Telefónica Tech

Security Status Report 2023 - H1

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

telefonicatech.com

Índex

EJECUTIVE SUMMARY

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

This first half of 2023 has been characterised, among many other incidents, by a bug that has caused quite a stir. It has been found in large corporations precisely to defend themselves. The bug, in FortiOS and FortiProxy with SSL-VPN enabled Fortigate, consists of a code execution problem and the danger is that the exploitation details were made public on June 13. It is known as CVE-2023-27997. It's not unusual to see this kind of serious problem from time to time. In this case it is striking that, although it has been fixed since 8 June, there are still 340,000 vulnerable systems remaining in July. The industry still needs to be more agile in patching critical systems.

Regarding the way of attacking, we have observed this semester how certain attacks via Google's ad network have come back into fashion throughout the semester. This technique makes it possible to reach any page with ads, legitimate or not, to distribute ads from there that may contain malware. It has been used in ransomware campaigns and Google has had to take action to minimise the problem. This kind of problem of malware distribution through ads is a classic problem from more than a decade ago.

A worrying trend was observed in February and appears to be on the rise. The Linux version of the Royal ransomware attacked VMWare ESXi servers. This is no longer incidental. Since 2022, malware for Linux systems has been on the rise, both in number and sophistication. Although they will never cause as much noise as Windows malware, it is interesting to see the trend of attackers in this respect. Linux malware allows them on the one hand to attack infrastructures that host virtual machines, for example in the cloud, and hijack the system base rather than individual machines. On the other hand, Linux-based systems tend not to have as many embedded monitoring tools or may even be more neglected by administrators in this regard. It is important to pay attention to any platform because it will be the weakest link for attackers to exploit.

Last but not least, OneNote attachments, which had gone completely unnoticed this year as an attack vector, have become a problem this year. Attacks on this format have continued since the beginning of the year and the industry, although late, has been able to react until they are monitored and detected like any other format. Attackers found that this format tricked users into opening the file and embedding executables in it in a hidden way.

This semester, in addition to maintaining our specialised section on industrial threat analysis thanks to our **Aristeo** project, we have Maltiverse as a reference platform to analyse the main IoCs in the industry.

Whether you are an amateur or a professional, it is important to be able to keep up with relevant cybersecurity news: what is the most relevant 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 understand its current state and project possible trends in the short term. The information gathered is largely based on the compilation and synthesis of internal data, cross-checked with public information from sources we consider to be of high quality. **Here we go**

HIGHLIGHTS OF THE FIRST HALF OF 2023

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

JANUARY

- New malware distribution campaign via Google ads. Attackers take advantage of the possibility of buying ads and placing them at the top of search results. Although Google removes them after a complaint, this is a manual process and therefore not very effective in the face of repetition. The main reasons for the increased use of this attack vector are a lower cost than spam bots, fewer defensive measures implemented in the process and the ability to target a specific group of users.
- The use of password managers is on the rise and this means that attackers are paying more attention to this type of system, as we saw last year with LastPass, and an upward trend in attacks on these critical systems is expected. This time it is Norton LifeLock that has released a statement about the potential compromise of user accounts in its password manager. The irony, in this case, is high, the attack was carried out through credential stuffing (reuse of passwords found on the DarkWeb in other services).
- Microsoft announces plans to block XLL files from the Internet in March. In its fight against malicious files, it will block XLL files coming from the Internet, mainly email attachments. XLL is an extension for Excel add-ins and basically a DLL (dynamic link library) file. It is not common for such files to be used as email attachments, as they are usually installed by administrators. However, because the XLL extension is linked to an icon similar to other Excel-compatible extensions, they can be confused with other Excel file formats by clueless people.
- A group of Chinese researchers have published a scientific paper claiming that they can (but have not yet) crack a 2048-bit RSA cipher using quantum computers. In this case, cryptography experts do not agree with the conclusion, but the combination of lattice base reduction through factorisation with quantum optimisation algorithms may be a real threat as higher-powered quantum computing becomes increasingly available.
- Data stored on Amazon's S3 servers will be encrypted by default as of 5 January this year. Although this option had been available since 2011, it required intervention by administrators to activate it.
- On 11 January, the hacktivist group "GhostSec" announced that it had managed to run ransomware on an RTU (Remote Terminal Unit) device in a Belarusian operation. This announcement is highly relevant, as it would be the first time that such malware has been successfully executed on a device as limited (and frequently used in industrial environments) as an RTU. The specific model was a "TELEOFIS RTU968 V2" and the modified files contained insults against the current president of Russia.
- Several research groups analysed the case and concluded that the attack vector could have been the SHH service deployed by these devices, with a preconfigured weak password. They also

searched a meta-search engine and detected 117 devices in the same area exposed and with the service activated.

FEBRUARY

- A Chainalysis study on the ransomware industry shows a decrease in payments made in 2022 compared to 2021. What does this mean and what are the reasons for this decline? This reduction is probably due to a combination of factors, two of which stand out: economy of scale, like any other business, makes it very difficult to sustain the growth rates that ransomware has shown in recent years, and attackers increasingly need to be a moving target in the face of increased surveillance, so they reorganise more quickly and are less durable (1 year to 2 months of life), which can also affect their ability to make an impact.
- Belgium joins a growing list of countries launching national vulnerability reporting programmes, with the aim of protecting researchers who are looking for vulnerabilities, but do not plan any malicious use of them. Belgium joins the Netherlands, France and Lithuania in Europe.
- DDoS record: Cloudflare has reported that it has mitigated the largest distributed denial of service attack to date this February, with more than 71 million HTTPS requests per second. This is 35% higher than the previous highest-ranked attack of 46 million rps (requests per second).
- Security is often not a priority for IoT devices. This month we have seen several examples that try to advance the provision of resources for the IoT sector: the American Institute of Standards and Technologies (NIST) has announced a set of lightweight cryptographic algorithms (Ascon) will become standard in 2023, Microsoft has opened the code of CHERIoT, a real-time operating system that follows the security-first precept.
- The National Court has finally granted the request of the US authorities to extradite a 23-year-old British man who allegedly took part in the famous hacking in July 2020 of numerous Twitter accounts such as those of Joseph Biden, Barack Obama, and Bill Gates.
- The exponential growth in popularity of chatGPT is attracting malware distributors. They are trying to capitalise on the hype to ensure the impact of their attacks. Kaspersky researchers have detected a fake Windows desktop version of ChatGPT used for malware distribution.
- The Dole food company, which specialises in the cultivation and distribution of fruit and vegetables, announced on 22 February that it had been hit by a ransomware attack. The attack disrupted the company's operations, causing the temporary closure of its packaging and distribution plants and, therefore, cutting off supplies to shops in the US. In addition to the shutdown of operations, mainly in its Chilean plants, the attackers also took company information, including data of certain employees. On 18 May, Dole presented its first quarter financial report and quantified the costs of this attack at 10.5 million dollars

MARCH

- The database of known exploitable vulnerabilities (KEV Database) of the US cybersecurity and infrastructure agency (CISA) has almost tripled from 311 to 868 entries by the end of 2022. A study by VulnCheck reveals that the vast majority of new entries are not for new vulnerabilities, but more than 80% are old vulnerabilities, with the oldest one dating back to 2002.
- Github has introduced for all its users a feature that allows scanning code repositories for secrets that may have been accidentally incorporated. The feature can be launched from the user's own Github profile and supports more than 100 API token formats.
- The cyber security company Netscout has published an analysis of the effectiveness of removing more rental services from DDoS attacks. The elimination by the end of 2022, in a joint action by Europol and the FBI, of more than 50 DDoS services has resulted in significantly fewer attacks. The continuation of this trend after three months also indicates the absence of new major players in this sector.
- Voice over IP software provider 3CX was compromised to launch a large-scale supply chain attack. Although 3CX has more than 600,000 customers, two factors meant that the impact was not huge. On the one hand, detection was very quick (weeks) from activation, for context at SolarWinds it took nine months. On the other hand, it was a highly targeted attack, targeting companies in the cryptocurrency space and not generalists.
- Microsoft has announced that it plans to progressively block emails from on-premises Exchange servers that are not properly patched and are “persistently vulnerable”

APRIL

- Samung ChatGPT leak: With the emergence of generative artificial intelligence, many employees have been seduced by the acceleration capabilities that these systems can provide and have not considered the potential privacy implications of their use. In particular, Samsung notified its employees this April to limit the use of chatGPT after detecting the publication of internal and restricted source code and documents for the detection of faulty chips.
- Also, in March we talked about the KEV (Known Exploited Vulnerabilities) database of the US agency CISA, as the company Rezilion has scanned the internet for systems exposed to the more than 800 vulnerabilities described in the database, and the results are not good. More than 15 million systems globally have been detected that would need to be patched to prevent a simple attack. The two most exposed vulnerabilities are, logically, associated with web servers (specifically Apache), but we can find surprising data such as the almost 200,000 systems exposed to Heartbleed, whose discovery is almost 10 years old.

