Telefónica Tech

Security Status Report 2022 H2

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

telefonicatech.com

Índex

RESUMEN EJECUTIVO

The purpose of this report is to synthesise the cyber security information of the past 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.

The second half of 2022 has been characterised by several attacks on large companies that have caused a lot of talk. For example, Uber, which used a very human way of circumventing the second authentication factor: the "fatigue" of the driver by receiving dozens of messages asking for confirmation of access in a short period of time and also at inappropriate times. Another high-profile attack (and there have been several already) on LastPass has once again called into question the security of using cloud-based password managers. Many other companies and even countries have suffered attacks, although we have only seen them reflected in their consequences: the leaks. In the last half of 2022. Cisco, Microsoft, Toyota, Revoult? And even the personal data of the Chinese population has been leaked.

In contrast, attacks using Office macros as an attack vector have decreased. The reason is that Microsoft has made it increasingly difficult for them to be executed by default and attackers have exhausted many of the technical possibilities for circumventing controls, thus alerting EDR and protection systems to be able to hunt down new execution formulas. Attackers are therefore looking for new, more complex but perhaps more effective formulas, such as the zero days in Chrome, which, despite their difficulty, have been nine in 2022.

In this scenario, however, professional ransomware remains the jewel in the attackers' crown, because it is still a lucrative business. But how much? There are many estimates, and all can be more or less accurate. At the end of 2022, the FBI offered a concrete figure that seems quite reliable: Hive, one of the most active ransomware organisations, had earned $100 million from 1300 victims. And all this since June 2021, when activity began to be observed. For a time, they shared resources with the Conti gang. This gives an average of about $77,000 per victim. The average is tempting, but it does not reflect reality, because Hive has had some very lucrative and high-profile heists, with loot far exceeding this average. In fact, Hive publishes on its website, along with each victim, the number of employees and the company's profits. It gives a clue as to how much they can extort based on these parameters. On average it works out at 81 victims per day every day. Some of these attacks will have required months of preparation, others will be quicker. But the certain conclusion from these numbers (which we cannot guarantee either, because there will be victims that never come to light) is that the workings of Hive in particular and ransomware gangs in general are greased. Such an infrastructure requires investment in recruiting victims, attacking them (breaking into their systems), network time, victim care for collection, money laundering, and so on. It is also worth noting that the gangs are not usually very numerous, at least in their technical core, so we conclude that they are very productive per attacker.

This semester, in addition to maintaining our specialised section on industrial threat analysis thanks to our **Aristeo** project, we are adding 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 cyber security 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 SECOND HALF OF 2022

The following are the news items that have had the greatest impact over the course of the second half of 2022.

JULY

- Maddie Stone, one of the lead researchers on Google's Project Zero team, which is responsible for finding, analysing and trying to collaborate with vendors to fix dreaded 0-day vulnerabilities, published a tough report stating that in **the first half of 2022 more than half of all 0-day vulnerabilities are variants of already known vulnerabilities**. This demonstrates a lack of root-cause analysis by vendors in the resolution of vulnerabilities.
- Microsoft keeps thinking about macros and their impact. In less than two weeks it goes from completely blocking them for documents downloaded from the internet to reversing the change and finally reintroducing them.
- China suffers the first large-scale data leak, at least the first to be public. When you have a population of 1.4 billion people a **leak of such gigantic proportions** is a matter of time. Several international media have verified the authenticity of the sample posted on a DarkWeb forum which appears to be part of a database of the Shanghai National Police and which according to the advertiser ChinaDan consists of **data on more than 1 billion Chinese citizens** with sensitive information including names, addresses, identity numbers, mobile phone numbers, police, and medical records.
- **Prestashop**, the most popular open-source e-commerce platform in Europe and Latin America, used by around 300,000 customers worldwide, detected an attack using a combination of vulnerabilities, including a **0-day SQL injection, that allowed code execution with the aim of stealing customer payment information**. PrestaShop have published a series of checks to verify the impact and recommendations such as disabling the MySQL Smarty Cache function that was used to carry out the attacks.
- **"Rolling-PWN"**: Vehicle manufacturer **Honda is redesigning newer cars** to eliminate a vulnerability that apparently affects **models from 2012 to 2022**. The problem is related to remote keyless entry. Researchers at Star-V Lab have discovered a vulnerability in the key rotation system of the random key generator that manufacturers use to prevent replay attacks and that allows them to reuse the keys to unlock or even start the car.
- The SEMAE (Municipal Water and Sewage Service) of the municipality of São Leopoldo in Brazil suffered a cyber-attack the week of 4 July. A ransomware was executed that encrypted even the backups. The municipality has more than 230,000 inhabitants.

AUGUST

- **Twilio**, a giant in SMS management as well as other customer contact channels, suffered a phishing attack affecting 163 customers. It does not seem very relevant, as it represents 0.06% of its customer base, but its particular role in the digital ecosystem makes the importance of the attack much greater and shows the sophistication of the attack. **An attack targeting a company that provides SMS services that can serve as a second factor of authentication** for its corporate customers, like Signal, Okta or Authy is significant as **it can trigger multiple supply chain attacks**.
- Google reports **the largest DDoS** (distributed denial of service) **attack in history**. A Google Cloud Armor client received a series of HTTP attacks that reached 46 million requests per second and lasted just over an hour. The attack was executed using requests from more than 5,000 IP

addresses in more than 100 countries. Researchers indicate from the characteristics of the attack that it may be **related to the Mēris botnet**.

- Owners of on-premises Confluence servers (Confluence Server and Data Center), in particular those using one of its most popular applications called Questions for Confluence, must update due to a critical vulnerability (CVSS 9.9) caused by **hardcoded credentials that gave access to those servers and were posted on Twitter only a day after Atlassian released the patch** disabling that user.
- A developer named Stephen Lacy discovered a curious malware attack on Github in August. An attacker created more than **35,000 repositories with copies of popular repositories to which he added malware**. If a user used the modified copy instead of the original, the attacker would get their environment variables and a backdoor to their systems. Github removed the repositories identified as malicious within a week.
- Multi-factor authentication is becoming a requirement in software development and publishing platforms. This month RubyGems (Ruby), joins npm (javascript), NuGet (.Net) and PyPi (Python) in announcing the obligation to use two-factor authentication (at least for libraries with the most downloads) in order to publish libraries or software packages. This trend may be part of the drive for more security in the software industry but may also stem from the rapid increase of incidents in relatively small opensource projects that triggered huge supply chain attacks.
- An attacker managed to use a forgotten URL in the installation process of the web administration panel of bitcoin ATMs managed by Crypto Application Server (CAS) of the company General Bytes. He **gained administrator access and reconfigured the ATM** so that when a user sent money to the ATM to be picked up in person, the money was redirected to the attacker's wallet.
- The CL0P group publishes an advertisement on its TOR site claiming to have successfully attacked the Thames Water company, including SCADA systems and control panels. This advert, however, includes information from that company as well as from another company called South Staffordshire PLC. The latter company acknowledged the attack, stating that water supply was not affected thanks to the "robust systems and controls over water supply and quality" they have in place. The cybercriminal group, meanwhile, published images of the HMI and stated that "it would be easy to change the chemical composition of your water, but it is important to note that we are not interested in causing any harm to people".

