albeit with a very low acceptance rate by Apple (27%). If Oracle, Microsoft and Google are the companies with more bugs corrected regularly, this semester sneaks in Linux, Adobe along with Microsoft, leaving Google and Oracle in fourth and sixth place respectively.

Concerning Aristeo, **more than 313 million cyber security events** were detected in the first half of 2024. This is down slightly from the data recorded in 2H2023, 322 million, and up from 2Q2023, when just over 300 million events were recorded. However, the figures remain in very similar ranges.

Something very curious is a significant decrease in the activity of the Top-10 “usual suspects” countries of origin of attacks. However, this decline reinforces the idea of increased activity at the global level. The answer is that, although the number of events in the most active countries has fallen, this activity has moved to other countries traditionally outside the Top-10, so malicious activity is more “spread out”.

The analysis of the Maltiverse data highlights the appearance of new TLDs among the most used for malicious activity: “my.id” appears very high in the ranking **and even manages to oust “biz” and “dev”.**

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.

CYBER SECURITY

El error del billón de dólares
Microsoft Secure Future Iniciative (SFI): redoble de tambores
SSDLC: La clave para un software blindado
Ataque a la cadena de suministro en Linux: A fuego lento
23 and me o sobre cómo no gestionar un incidente de seguridad
Ciberseguridad y el golpe de los 10.000 millones de dólares

ARTIFICIAL INTELLIGENCE

Ataques a la Inteligencia Artificial (I): Jailbreak
Ataques a la Inteligencia Artificial (II): Model Poisoning
Ataques a la Inteligencia Artificial (III): Data Poisoning
Ataques a la Inteligencia Artificial (IV): Privacy Attacks
Inteligencia Artificial aplicada a la Ciberseguridad industrial (OT)
Evaluaciones de impacto de derechos fundamentales sobre sistemas de IA de alto riesgo en el RIA

MALWARE

Malware distribuido durante entrevistas de trabajo fraudulentas
Distribución de malware: ficheros en comentarios de GitHub
'Living off the land': cómo los atacantes emplean tus propias herramientas en su provecho