- The lockdown mode launched by Apple in mid-2022 scored its first successes by stopping a 0-day attack, from the NSO group as reported by Citizens Lab in its analysis, which did not require any user interaction, on an iOS device with the functionality enabled. The victim was even notified of the exploit attempt on their handset at the time of activation.
- Uncommon but sometimes happening, HP has had to advise customers of some laser printers to downgrade the firmware on their printers, as the latest update introduced a data exposure vulnerability that they have not yet managed to patch. They expect to be able to release a new patched version within the next 90 days.
- Subscription trojans for Android continue to do damage following a Kaspersky study. This time it is a family of trojans known as Fleckpe. The malicious code hides in photo editing or wallpaper apps and acts silently by opening a browser in stealth mode to subscribe victims to premium services if confirmation with a code is required the app first requests access to notifications and reads them automatically without user interaction. The app then functions normally, increasing the chances of the attack going undetected for a longer period of time.
- Researchers from Bitsight and Curesec have discovered that the SLP (Service Location Protocol) used since 1997 by printers, computers, routers, etc. to facilitate service discovery can be used in DDoS attacks because of its high amplification factor of more than 2200, the third highest amplification factor known to date. This protocol is more oriented towards LAN use but is often exposed to the internet as it comes in the standard HW and SW versions. More than 70,000 servers have SLP ports exposed to the outside world according to the study.
- Every April, since about 10 years, the "OPIsrael" operation is activated. On 5 April, the Israeli postal service had to shut down some services due to a cyber-attack. Two days later, water controllers in the Jordan Valley were blocked and displayed an anti-Israeli message. Other, less sophisticated, actions involve attacks against university websites, transport services, government...

MAY

- Rapid Security Responses is a new mechanism that has been put in place on Mac systems that resembles Windows out-of-cycle patching. They try to speed up the mitigation of critical zero-days and other urgent security improvements. This speeds up the response and makes installation faster by not having to perform a full system update. They will be identified by a letter after the version e.g., iOS 13.3.1 would become iOS 13.3.1(a).
- Automattic, the company behind the Wordpress.com product, i.e., hosting service. It has forced the update on millions of websites that use the Jetpack plugin. Jetpack is one of the plugins it maintains and installs almost by default on every Wordpress, precisely because it prevents brute force attacks, makes backups, etc.

- It has more than 5 million active installations and at the time of publication there were no known active attacks on the vulnerability, found through an internal audit, in its API since version 2.0 (2012) and that would allow the authors of a site to modify any file in the Wordpress installation.
- The new TLD (Top Level Domain) .zip launched by Google has generated a lot of controversy in the cybersecurity field since many experts agree that it can trigger new attacks due to the familiarity of users with this type of compressed files. For example, using the Windows file explorer search engine, if a user searches for example.zip and does not find it, it will automatically open it in a browser that will reach this new TLD.
- Scalper bots is the name given to tools that try to automate the rapid consumption of a scarce resource on the Internet and then sell access to that resource to victims for a higher price or at a cost when it was free. For example, concert ticket scams, etc. In May, a botnet was dismantled in Spain that was dedicated to booking all appointments for asylum requests. They then sold the appointment bookings to foreigners who needed these services for a price between 20 to 300 euros when in fact it is a free service. Seventy people have been arrested in connection with the scheme.
- Academics at the University of Maryland have discovered that some devices seized by US authorities and not claimed by their original owners are being auctioned without being returned to their factory state or the data on the devices being wiped clean. This exposes the owners to possible crimes of extortion or leaks of sensitive information. Of the 228 units seized by police and purchased by investigators through the PropertyRoom.com website, they were able to extract social media messages, identification documents, bank accounts and cards, and even sexually explicit videos and photographs.
- The utopia of a password-free world seems a little closer after Google's announcement to introduce passkey support for personal accounts. With a passkey you can access your Google account by authenticating yourself on a local device, for example through biometrics.
- Mandiant identifies a new malware, called "CosmicEnergy", designed to disrupt the power supply by interacting with RTUs and communication systems based on the IEC-104 standard. Such devices are commonly used in Europe, the Middle East and Asia. The analysis reveals capabilities comparable to the Industroyer malware, which caused serious problems in Kiev in 2016. The team's research found a trace of a project called "Solar Polygon", which was a project developed by Rostecom-Solar, a Russian cybersecurity company that received a grant from the Russian government in 2019 to run training and incident response exercises. How this malware would have ended up outside of its legitimate use is a mystery.

JUNE

- TrendMicro researchers warn of the power of a malware obfuscation engine called BatCloak that virtually renders malicious code undetectable (FUD: fully undetectable malware) based on data from more than 750 samples. 80% of the samples obtained by the researchers in 2022 are not detected by any antivirus engine. This provides an ideal scenario for attackers to incorporate malware through batch files processed by BatCloak.

- Toyota has reported finding new exposed servers with customer data from 2015 and 2016 respectively, adding fuel to the fire, as it follows notification of the discovery in May of a database exposed with customer data in Japan for nearly 12 years.

- OWASP has published a draft of the Top 10 security risks associated with working with applications based on large language models (LLMs), the highest risk being prompt injection vulnerabilities that allow sophisticated input manipulations to cause an unexpected effect such as the disclosure of information or actions not authorised or intended in the application design.

- Microsoft attributes the cybercrime group Clop as the perpetrator of the attack on Progress Software's MOVEit servers. More than 100 companies have already been identified as affected by information theft or extortion after exploiting the zero-day SQL injection vulnerability (CVE-2023-34362). The attack shows a high level of professionalism with more than 2 months of preparation phase and an attack on the eve of a long weekend in the United States, the country with the highest number of active attacks. Censys shows between 2500 and 3000 MOVEit servers exposed on the internet so unfortunately it looks like the extortion division of the criminal gang is going to have their work cut out for them.

- Freaky Leaky SMS: A team of academics has discovered a new technique that can allow an attacker to determine the location of a mobile phone user with high accuracy. The timing attack involves sending several SMS messages and measuring the time between sending and delivery of the SMS delivery reports automatically generated by the telco serving the victim. The authors achieve 96% accuracy in some scenarios.

- Finally, Microsoft is going to change the default SMB configuration so that requests are signed. Although this option has existed since Windows 98, it was not set by default as it slows down information transfers. Without such a signature, "NTLM relay attacks" could be executed.

- On 3 May, Dallas, one of the 10 most populated cities in the US, was hit by ransomware that left the city's main services disrupted. A month later, on 9 June, city officials announced that they had made progress in restoring these systems to 90 per cent, although much remained to be done. The Royal ransomware attack knocked out libraries, animal shelters, security departments and other government services, online payment systems, water flow meters, etc. In addition, the attackers got hold of information that they later threatened to release if they did not receive payment in return.

MOBILE

Apple iOS

New security features

Apple announced new security and privacy measures on 5 June. These include the most noteworthy of them.

One of the measures is a lock mode in Safari's private browsing, which will allow the browser to be locked if Apple's native browser has not been used for a certain period of time. This is intended to prevent anyone with access to the device from being able to see which tabs were active in this mode.

The selection of photos to share with applications has been improved by presenting a dialog with more options.

A very fashionable aspect of user tracking via URL parameters has also been improved. On some websites, users are tracked via custom parameters that uniquely identify each user, Apple has improved the detection and filtering of these parameters, making them more difficult to use.

In addition, it will implement a mechanism to warn of explicit content in material shared via messages. This mechanism was somewhat controversial (in fact, its implementation was halted) as it was unclear how it was being implemented. We look forward to hearing more details about how this feature will work.

Otra característica es la de compartición de contraseñas entre contactos conocidos y autorizados desde un dispositivo. La idea es más la posesión de contraseñas que todos pueden ver, usar y cambiar. Una característica que soluciona ciertos problemas de usabilidad pero que está por ver como se desenvuelve, desde el punto de vista de la seguridad, en un uso real.

Finally, an interesting fact. If you have changed your password on an iOS device, there will be a 72-hour grace period during which your old password will still be valid. No doubt a measure that perhaps comes from the high percentage of users who forget their new password.

Vulnerabilities and new releases

We take a look back at the security updates for the iOS operating system that the first half of 2023 has brought us.

iOS 16.3

It's January, we come from iOS 16.2 and with one month to go Apple is releasing the third revision of the current branch of its mobile operating system. On the 23rd of the first month of 2023, iOS 16.3 sees the light of day. This time it comes with a batch of 17 CVEs or patched vulnerabilities of varying severity.

Among the 17, those corresponding to the HTML Webkit rendering engine, three in particular, which could allow the execution of arbitrary code by simply visiting a malicious web page, could be of some danger.

iOS 15.7.3 y 12.5.7

On the same day in January, version 15.7.3 was released, a patch level that fixes five vulnerabilities, none of which allows arbitrary code execution, but does allow privilege elevation at kernel level.