SEPTEMBER

- Trellix publishes the technical details of **a path traversal vulnerability in Python's tarfile module** that has been known for 15 years. Interestingly, **in this case it is not that the vulnerability went unnoticed, but that it was not given the importance it deserved** and with the globalisation of SW and supply chain dependencies the impact is much greater than expected.
- Financial technology company **Revolut is the victim of a cyber-attack** affecting just over **50,000 customers**. Although the exact details are not known, all indications point to a social engineering attack to gain access to a customer database containing personal customer information such as address, telephone and account numbers. Revolut reports that its customers' balances have not been compromised and that no passwords, PINs or bank card information was accessed.
- Denmark follows the lead of Austria, France and Italy in declaring the use of Google Analytics illegal within the country as it breaches the GDPR. The Danish data protection agency urges companies to adjust the tool by using a reverse proxy to pseudonymise information before sending it to Google's servers in the US or to stop using it.
- A detection of the use of Cobalt Strike was so far a clear indicator of an attack in progress. From this September onwards, defence teams will need to add the use of **Brute Ravel**, another redteam post-

exploitation communications coordination tool, as an indicator of an operation after **a cracked version of this software was made available to cybercriminals** on multiple underground forums.

- Albania severed diplomatic relations with Iran following the attribution of a cyber-attack on Albanian government computer systems in July 2022. Although Iran denied involvement, NATO, the White House and the British government issued publications supporting the Albanian government. **This is the first time that a cyber-attack has permeated the political sphere in such a direct way, leading to diplomatic conflict**.
- The relative calm at **MS Exchange** is over after the ProxyShell incident. In September, **two critical vulnerabilities were detected that were being actively exploited**. The presence and combination of both vulnerabilities in a chained fashion leads to remote code execution, elevation of privileges and the ability to finally take control of the server. Estimated **to affect more than 200,000 mail servers**, Microsoft was working out of cycle to patch the vulnerabilities given the urgency of the situation.
- The General Staff of the Portuguese Armed Forces acknowledges two cyber-attacks that were detected through documents found by the USA for sale on the Darkweb. The President of the Internal Security Observatory indicated that this is "irreparable reputational damage" and urged the recruitment of more cybersecurity personnel.

OCTOBER

- **The Raspberry Robin worm** that spreads via infected USB devices has been making headlines in recent months by infecting a large number of Windows systems. Deutsche Telekom's CERT detected that many of the infections could be traced back to the use of USB devices in print and copy shops. The framework used by the post-infection Raspberry Robin malware uses **advanced obfuscation, anti-sandboxing and security tool evasion techniques, including installing fake malware** to confuse researchers about what they are analysing.
- **A critical vulnerability in OpenSSL** put major system administration teams on alert for a week this October. Some compared it to Heartbleed, finally downgrading its criticality from critical to high. It remains an important vulnerability because **it can lead to arbitrary code execution** or a denial of service under certain conditions. **Exploitation**, however, **is not straightforward** as there is little usable space to launch the attack and the digital certificate needs to be signed or accepted by the user.
- An American cryptography expert Nicky Mouha discovers a **buffer overflow** vulnerability in the implementation of **SHA-3** in a **well-known open-source library called XKCP** that provides several cryptographic schemes. Attackers could execute arbitrary code and remove expected cryptographic properties in SHA-3. Patches are generated for the XKCP distributions for Python, Ruby and Php.
- A **first draft specification** for a new W3C (World Wide Web Consortium) standard is published **to standardise the password change URL** with the following format: https://example.com/.well-known/change-password. The idea proposed by two Apple engineers is to allow tools to automate the discovery of password change pages and thus make it easier for the user to change passwords on various services automatically.
- The popular **e-commerce platform** Magento, now called Adobe Commerce, is affected by two vulnerabilities, one of them qualified as **critical Cross-Site Scripting**, which used in combination allowed an attacker to execute arbitrary code. Adobe releases patches for the affected versions, yet some Magento security firms such as Sansec suggest upgrading to new versions of the platform instead of applying the available patches whenever possible, which denotes that the patch does not address the root cause of the problem.

- A Symantec report finds that the **espionage group The Wichetty hid mlaware in an old Windows logo** that was downloaded from a trusted public source to avoid arousing suspicion and then extracted the backdoor by processing the image. Symantec describes the attacks analysed as targeting two governments in the Middle East and a stock exchange in an African country, **relevant victims for an attack using sophisticated techniques such as this**.
- The National Renewable Energy Centre suffered a cyberattack that left the entire workforce in Sarriguren, Navarre, without access to its systems. In April, wind turbine manufacturer Nordex also suffered a cyber-attack that left an unspecified number of the company's approximately 1,000 workers in Navarre without access to its systems.

NOVEMBER

- Kaspersky researchers identify a **phishing campaign** that employs a new stealth technique, **via Google Translate links**. From the user's point of view, they will see a link to a seemingly legitimate Google service that translates the website on the fly and serves the, in this case, malicious content via a seemingly innocuous connection. **This evades one of the traditional domain-checking defences a user has in place to detect phishing**.
- **A phishing network that defrauded 12 million euros was dismantled in Spain**. The national police issued a statement announcing the arrest of six members of **a criminal gang that had phished more than 12 million euros from a total of almost 300 victims**. The investigation began with a report that a Spanish financial institution was being impersonated to offer **fake financial transactions in equities and cryptocurrencies** to French customers.
- **Attributing the origin of a group of cyberattackers is always complicated** and security researchers rarely state this categorically. **This November, the internal chats of the Yanluowang gang were leaked and it became clear that its members were not Chinese but Russian**.
- Given the rapid growth in users that the **Mastodon** social network has experienced as a result of the exodus from Twitter, it was only a matter of time before **someone used the social network's infrastructure**, in this case distributed, **to set up Command & Control communications**. The attacker used the "about me" page to tell the malware to connect to the mastodon ioc.exchange server where to find the actual C2.
- **Github**, the well-known source code management platform, adds a feature that allows security researchers **to report vulnerabilities in public repositories to their respective owners through a private channel**. This functionality will help researchers to avoid having to use the issue system that is visible to the general public including potential attackers. Yet another step in **the securitisation of open-source code that is so much in the spotlight after serious supply chain incidents such as Log4Shell**.
- Google's Project Zero team warns that there is **a significant delay in patching vulnerabilities in the Android ecosystem**. Specifically, after detecting five exploitable vulnerabilities in **the ARM Mali GPU driver** and working with ARM to generate end-user level patches, these vulnerabilities are still exploitable as **Android phone manufacturers such as Google, Samsung, Xiaomi, etc. have not yet passed them on to their phone users**.
- A malicious actor called Ryushi offers for sale on a well-known underground forum a **database of 400 million Twitter users**. The seller claims that the data was extracted through a vulnerability and includes emails and phone numbers of users of the platform. This news comes after Twitter earlier this year acknowledged the authenticity of a leak that was offered for sale on the Dark Web containing **personal data of 5.4 million users and for which the Irish data protection agency was conducting an ongoing investigation for breach of GDPR**.