In addition, a patch (CVE-2022-42856) is also published in version 12.5.7 that allows arbitrary code execution in WebKit, i.e., when visiting a malicious website with Safari. Apple confirms that the bug is being actively exploited, especially in versions below or prior to 15.1.

iOS 16.3.1

13 February, group of three patches, one of special interest. Like the one discussed above for 12.5.7, we have a new bug affecting Webkit that makes it possible to execute arbitrary code just by visiting a malicious website. It has the CVE-2023-23529. Apple also confirms that it is being actively exploited.

iOS 16.4

We almost finished March without any updates, but on the 27th of that month the new version of iOS 16, version 16.4, was released, and it comes with a long list of security fixes. No less than 37 patches. Although only one of them allows the remote execution of arbitrary code, the large number of flaws relating to the evasion of measures to protect data considered personal or private by malicious applications is striking.

iOS 15.7.4

On the same day as the release of iOS 16.4, the still-maintained iOS 15.7 branch receives its fourth iteration, this time with a batch of 19 patches, four of them fixing bugs that could lead to arbitrary code execution remotely. It also includes the iOS 15 patch for the above-mentioned CVE-2023-23529.

16.4.1 y 15.7.5

Again, an urgent patch and again affecting WebKit (Safari's rendering engine), for a change actively exploited. This patch fixes two vulnerabilities including the commented one. Its license number is CVE-2023-28205.

Interestingly, it is released for iOS 16.4.1 on 7 April and three days later, on 10 April, for version 15.7.

16.5 y 15.7.6

It is 18 May and on the same day they release the fifth iteration of branch 16, which reaches its halfway point, and the sixth for 15.7.

For branch 16, 38 patches have been confirmed, five of them with particularly dangerous fixes, as the bugs allowed remote execution of arbitrary code and some of them were even actively exploited.

For 15.7, 16 vulnerabilities are fixed, three of them with arbitrary remote code execution flaws.

16.5.1 y 15.7.7

We had a new fright at the end of the semester. Emergency patch covering two serious bugs in iOS 16.5. The CVE-2023-32439 affecting WebKit (Safari) and the other, CVE-2023-32434, affecting the kernel. Both actively exploited.

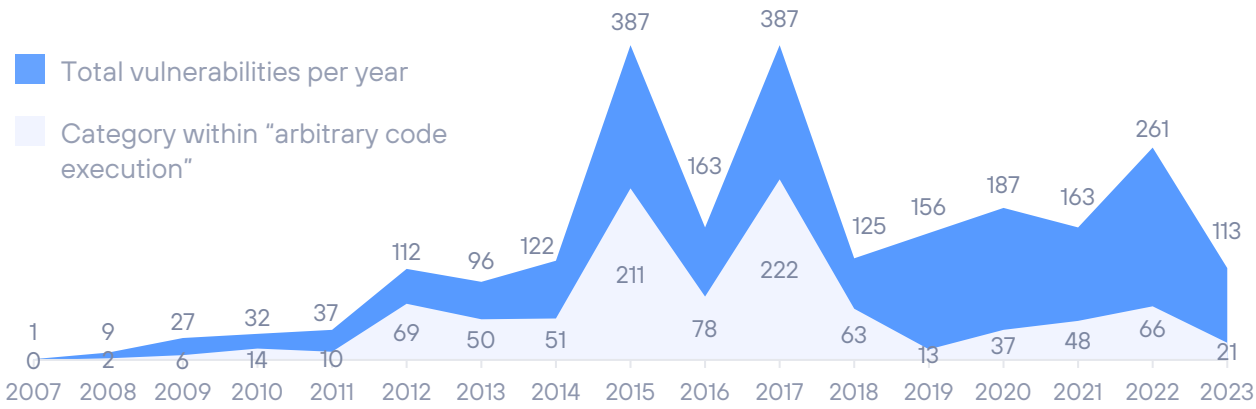
For 15.7, the seventh patch, and also an emergency one, it covers the above bugs plus an additional one for WebKit that has also been seen to be actively exploited. Its license number is CVE-2023-32435.

iOS vulnerabilities evolution during the first half of 2023

The first half of 2023 closed with 113 unique vulnerabilities patched, around a dozen of them considered high-risk, with the possibility of executing arbitrary code. Some of them affecting the operating system kernel itself.

If the trend continues, it is possible that we will see a year similar in numbers to 2022.

VULNERABILITIES IN IOS 2023-H1
Evolution of vulnerabilities per year



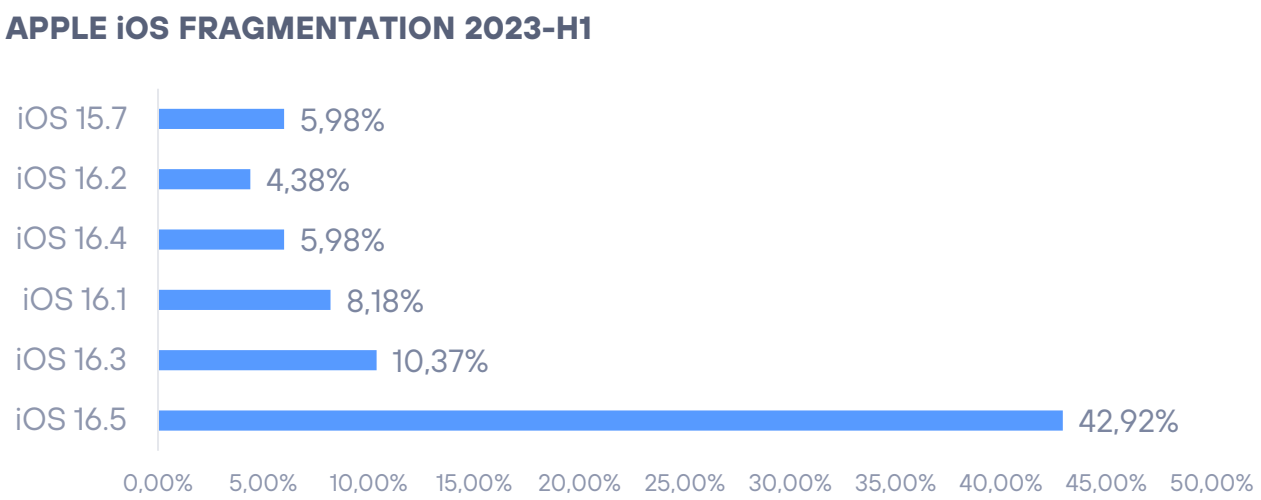
Release fragmentation during the first half of 2023

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

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

As usual in Apple's release cycle, we have iOS 16 at the halfway point of its lifespan (as long as Apple continues at the same pace of releasing new versions).

Currently, branch 16 is taking the lion's share of the iOS release pie:



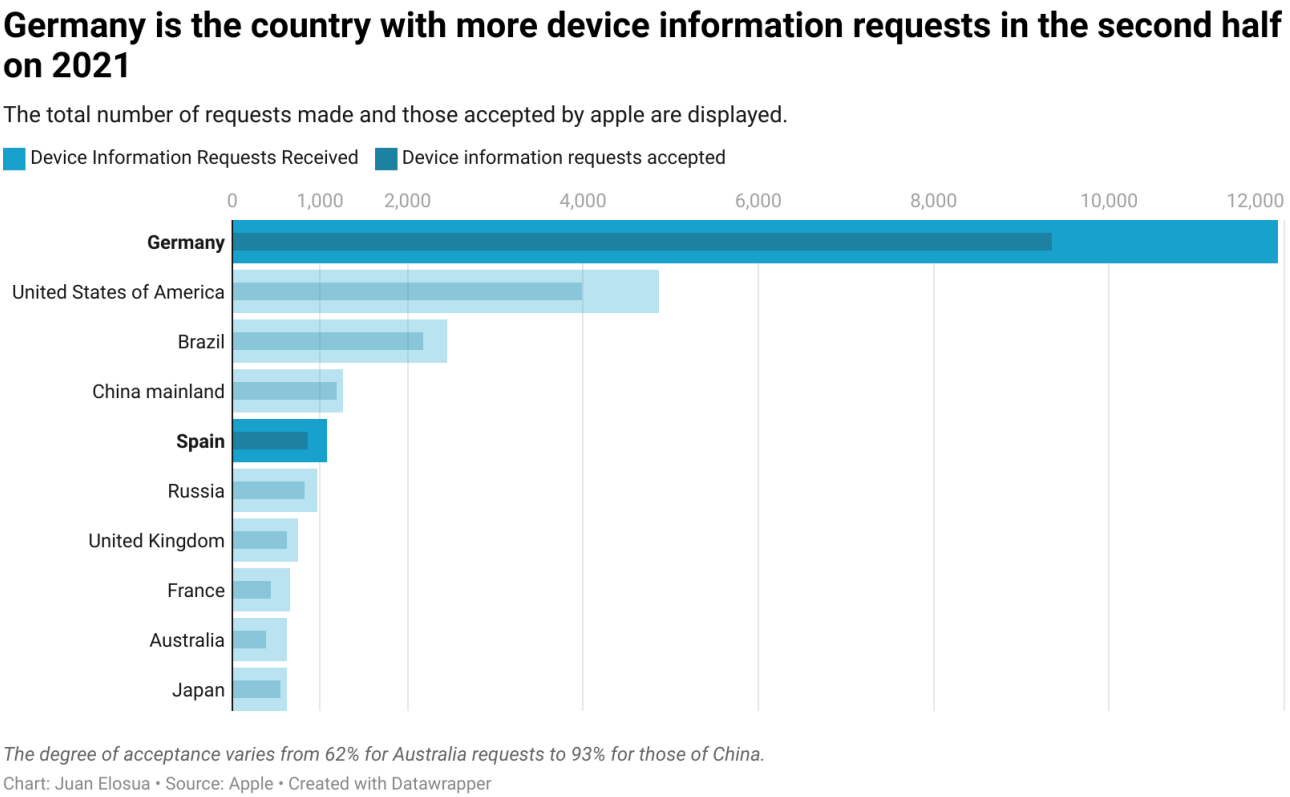
Only iOS 15.7 is minimally represented, and resists change with a 5.98% share.