- Microsoft researchers were investigating a series of attacks against the Indian power grid when they noticed the use of Webserver Boa as an access vector in the attacks. This software is used in routers, security cameras and other IoT devices related to the OT world... and has been unsupported since 2005. The researchers also said they have identified more than a million such components.

DECEMBER

- **Android system certificates from Samsung, LG, mediatek and other manufacturers are used to sign malicious apps with malware**. This is a serious problem as system certificates are considered by Android to be strongly trusted and therefore have access to almost the entire system. Following the finding, security researchers at Rapid7 pointed out that, although malware signing is usually associated with state-sponsored cybercriminals, in this case **some of the signed apps were simple adware, which may denote that these certificates have been widely available on underground forums**.
- **Ninth 0-day published for Google Chrome**, in this case a type confusion vulnerability. Exploitation of this security flaw could allow a remote attacker to potentially exploit stack corruption via a manipulated HTML page. The number of serious bugs in Chrome has been increasing significantly for some time now. Google gives its reasons for this, but it is also true that **the profitability of vulnerabilities in the chromium engine is now much higher as it affects Chrome, Edge, Opera browsers**. In short, this is a very appetizing hotspot for attackers.
- After a year of **Log4Shell**, the vulnerability management platform Tenable, publishes that after a series of tests concludes that **72% of organisations are still vulnerable** to Log4Shell and that **from May 2022 to October 2022 the organisations that have remediated the vulnerability have doubled to form the remaining 28%**.
- Two security researchers from Kaspersky and Stairwell publish **a plugin for IDA Pro that uses the famous chatGPT artificial intelligence language model to explain the decompiled functions. A big caveat: the explanations may not be accurate**, for example StackOverflow has banned ChatGPT-generated responses due to the large number of bugs they contained.
- **After countless accidental security incidents, the cloud storage service AWS S3 has finally decided to change its default settings from "public" to "block public access"**. This reveals the importance of defaults and the principle of privacy-by-default. From April 2023 onwards, if you really want to have content in S3 open to the general public, you will have to deploy an ACL (Access Control List) to make it effective.
- LastPass reports that its cloud storage system was breached using stolen access keys in an incident last August, where attackers gained access to the company's technical information and source code. **Using these keys, the attackers were able to steal customer account information and data stored in the vault, including passwords and notes**. While the vault data is encrypted, the company has warned its customers that **attackers could attempt to brute-force their master passwords and gain access to all stored information**. The latest statement from LastPass admits that the urls for a given customer are not encrypted but simply obfuscated in a proprietary binary format, which is a problem as an attacker knowing the sites you use can launch a targeted phishing attack with a much greater chance of success.
  The NSA, CISA and ODNI, publish a paper that presents both the benefits and risks associated with 5G network slicing. It also provides mitigation strategies that address potential threats to 5G network slicing. The guidance is based on the ESF's potential threat vectors for 5G infrastructure, published in 2021. The Network Slicing technique is especially useful for 5G networks in professional and industrial uses.

MOBILE

Apple iOS

New security features

We close 2022 with iOS 16.2 (second revision of version 16) released on 12 September 2022. Let's take a look at the main security features that iOS 16 has brought us.

The new version of iOS already includes the announced "Lockdown Mode", a special mode of operation in which the system restricts various functionalities that contribute to increasing the surface of exposure to new exploits. This means, that a full application blocks all attachments except for images or the creation of preview links. It is not a mode aimed at the average user, but at an audience exposed to very specific attacks.

iOS 16 incorporates a new feature to alleviate the use of passwords and their many conceptual errors: "Passkey" allows the use of authentication without passwords in services that implement the WebAuth protocol, relying on the biometric verification already provided by the devices, i.e., Face ID and Touch ID.

One of the most attention-grabbing features is called "Rapid Security Responses". It is a new ability of the operating system to install security updates so that an October update is not required. There was a problem in the Mail application that could cause a denial of

update is not required, but more frequent updates as patches become available, as has been the case up to now. Although optional, this is a very interesting option for those who want to apply security patches as soon as they become available without having to wait.

Vulnerabilities

Regarding the release of versions in the second half of 2022, the cycle was opened in August with an emergency update: 15.6.1 fixed two very serious problems that in combination could allow control of the device victim of an attack.

On the one hand, it patched a vulnerability in WebKit (the rendering engine of the Safari browser) that allowed arbitrary code execution. On the other hand, a bug in the system kernel that allowed the same impact was fixed. Both vulnerabilities were detected while they were being actively exploited.

Back in September, just as iOS 16 was released, iOS 15.7, the seventh revision of the system, was released in parallel with a batch of twenty security patches, three of them for remote execution of arbitrary code. Of particular note was the security flaw in the "Neural Engine", a physical component of the system responsible for accelerating the calculations of processes related to machine learning, among others.

iOS 16 was released with as many as 46 security patches, a rather large number for the beginning of its journey. Four of the fixed bugs allowed the execution of arbitrary code.

A few days later a small patch, 16.0.2, was released, but it did not contain any security updates. Likewise, (now with a security patch), the 16.0.3 “Messages” when processing maliciously manipulated mail.

October 24 brings the first major revision of iOS 16. Version 16.1 contained 38 security patches, seven of them fixing vulnerabilities that could lead to arbitrary code execution. For version 15.7, patch 15.7.1 was released a few days later with 18 patches, two of them fixing arbitrary code execution.

In November, an emergency update was released due to two critical bugs in the popular libxml2 library, used by many applications for handling xml files.