Apple Transparency Report

Governments sometimes need to rely on large corporations to help them do their job. 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 be vital to the investigation and avert a catastrophe. Apple publishes a comprehensive report every six months on what data is requested by governments, which data is requested and to what extent the requests are fulfilled. We update here some data that we have extracted from the information published by Apple for **the second half of 2021 (the last published by Apple as of the first half of 2023)** on the activities and requests from governments to the company.

Device based requests

It represents requests from government agencies for Apple device information, such as serial number or IMEI number. 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.



The degree of acceptance varies from 62% for Australia requests to 93% for those of China.

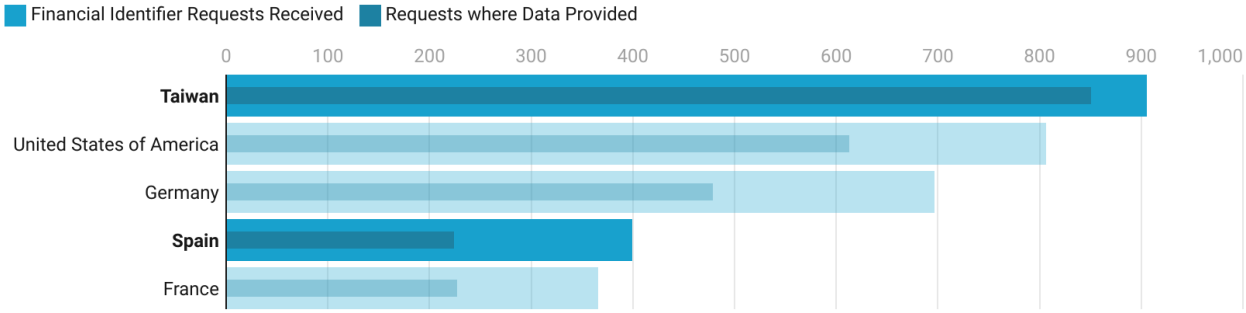
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Financial data based requests

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 leads fraud requests made in the second half of 2021, with Spain in a surprising fourth position.

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



The degree of acceptance for the 5 countries with more requests volume varies from 56% for Spain to 94% for Taiwan.

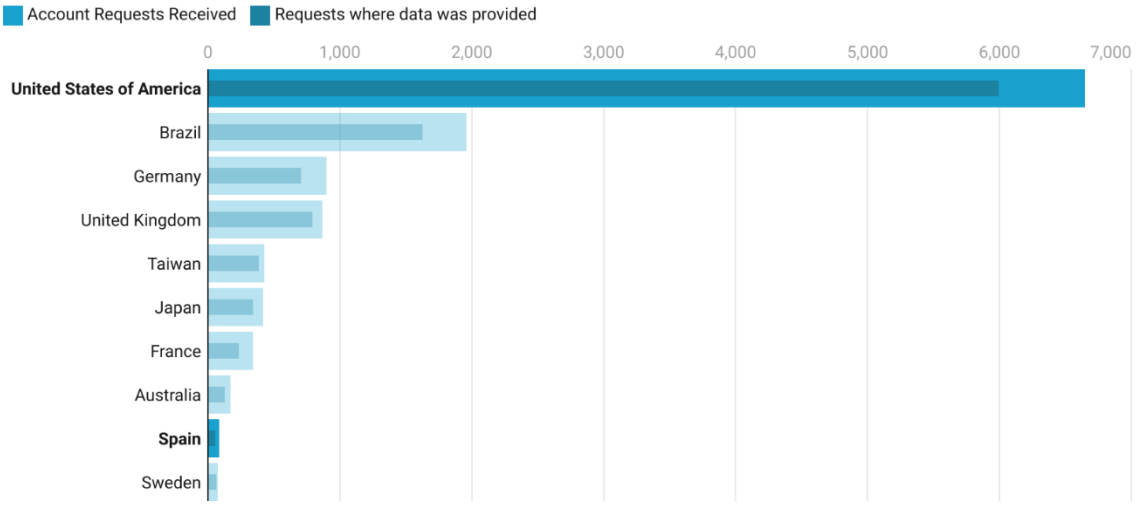
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Account based requests

Governments are making requests to Apple regarding accounts that may have been used in contravention of the law and Apple's terms of use. These are iCloud or iTunes accounts and their name, address and even content in the cloud (backup, photos, contacts...).

USA is, by far, the country with more account information requests made in the second semester of 2021.

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



Out of 84 requests made by Spain 47 were accepted by apple in the second half of 2021 (56%).

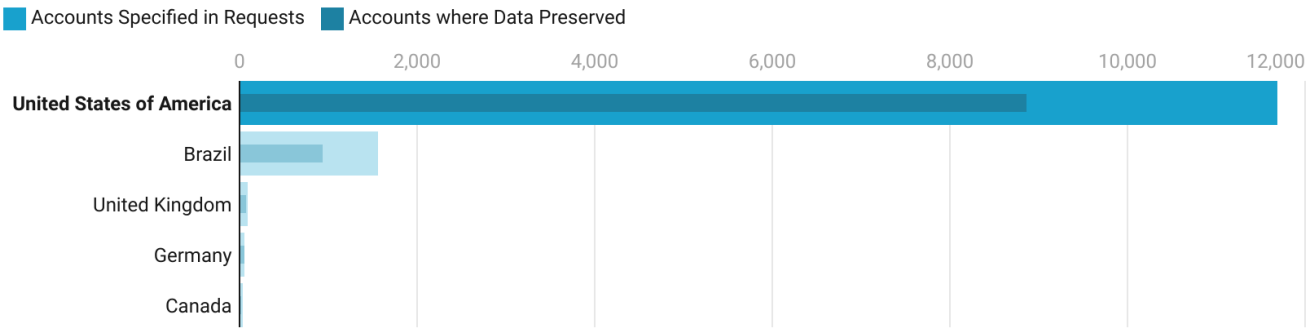
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Requests related to the preservation of accounts

Under the context of the U.S. Electronic Communications Privacy Act (ECPA), Apple can 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 data subject.

USA is the country with more account preservation requests in the second six months of 2021.

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



Spain,did not issue a single requests during the tthis period.

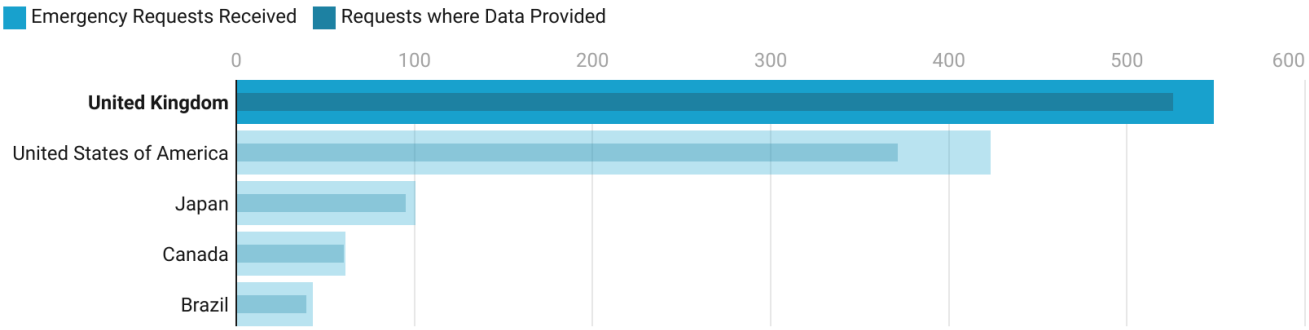
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Emergency based 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 with more requests to access accounts due to emergencies in the second semester of 2021

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



Spain, ranks in position 29 in the second half of 2021, with only 1 request to access accounts due to emergencies that was accepted.(100%).

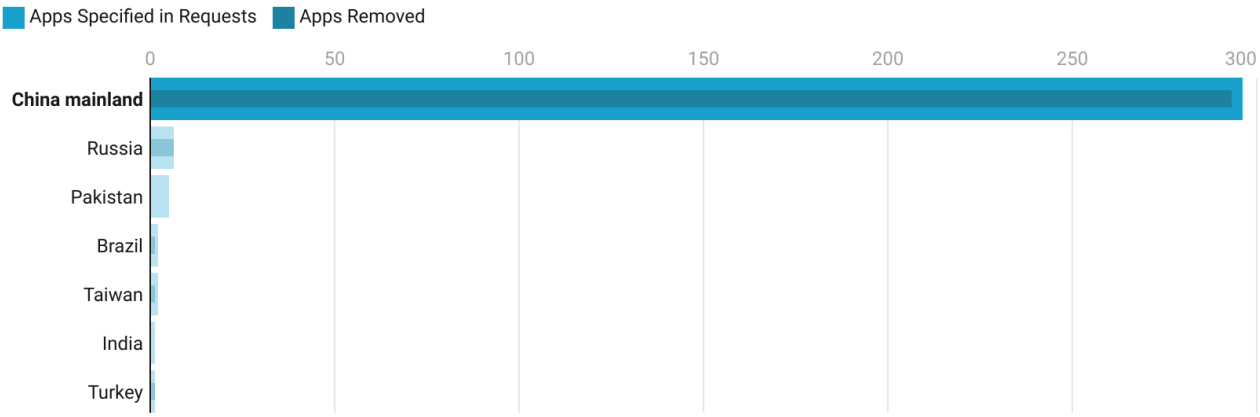
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Petitions concerning the removal of apps from the market

It usually has to do with applications that are supposed to violate the sovereign law of the applicant country/region.

China requested 296 apps takedowns in the second half of 2021 and 99% were accepted by Apple.

Apps takedowns requested in their market are shown in combination with those effectively deleted.



This number triples the amount of apps whose takedown was requested by China in the first half of 2012.

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 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.
- Taiwan has doubled its requests for account information due to fraud in 2021, from 1,000 requests in 2020 to more than 2,000 in 2021.
- The United States requests by far more than any other country for account preservation and access to the data hosted on it. What stands out from our analysis is that Brazil is a very strong second with 10 times more requests for preservation and access than the third.
- 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 access to US accounts. 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 removals from the App Store. The difference is enormous with the rest of the world: from almost 300 apps whose removal has been requested by China in the last six months of 2021, we go to only 6 for Russia, which occupies the second place in this list.

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. For example, Apple counts the number of requests for device information, and in turn each request can contain an indeterminate 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, that's what they are talking about, requests, not specific accounts. For example: Apple receives 10 requests, with 100 devices among all the requests and then says it has fulfilled 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

Android 14 is about to come out of Google's oven as we approach the anniversary date of Android 13 on 13 August. Version 14 is known internally as "Upside down cake".

The first security measure in the new Android will be rather curious: it will prevent the installation of apps for Android 5.1 and earlier versions. That is, until 14, apps that were literally years old were allowed to be installed, including a good catalogue of malware from the distant past.

Android 14 will finally implement a more granular selection of which files we can share with a given app. A feature very much inspired by what iOS has been offering for quite a few versions now.

The integration of "Passkey" into "Credential Manager" is also a step forward, allowing users to enjoy a more integrated and fluid experience of this alternative authentication method to passwords and very focused on the possession of the device.

A further step in connectivity: Android 14 will support satellite communications. If the chip supports it, it will allow users to connect and make calls (for example, and importantly: emergency calls) if we don't have a connection to telephone antennas, but we do have a satellite connection.

Android 14 is just a few days away from being made official, and we'll see what new features it brings when it is officially released.

Vulnerabilities

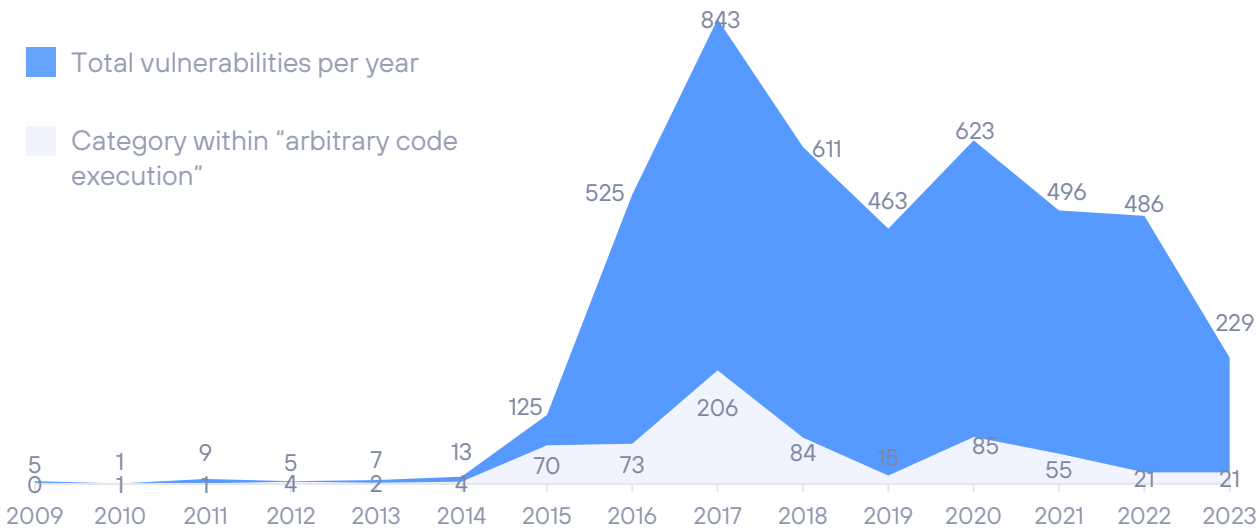
Android releases a set of patches every month, usually within the first week. In this first half of 2023, six bulletins have been published with a distribution of 33, 35, 39, 43, 38, 38, 41 patches or fixed CVEs. Similarly, by appearance, critical bugs are distributed as 1, 2, 3, 9, 1, 5 respectively.

In total, 229 patches (previous half-year was 256); 21 of them are considered critical (14 in the previous half-year).

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

ANDROID VULNERABILITIES 2023-H1

Vulnerability evolution per year



Fragmentation on Android systems

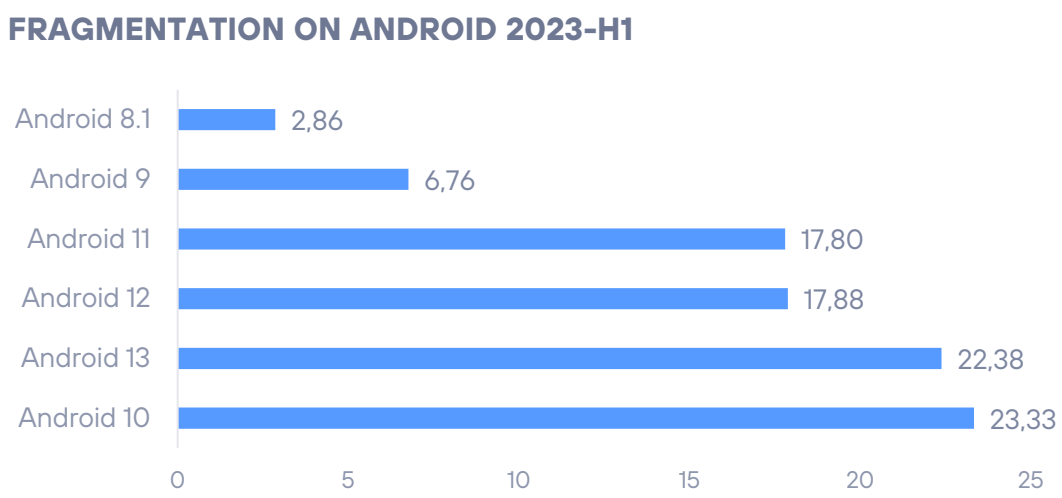
Statcounter's latest publication at the time of writing this report indicates that the most widely deployed version of Android is version 10, with a share of 23.33%, followed by version 13 with a share of 22.38%.

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

The new version, Android 13, which was only 6.72% available in the previous six months, manages to climb to second place, but it is nevertheless surprising that version 10 still has some traction and is climbing up the rankings. This may be due to the fragmentation of versions below version 13 or a change in the vendor's measurement methodology.

The remaining portion is shared by versions 12 with 17.88%, and 11 with 17.8%.

It is still alarming that Android 9.0 and 8.1 still have a combined share of 9.62%, down from 14% in the previous half year. As we have already mentioned, it is a danger that these units are still in operation and with such a significant number of devices. They do not receive security updates and have potentially vulnerable software. A significant risk.