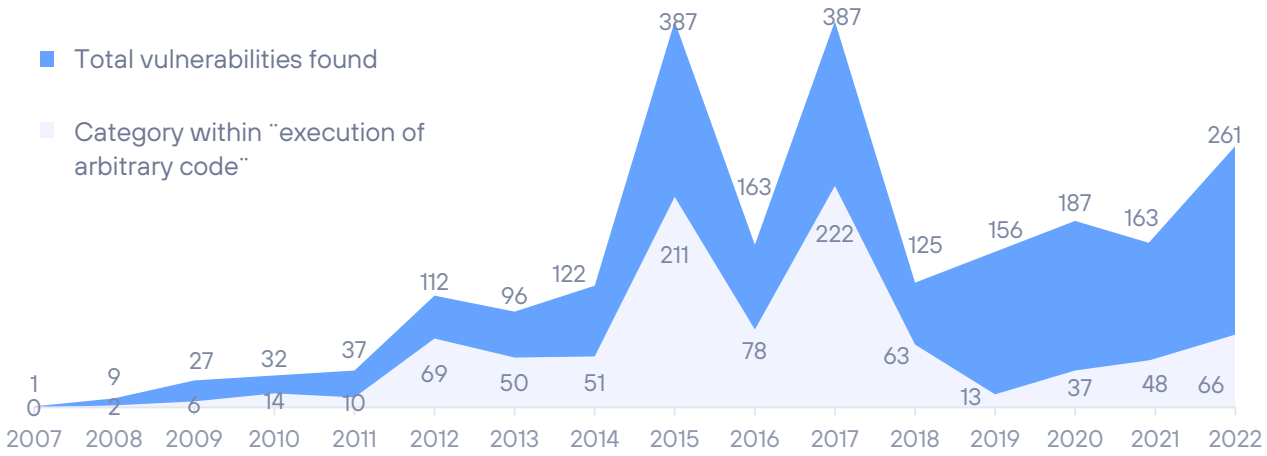
November closed with a scare: an emergency patch for Webkit that was being actively exploited. We jumped to iOS 16.1.2.

In mid-December, and to close the year 2022, patches are released: iOS 16.2 and 15.7.2 respectively. The former with 37 patches, 11 of them relatively serious, and 17 for iOS 15 with seven of them shutting down arbitrary code executions.

Evolution of vulnerabilities in iOS during the second half of 2022

The second half of 2022 closed with 167 unique vulnerabilities patched, around thirty of them considered high-risk, with the possibility of executing arbitrary code. Some of them affecting the operating system kernel itself. This brings to a close 2022 with 261 bugs patched. The annual number of bugs has continued to grow since the peak of 2017.

VULNERABILITIES IN IOS 2022-H2
Annual evolution of vulnerabilities



Fragmentation of versions during the second half of 2022

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.

On the date of issuing, no version fragmentation data was available from Apple, so the figures below are from StatCounter.

As usual in Apple's release cycle, the new version (iOS 16) reaches full user numbers in this half year, with a combined share (16, 16.1, 16.2) reaching almost 60% of the pie. Behind it is iOS 15, with a resistance of 25%, which will fade over the six-month period. Versions prior to iOS 15 already represent a minimal and negligible amount.

Apple currently supports iOS 15 and iOS 16, covering devices from the iPhone 6S (introduced more than seven years ago) to the iPhone 14.

Apple Transparency Report

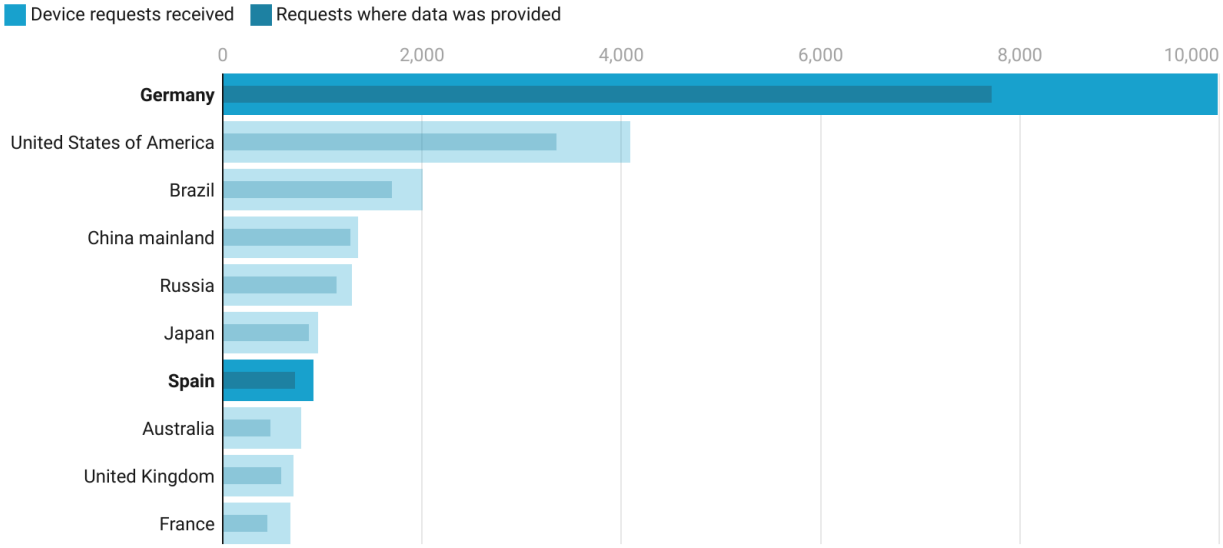
Governments sometimes need to rely on large corporations to help them do their job. When a threat involves knowing the identity or having access to the data of a potential attacker or a victim in danger, the digital information stored by these companies can be vital to the investigation and avert a catastrophe. 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 we have extracted from the information published by Apple for **the first half of the year 2021 (the last published by Apple)** on the activities and requests from governments to the company.

Device-based requests

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

Germany is the country with more device information requests in the first half of 2021

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



The degree of acceptance varies from 60% for Australia requests to 94% for those of China.