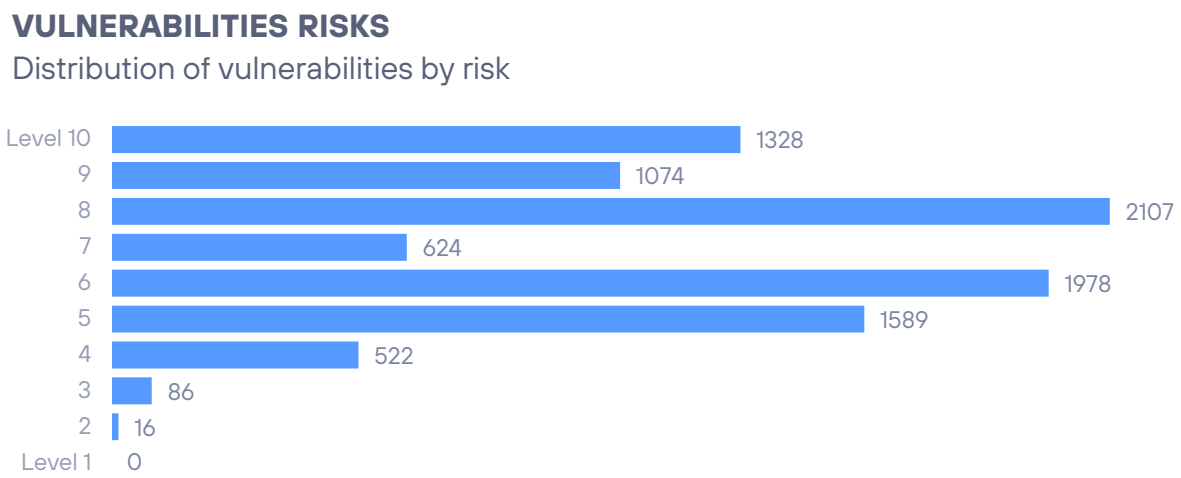
SIGNIFICANT VULNERABILITIES

In this section we comment on some of the notable vulnerabilities, in our opinion, of the first half of 2023, i.e., those that stand out for their special relevance or dangerousness.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2023-20076	Cisco IOx application hosting	A vulnerability in the IOx application space, which is based on incorrect parameter sanitisation, can allow a remote (authenticated) attacker to execute commands as root and even deploy and activate an application in this environment with a modified load file.	8.8
CVE-2023-27997	FortiOS & FortiProxy from Fortigate	Code execution on SSL-VPN-enabled Fortigate devices.	9.8
CVE-2023-22601	InHand Networks routers, InRouter 302 & 615	Two InHand routers, intended for use in industrial environments, are affected by an insufficient ability to generate random values when calculating the client ID when establishing MQTT connections. This could result in an attacker being able to calculate this ID and obtain information from other devices connected to the same platform.	8.6
CVE-2023-32347	Teltonika's Remote Management System	Teltonika's remote management system (version 4.10.0) only uses the MAC of the devices and their serial numbers to authenticate them during access to the system. This implies that someone who knows these two parameters could identify themselves as one of these devices and steal the device's credentials, as well as execute code as root using the legitimate device's options panel.	9.8
CVE-2023-1424	Mitsubishi Electric Corporation MELSEC iQ-F Series	Versions of these field devices are vulnerable to DoS attacks and malicious code execution via buffer overflow. For code execution, the attacker must know the internal structure of the products.	9.8
CVE-2023-21716	Microsoft Word	A flaw in Microsoft Office wwlib, allowing attackers to remotely execute code with the privileges of a victim who opens a malicious RTF document.	9.8

Vulnerabilities in figures

Regarding specific numbers of vulnerabilities discovered, the distribution of published CVEs by risk level (scoring based on CVSSv3) was as follows. The number of vulnerabilities in general has soared compared to the first half of the year.

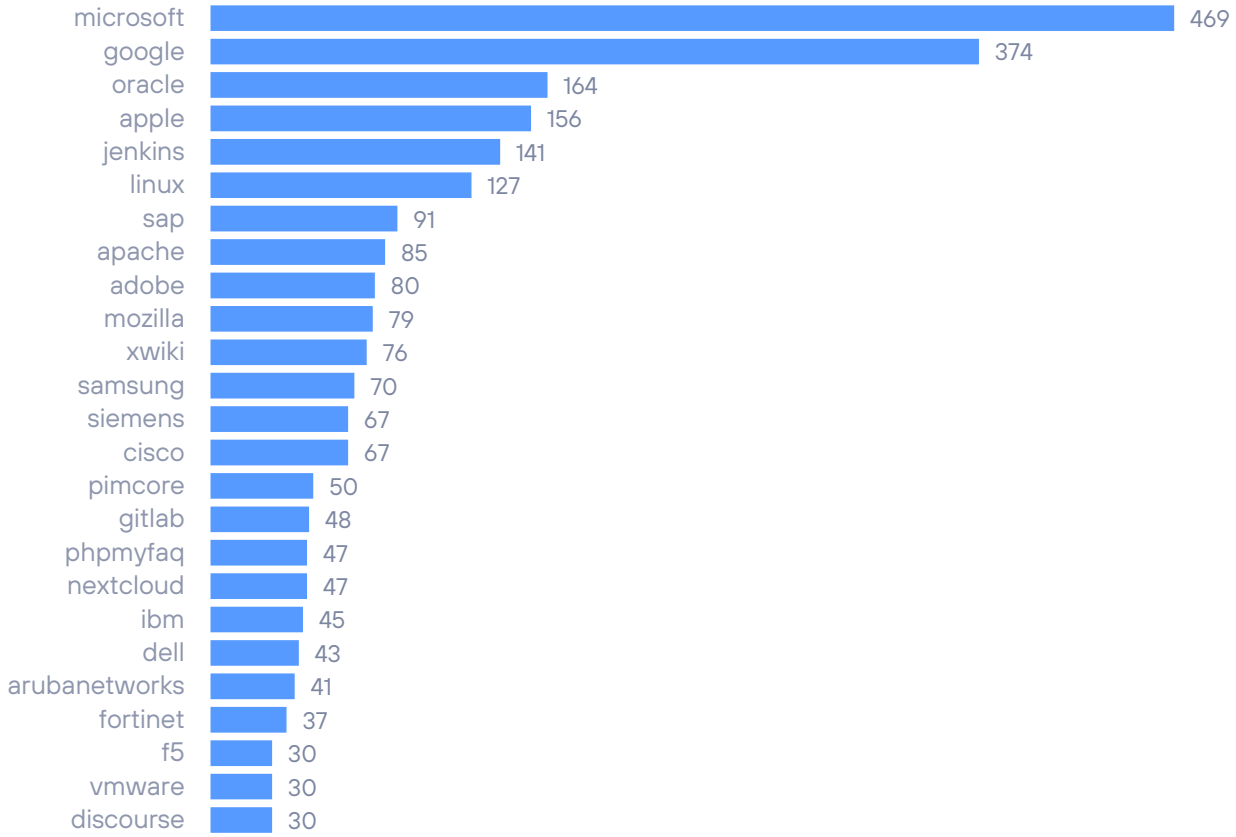


Top 25 companies with most accumulated CVEs

During the first half of 2023, Microsoft has led by far in terms of number of known vulnerabilities, followed by Google. In general, it is common for the big three, along with Oracle, to always be among the top three in terms of number of vulnerabilities.

VULNERABILITIES BY MANUFACTURER

Top 25 manufacturers by cumulative CVEs



APT OPERATIONS, ORGANISED GROUPS, AND ASSOCIATED MALWARE

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

We warn that the attribution of such operations, as well as the composition, origin, and ideology of organised groups, is complex and cannot necessarily be completely reliable. This is due to the capacity for anonymity and deception inherent in this type of operation, in which actors may use means to manipulate information in such a way as to conceal their true origin and intentions. It is even possible that in certain cases they may act in the modus operandi of other groups in order to divert attention or harm the latter.

Significant APT activity detected during the first half of 2023:

APT 15 - Playful Dragon: respect the elderly

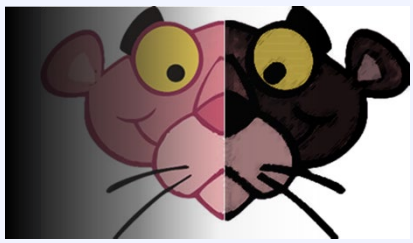
This group of Chinese origin (AKA "Flea"), listed **19 years ago**, specialises in cyberespionage and was the creator of the "Mirage" RAT.

This time, it has been detected using the "Microsoft Graph" API as a backdoor in its latest campaign against foreign ministries in several American countries, according to Symantec researchers.

In addition, the group uses Onedrive as an intermediate step to make the connection to the C&C server, which is a technique that they had not previously used, although it has been seen in another long-established group: Swallowtail (AKA APT-28), of Russian origin.

More information: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15

Dark Pink: Pink is the new black



We wrote about this group in the previous report, and they are still a trend. Discovered and catalogued in the second half of 2022, it is now easier to detect their movements. It is suspected that they have been running their operations since 2021 and focused on the geographical area of Indonesia (with operations in other countries and regions).

In this semester, they have been detected attacking governmental, military, and educational organisations in their preferred region. In addition, they have been renewing and refining their TTP catalogue and tools, indicating that they are alive and successful. We are sure we will read about them again...

More information: https://www.bleepingcomputer.com/news/security/dark-pink-hackers-continue-to-target-govt-and-military-organizations/

Golden jackal: Too quiet for a jackal...

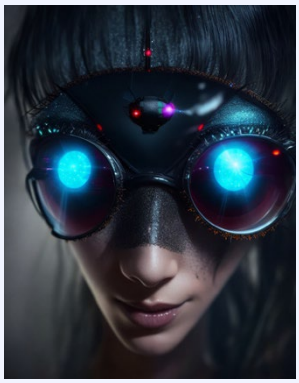
This group, which is estimated to be created in 2019, targets government and diplomatic entities in the Middle East and South Asia. Kaspersky researchers have detailed a very interesting article in which they uncover a group focused on espionage and with high technical skills and a stealthy attitude, which are two very rare characteristics for a jackal. The term "jackal" is used to describe APT groups with a hacktivist orientation. Jackals, therefore, tend to be noisy and unsophisticated. Their activity, moreover, is centred on hits for effect, so espionage activity is not usually their preferred activity.