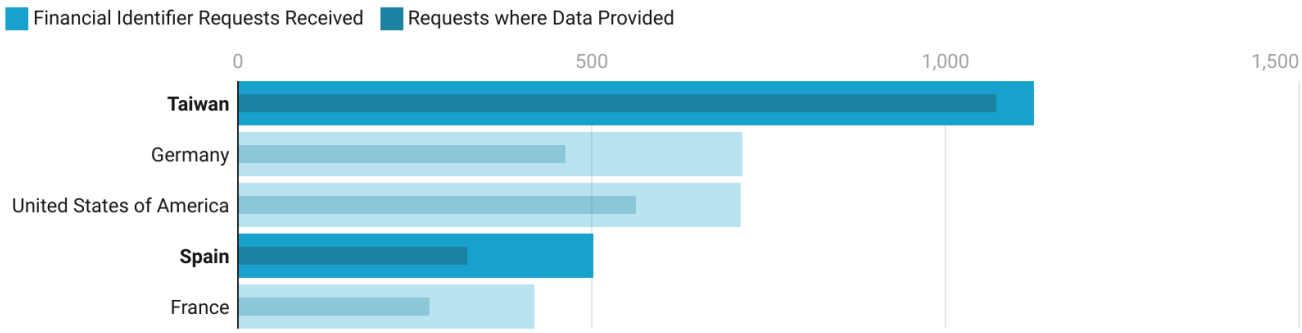
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Requests based on financial data

These requests come about 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 doubles any other country in fraud requests made in the first half of 2021.

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 64% for Spain to 95% for Taiwan.

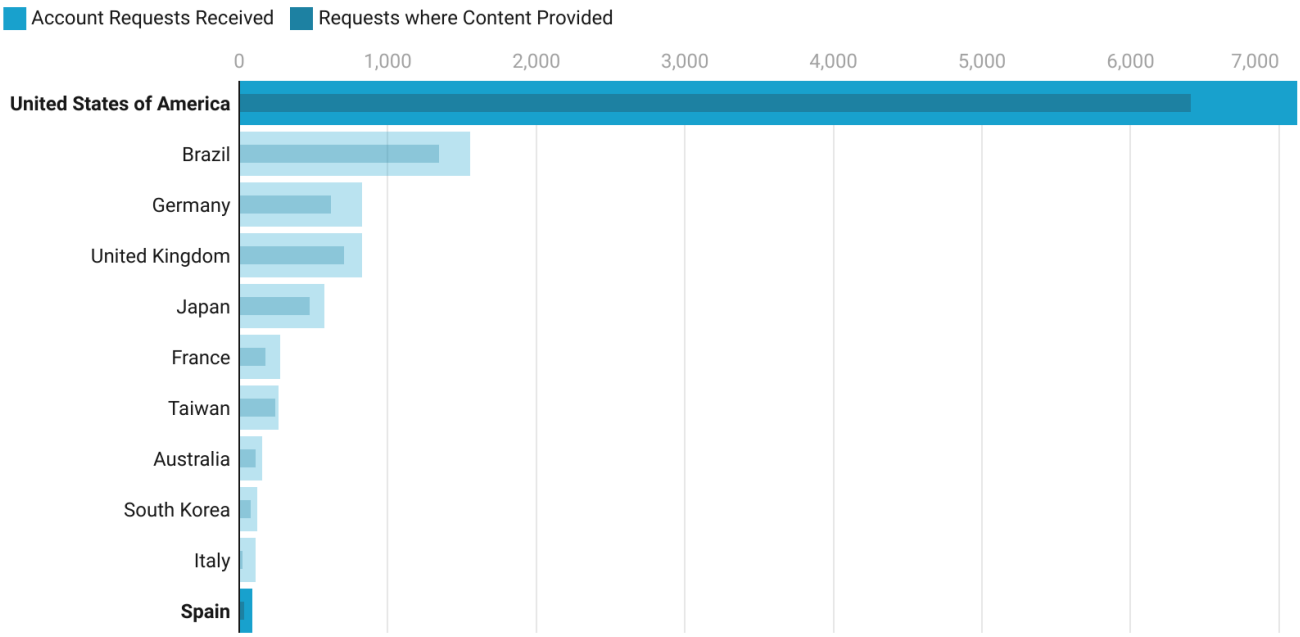
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Account-bassed requests

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

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

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



Out of 93 requests made by Spain only 41 were accepted by apple in the first half of 2021 (44%).

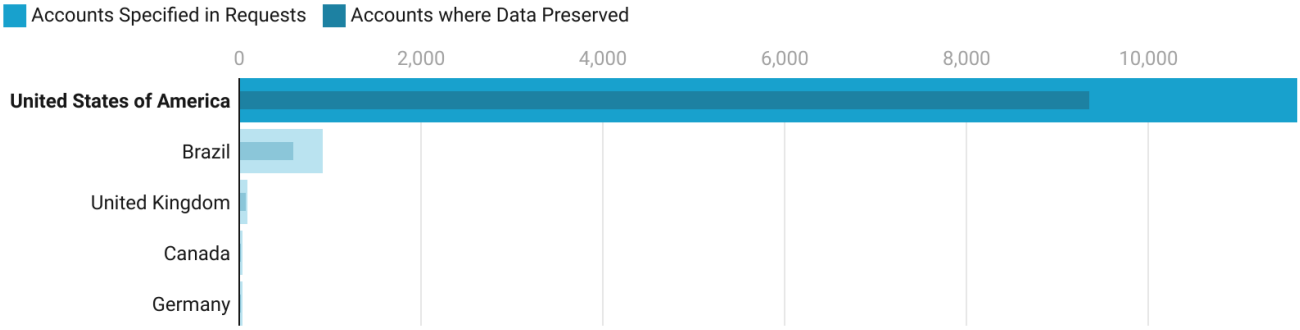
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Requests related to account preservation

Under the context of the U.S. Electronic Communications Privacy Act (ECPA), Apple 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 first six months of 2021.

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



Spain, ranks 30th in number of requests, only a single requests was made and was rejected during the the first half of 2021.

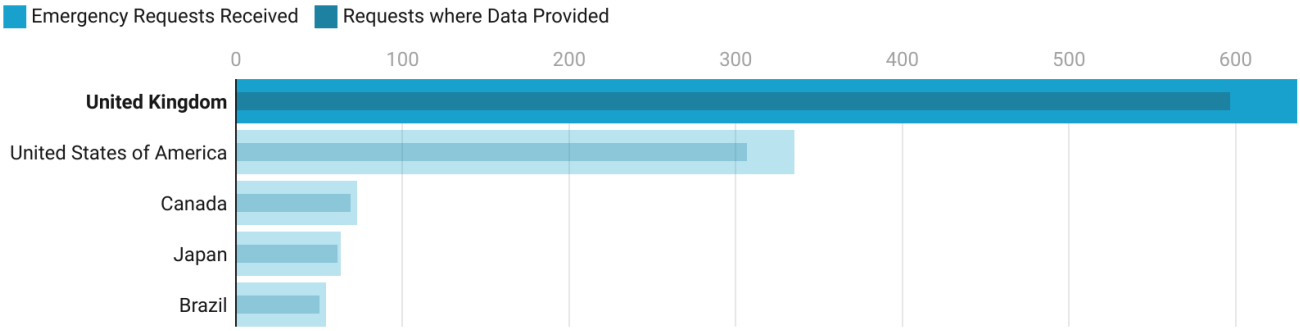
Chart: Juan Elosua • Source: Apple • Created with Datawrapper