Goldenjackal, however, is not. They have a well-prepared .NET toolkit of their own and their TTPs (the ones that are known) do not seem improvised. Reading the Kaspersky team's analysis, one senses that this group is thorough and highly skilled. We would go so far as to say that they seem to have a distinctly professional tinge in the way they go about preparing everything, including their versatile catalogue of tools. And, above all, they are very, very quiet. Very limited target list, very little noise, zero published information...

Regarding a possible relationship with other groups, the researchers observed similarities with the APT group "Turla" (of alleged Russian origin) in the algorithm for generating the victim's UID and in the TTPs. However, Goldenjackal's TTPs are not fully known, and the algorithm was already known, so this is not definitive either.

More information: https://securelist.com/goldenjackal-apt-group/109677/

Lancefly: The first silent fly



Summer is here and it's time to talk about flies, but in this case "cyber-flies". This group, which operates in South and Southeast Asia, primarily engages in espionage targeting government, telecommunications, and aviation environments. It was detected thanks to the trail of a custom backdoor they use in their actions, Merdoor. This backdoor was detected in 2020, but Symantec's team of researchers have found evidence of its existence dating back to 2018 and therefore also pinpoint the birth of this APT Group.

Lancefly has been included in the Chinese orbit due to the use of the same RAT used by APT Group 27 (AKA "Emissary Panda") and elements in its rootkit with the same nomenclature as those also used by this other group, which we told you about in the previous report. In addition, Lancefly also uses another RAT, ShadowPad, which is thought to be used exclusively by other "pandas" (APT Groups of Chinese origin).

More information: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

OT THREATH 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. 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 sectorised attacks, 0-day vulnerabilities, etc.

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

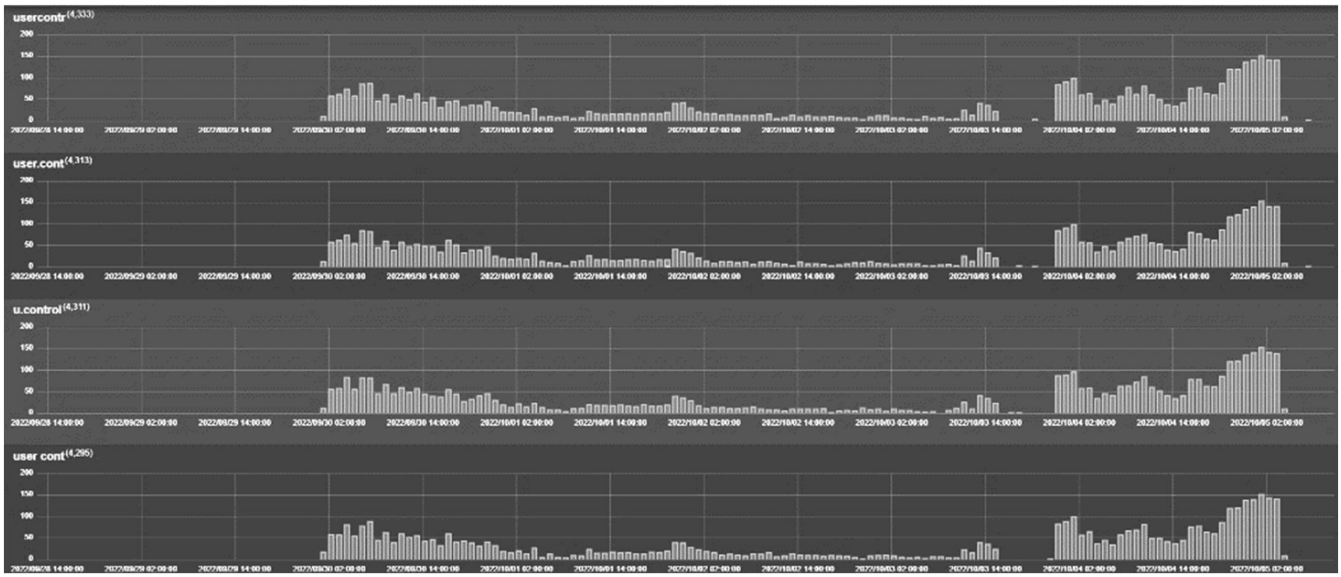
More information: https://aristeo.elevenlabs.tech

Information Analysis

In the previous semester, as a concrete case, we analysed a table of access attempts to an RDP system located in an engineering bay (industrial control PC). What we observed is that the attackers knew that this RDP was not an IT service as such, but a gateway to an industrial control system. In addition to access attempts with strings that included "SCADA" in the top 3, we observed the use of proper names in the access attempts, which also varied depending on the global exposure point we used for the decoy we exposed for a customer in central Europe.

Therefore, when we exposed the lure in Spain, the attackers used "David", "Laura", "Miguel"... and when we went to France, it was "Isabelle", "Emanuele", "Guillaume"... When we placed the lure in a different location, the names also varied, and the attackers used the most common names in that country. As we indicated in the previous report, we consulted the access attempts against the "INE" (Instituto Nacional de Estadística) of that country and noticed that the access attempts used the 10 most common names indicated by this institute. But this was just a reminder. What more can we add?

In addition to observing this curious fact, we also demonstrated Aristeo's ability to detect patterns. Let's take as a sample values that were also repeated in Spain, France, and the other country we can't tell you about: "usercontr", "user.cont", "u.control" and "user cont".



This pattern is taken by collecting different IP addresses and different countries of origin and destination.

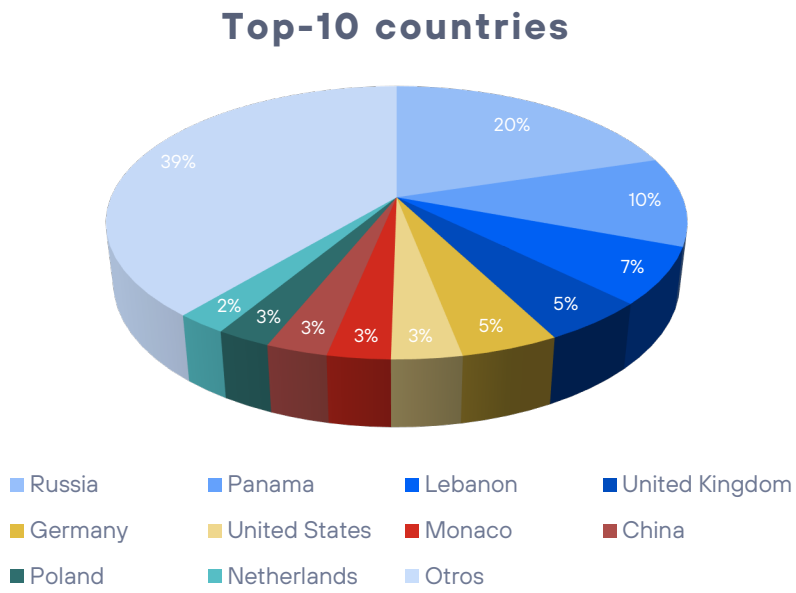
What does this mean?

That different IP addresses located in different parts of the world were executing the same action with the same credentials against our industrial decoy. Moreover, this decoy was not located in a specific country, but we were "moving" it around Europe. Therefore, such attempts constituted a **targeted campaign against TO environments**, at least within the EU space. Whether the target was specifically the industrial sector, the customer, or all kinds of OT environments, we left that information for our customer.

We know that these values are quite generic, but they serve to quickly show the similarity between the values and the pattern of Aristeo's detections. We also detected other types of values related to the client and more directed to the OT domain, but we believe that this tuple is a good sample button.

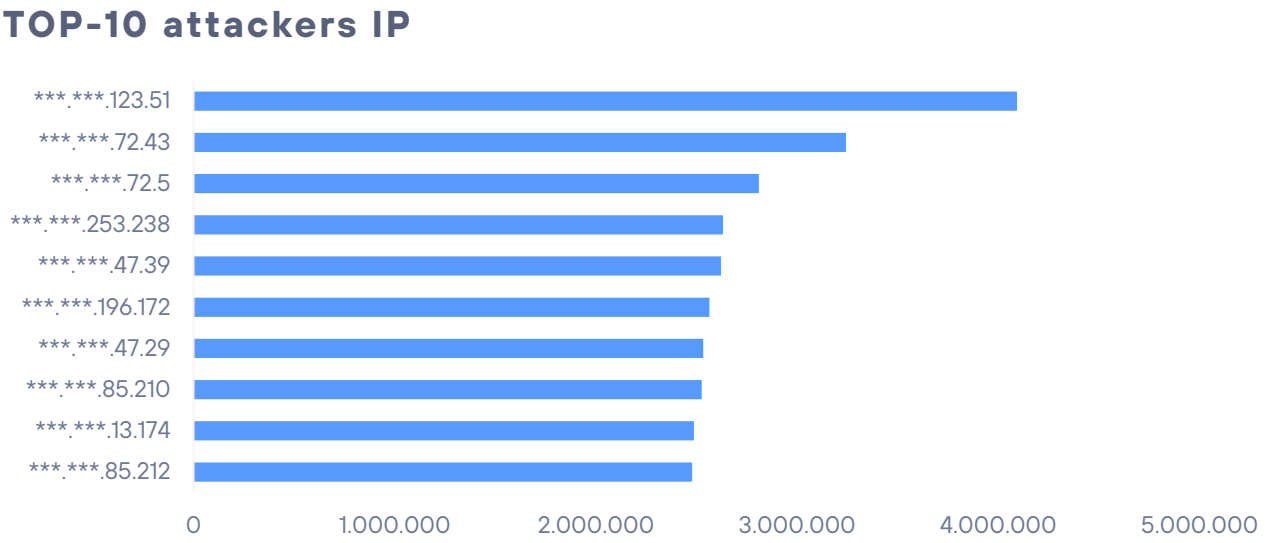
And now, let's move on to the general statistics of the information recorded. In the first half of 2023, **more than 300 million cyber security events** were detected. This is an increase compared to the data recorded in the second half of 2022. However, it is still lower than the more than 415 million events detected in the first quarter of 2022.

The distribution by country is as follows:

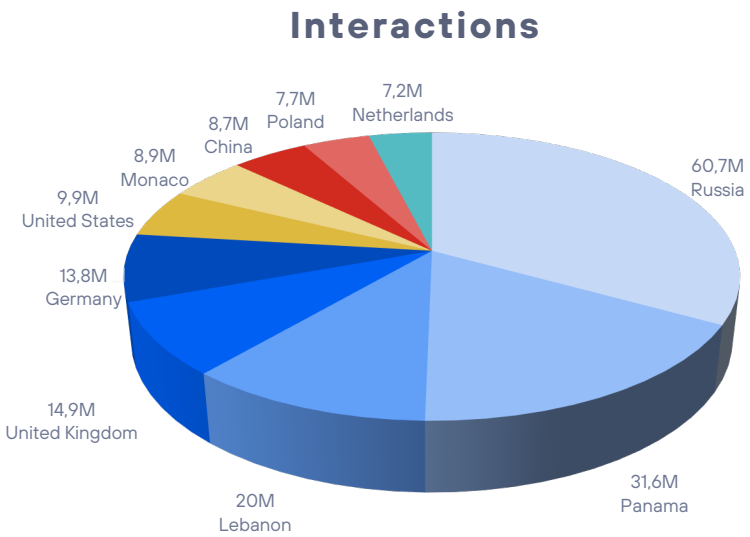


The geographical dispersion of the TOP-10 remains similar to previous reports, which is a clear trend, albeit occasionally disrupted by international events. Also striking is the increased weight of Panama, but that will be discussed in two charts.

Let's now take a look at the ten IP addresses with the most interaction with the Aristeo system. Slightly more than 54% come from various Eastern European countries. In this semester, the rise of Panama as a country of origin is also reflected in this graph. In fact, almost 28% of this TOP-10 are IP addresses with this origin. However, we have detected that the majority of these IP addresses originate in the Netherlands. Others, however, were captured directly from Panama and appear to be compromised systems.



We can see below how the countries with the greatest presence in our Aristeo are distributed in terms of activity. In this semester, the striking fact is the rise of Panama as the country with the second highest number of detections, which is as striking as the decrease in detections of origins from the USA. We do not know if these two data are related, and we cannot analyse the drop in results from the USA, but we do have the impression that the results from Panama are due to several campaigns against certain financial targets in this country.



THREAT ASSESSMENT 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: 205,273 IP addresses, 54892 domains and 298,086 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 that is 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 categorise it appropriately, so we know what type of threat we are dealing with. This is precisely what we asked in the Maltiverse database and came up with these results:

Type	Quantity	Percentage
Malware Download	150443	50,47%
Phishing	103138	34,60%
Qakbot	18605	6,24%
Malicious URL	11614	3,90%
Cobalt Strike	9397	3,15%
Vidar	1023	0,34%
Raccon	556	0,19%
Astaroth	509	0,17%
Amadey	406	0,14%
DCRat	356	0,12%

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 categorisations are more explicit and even indicate to which malware family they belong.

For example, "Qakbot" has a record number within its speciality: more than 6% of all URLs are related to this malware family that wreaks havoc among online banking users.

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 more fraudulent use. A server can be hosted in one country and the criminal organisation using it can be of another nationality.

Country	Quantity	Percentage
Estados Unidos	40231	19,60%
China	35111	17,10%
India	14343	6,99%
Rusia	11187	5,45%
Alemania	8775	4,27%
Corea del Sur	5382	2,62%
Singapur	4803	2,34%
Brasil	4429	2,16%
Indonesia	4358	2,12%
Vietnam	3566	1,74%

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

What type of maliciousness do IP addresses engage in?

Type	Quantity	Percentage
Mail Spammer	135858	66,18%
Malicious host	57987	28,25%
Proxy	51314	25,00%
SSH Attacker	34879	16,99%
Bruteforce	22928	11,17%
Port scanner	22509	10,97%
Hacking	22199	10,81%
HTTP Spammer	20538	10,01%
HTTP Flooding	19283	9,39%
HTTP Attacker	13087	6,38%

At the top of the ranking, we find the undeniable winner: SPAM. This has been the quintessential ranking for decades now, and SPAM marking rules are very sensitive to this activity. Practically, we could say that almost every public IP address will have been marked as SPAM at some point.

The rest, except for the generalist categorisation of "Malicious host", is similarly divided and almost evenly distributed. For example, and these are also classic activities, we have 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 carry out an Internet census 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 as 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 made up of several levels. If you look at them, they are sections 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 categorised as malicious by their top-level domain. The result looks like this:

TLD	Quantity	Percentage
com	21219	38,66%
org	2918	5,32%
app	2547	4,64%
top	2522	4,59%
net	1883	3,43%
xyz	1641	2,99%
site	945	1,72%
link	788	1,44%
dev	732	1,33%
click	672	1,22%

It is no surprise that ".com" dominates the ranking, as it is the TLD with the highest number of domains. However, there are certain TLDs in the table that deserve additional observation, for example the ".app" and ".xyz" TLDs.

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

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

What is the malicious categorisation of the domains studied?

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

Let's see, finally, how they have been categorised over the last six months.

Category	Quantity	Percentage
Phishing	34697	63,21%
Qakbot	9067	16,52%
Malware download	2048	3,73%
Cobalt Strike	1636	2,98%
Vidar	1527	2,78%
Prometei	1440	2,62%
Astaroth	1031	1,88%
CryptBot	698	1,27%
Infy	648	1,18%
Ice Fog	371	0,68%

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. However, the relative number of the Qakbot family is surprising and, as when talking about URLs, it stands out from the rest of the families.

Let's see what happens in the next six months. Let's see how the malware families fluctuate (or not) in this particular.

RECAP

The number of vulnerabilities fixed in iPhone may reach a good number this year, based on the numbers we've seen in the first half of the year. In 2022, a record was reached that has not been seen since 2017. On the other hand, the trend on Android is downwards, with similar or even lower numbers this year, when the trend is around 500 bugs. On the other hand, if 2022 was one of the years with the lowest number of critical vulnerabilities, 21, this year it has already been matched in only 6 months of 2023.

Regarding Apple's transparency report, the German government is once again the one that has generated the most requests for information on devices in the second half of 2021. Taiwan has doubled its requests for fraud account information in 2021 from 1,000 requests in 2020 to more than 2,000 in 2021. The United States requests by far more than any other country for account preservation and access to the data hosted on it. What stands out from our analysis is that Brazil comes in a very strong second place with 10 times more requests for preservation and access than the third.

Microsoft, Google, and Oracle are the companies with the most bugs fixed, as usual, although sometimes swapping order.

Regarding OT security, more than 300 million cybersecurity events were detected in the first half of 2023. This is an increase compared to the data recorded in the second half of 2022. However, this is still lower than the more than 415 million events detected in the first quarter of 2022.

Based on the analysis of the data in Maltiverse, we can conclude that half of the infrastructure considered malicious is used to download malware (50%) and that 66% of malicious IPs are used to send spam. Most of the infrastructure tends to be located in the US. Even with the emergence of new top-level domains, ".com" is still the favourite malicious domain with 39% of the registered cases, far behind the second-ranked ".org" with just over 5%.

USEFUL LINKS

Do not just stay in the top layer of cyber security analysis, the half-yearly reports are cumulative and summarised. In Telefónica Tech's cyber security blog we have much more information and news that you may find interesting. Here are our most relevant articles.

IDENTITY

Web3 y la evolución de la Identidad en Internet

Los ataques más comunes contra las contraseñas y cómo protegerte

ARTIFICIAL INTELLIGENCE AND CRIPTOGRAPHY

Inteligencia Artificial aplicada a la Ciberseguridad industrial (OT)

Criptografía, una herramienta para proteger los datos compartidos en la red

Edge AI vs. Cloud AI: conoce sus diferencias y elige el mejor enfoque para tu proyecto de Inteligencia Artificial

Evolución de la Ciberseguridad: la IA como herramienta de ataque y defensa

MALWARE

Evolución de las técnicas de Spear-Phishing de los grupos criminales más conocidos y qué malware utilizan

Cibercrimen, una amenaza constante para todo tipo de empresas