Emergency requests

It is also possible, under the U.S. Electronic Communications Privacy Act (ECPA), 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 first semester of 2021

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

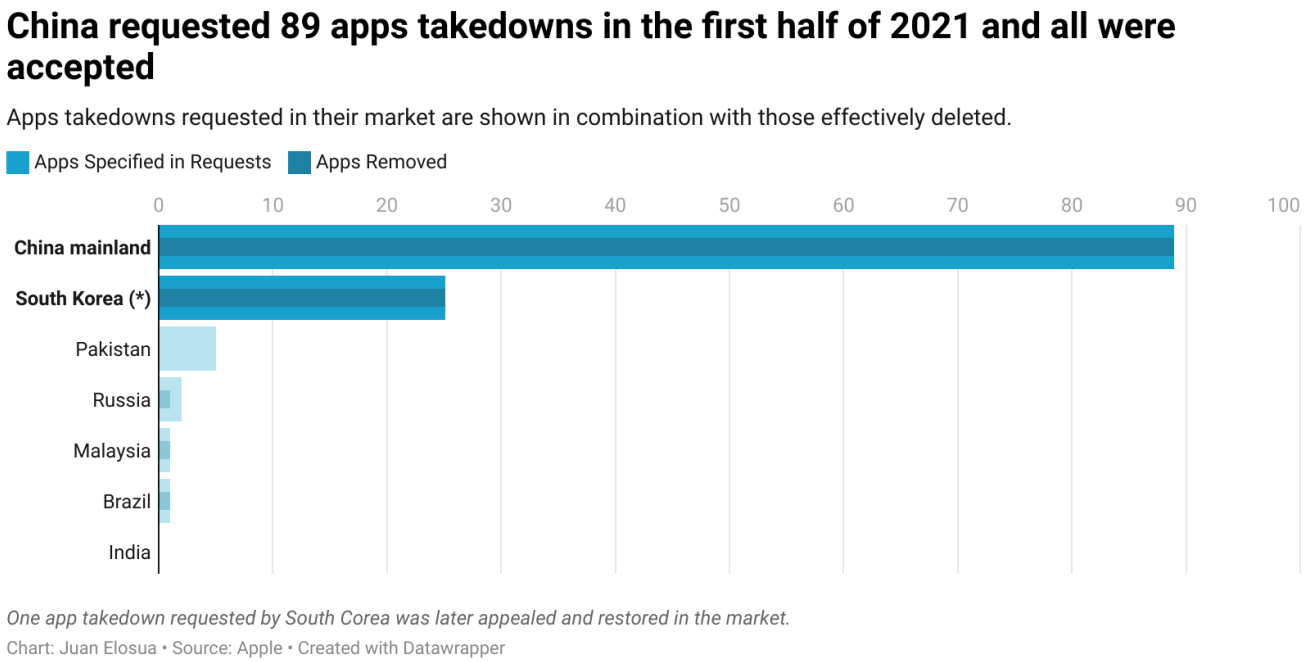


Spain, ranks in position 33 in the first half of 2021, with only 1 request to access accounts due to emergencies that was accepted.(100%).

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

Petitions related to the removal of apps from the market

It usually has to do with applications that are supposed to violate sovereign law.



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 fraud relies more on these locations. Interpretation is free. Some of the conclusions based on the data do seem clear:

- The German government has generated the most requests for device information.
- **Taiwan has substantially increased its requests for fraudulent account information**, with more requests in six months of 2021 alone (1,124) than in all of 2020 (1,030).
- The US requests by far more than any other country for account preservation and access to the data housed therein. **What stands out from our analysis is that Brazil is in a very strong second place with 10 times more requests for preservation and access than the third**.
- **The UK leads since 2020 in requests for access to account information for emergency situations**, those where danger to life or serious harm to individuals can be averted. Surprisingly, given the volumes of US account access, is there a pre-established procedure for launching such requests by its foreign department?
- Unsurprisingly, China is the country requesting the most app takedowns in the App Store. Based on what we observed in 2020, we see a significant reduction in the number of countries requesting app takedowns, mainly in Europe.

Clarification: 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 13 will be released on 16 August. This version is known internally as "Tiramisu". The new features of this major revision of Google's mobile operating system in the security section are mainly oriented towards privacy (always under the spotlight due to the numerous criticisms), as we commented in the previous report.

From this version onwards, it is possible to customise the selection of photos that can be shared per application. It is now possible to choose which photos can be accessed by each application instead of full access to the entire photo library or gallery.

Another privacy improvement is the removal of the requirement to access the user's geolocation when certain applications need to connect to a nearby Wi-Fi hotspot. Apps will now be able to browse and connect to nearby wireless hotspots without having to obtain the aforementioned geolocation.

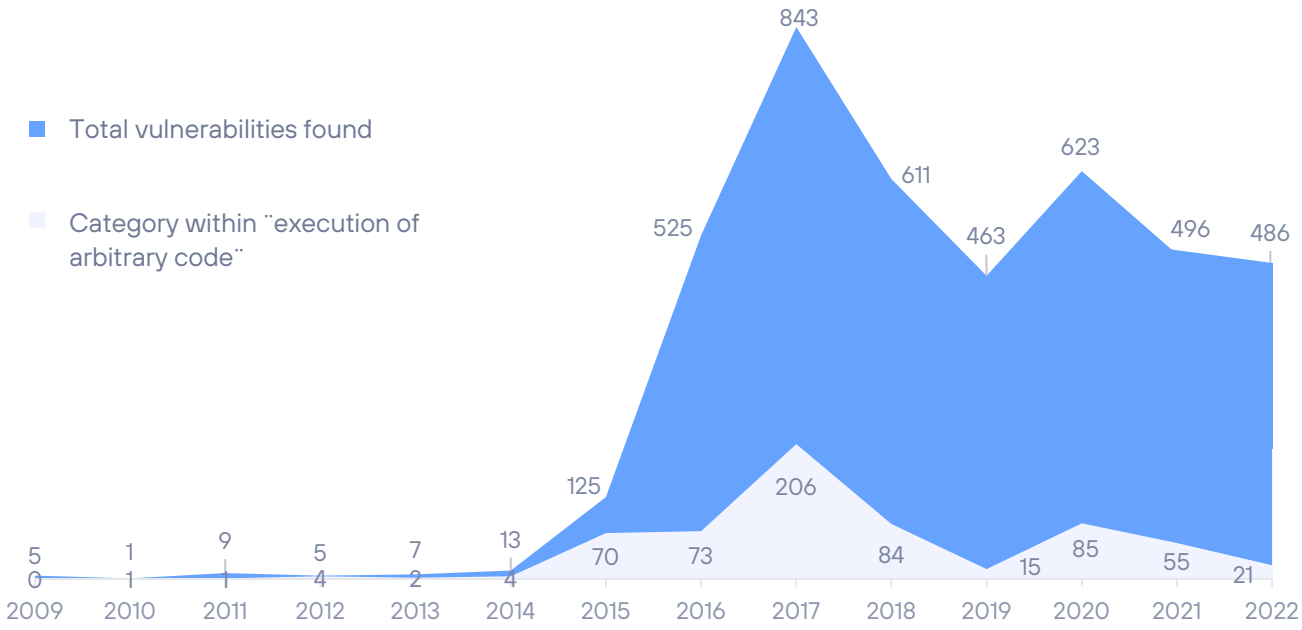
Vulnerabilities

Android releases a set of patches every month, usually within the first week. In total, **256 patches** have been released to fix various vulnerabilities spread across the six bulletins. Of those 256 patches, **14 fix vulnerabilities that have been rated as critical** and could facilitate remote execution of arbitrary code. This brings to almost 500 the number of vulnerabilities patched in 2022. Similar to last year but less serious overall.

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

VULNERABILITIES IN ANDROID 2022-H1

Annualy evolution of vulnerabilities



Fragmentation on Android systems

The latest release from *Statcounter* at the time of writing this report shows that the most widely deployed version of Android is Android 12, with a 28.29% share, followed by Android 11 with a 23.6% share. Practically the same numbers as the previous edition. 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, is only available in a meagre 6.72%, mainly due to the effect we mentioned in the previous paragraph: it takes a very long time for new versions to spread and be adopted by the devices.

The remaining portion is shared by versions below 11. Surprisingly, Android 10 still has a share of 18.38%. A surprising amount for an operating system version that is three years old and still, fortunately, receives security updates.

Alarmingly, Android 9.0 and 8.1 still have a combined share of almost 14%. We say alarming because these are versions of the operating system that do not receive security updates; which is equivalent to saying that 14% of the Android fleet (not counting the percentages of even earlier versions) is vulnerable.

VERSION	PERCENTAGE OF USE
13	**6,72**
12	**28,28**
11	**23,60**
10	**18,38**
9	**8,71**
8	**4,90**

SIGNIFICANT VULNERABILITIES

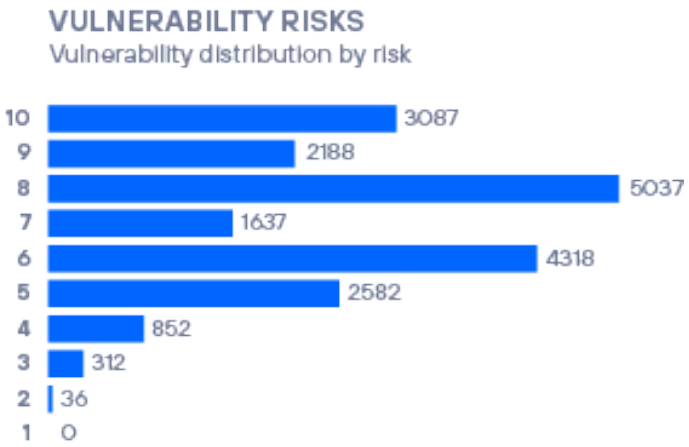
In this section we shall review what we consider to be some of the most significant vulnerabilities in the second half of 2022, i.e., those that stand out due to their particular relevance or danger.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2022-34265	Django framework	SQL injection in the Trunc() and Extract() functions allowed to take control of the system.	9.8
CVE-2022-2385	Kubernetes	A flaw in the IAM authentication process used in Kubernetes could allow an attacker to bypass existing protections against replay attacks.	8,1
CVE-2022-26138	Confluence	Confluence used a hardcoded password in the system that could be exploited remotely to log into Confluence and access any page to which the confluence-users group has access.	9.8
CVE-2022-27255	Realtek	Code execution on Realtek RTL819x chips related to network devices, due to a buffer overflow in SIP processing	9.8
CVE-2022-36804	Bitbucket	Command injection via HTTPs	9.9

CVE-2022-40684	Productos Fortinet	Restriction bypassing when authenticating through APIs	9.6
CVE-2022-4135	Chrome	New 0-day in Chrome, the eighth of the year. Code execution with sandbox exit.	9.6
CVE-2022-37300	Siemens: Varios	The forgotten password recovery mechanism could allow an attacker unauthorised access to the controller, in read/write mode, when communicating via Modbus.	9.8
CVE-2022-40674	Profinet SDK	A vulnerability has been identified in the Expat XML parser library (libexpat) that could allow arbitrary code execution.	9.8
CVE-2022-3214	Delta Industrial Automation: DIAEnergy	This industrial power management system allows the use of plaintext credentials that would allow remote code execution by uploading executable files in certain directories.	9.8
CVE-2022-3485	IFM: Moneo Appliance	An unauthenticated attacker could reset the administrator password by simply entering the device's serial number and gain full control over the device.	9.8

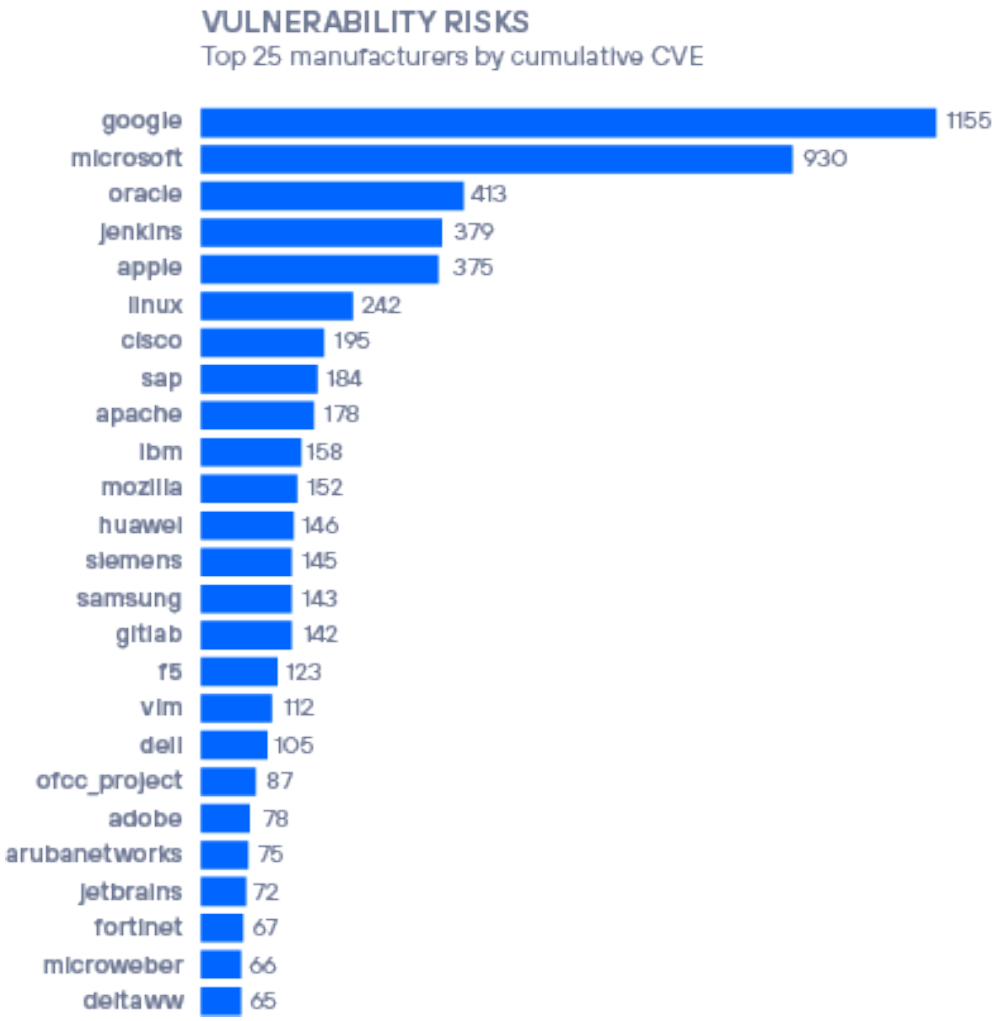
Vulnerabilities in figures

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 cumulative CVEs

During the second half of 2022, Google led by far in terms of the number of known vulnerabilities, followed by Microsoft. In general, it is common for the big three to always be among the top three in terms of number of vulnerabilities.



APT OPERATIONS, ORGANISED GROUPS AND ASSOCIATED MALWARE

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

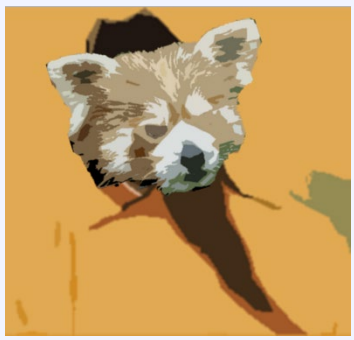
We note that the attribution of such operations, as well as the composition, origin and ideology of organised groups, is complex and cannot necessarily be completely reliable. This is due to the capacity for anonymity and deception inherent in this type of operation, in which actors may use means to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

Notable APT activity, detected during the second half of 2022.

Emissary Panda: They never deliver good news

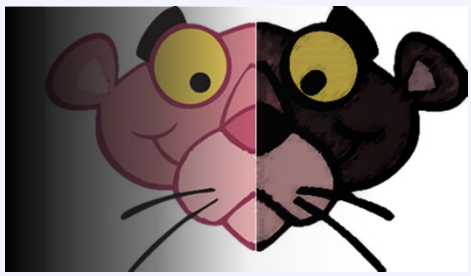
Belgium's foreign minister indicated in July that groups backed by the Chinese government had attacked his country's defence and interior ministries.

The Belgian government representative pointed to several APT groups, although one of them had already been mentioned earlier in the year. Specifically, this "Emissary Panda", which had been detected by German intelligence services using the HyperBro RAT in several commercial organisations to spy, infiltrate customer networks and steal trade secrets and intellectual property.



More information: https://diplomatie.belgium.be/en/news/declaration-minister-foreign-affairs-malicious-cyber-activities

Dark Pink: Smooth criminals



This group has been discovered by Group-IB researchers. The analysis, based on the second half of 2022 (although actions are suspected as early as mid-2021), has detected TTPs that are different from other existing groups, customised tools and a clear focus on military targets, ministries and government agencies.

So far, the activity attributed to them has been actions against military agencies in the Philippines, Malaysia (three times in two months) and governmental organisations in Bosnia and Herzegovina, Cambodia and Indonesia.

However, as new as they are, the initial attack vector is not new. A well-cooked spear-phishing attack..

More information: https://www.group-ib.com/media-center/press-releases/dark-pink-apt/

Polonium: Poisonous and sinister

This group, reportedly located in Lebanon but working in coordination with other Iranian-sponsored groups, was first documented in June 2022 by researchers at MSTIC (Microsoft).

Its targets have been organisations in Israel, with activity recorded from September 2021 and throughout 2022 in more than 20 organisations in various sectors, including defence. Although it uses its own tools (CreepyDrive, CreepyBox, Creepysnail...), it shares TTP (and targets) with some Iranian groups, such as Mercury.

This group mainly uses (from the name of the tools, one can guess) the OneDrive and DropBox storage services for C&C actions and exfiltration of information.

More information: https://www.bleepingcomputer.com/news/security/hacking-group-polonium-uses-creepy-malware-against-israel/

GhostSec: Who are you going to call?

As an illustration of this group, we cannot think of anything better than a real ghost. A self-described "cyber security expert".

This Palestinian group is, however, quite knowledgeable. In September, it was detected several times attacking Israeli targets. First, Otorio's group of researchers reported that this group claimed to have hacked 55 Berghof PLCs on Israeli territory.

A fortnight later, they again announced a successful attack. The compromise of a water purification plant. They also published screenshots of the system and claimed that they could go much further and poison the water if they wanted to, but that this was not their goal.

More information: https://www.securityweek.com/hacktivist-attacks-show-ease-hacking-industrial-control-systems

OT THREAT ANALYSIS

The following information comes from **Aristeo**, a system for capturing and analysing threats in the OT domain. 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 decoy-nodes, 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-signature has its own characteristics and reproduces a different process. Therefore, the protocols, devices, productive sectors... change in each one of them. Furthermore, the nodes are alive, which means that they can undergo alterations in their configuration at the will of the team of researchers working with them, or of the client who has temporary or permanent use of them. This variability may lead to slight discrepancies in the data shown in this section when compared between semesters.

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

Data analysis

This semester, as a specific case, we are going to comment on an interesting situation that caught our attention during the provision of a service to a client in Northern Europe. Specifically, we will discuss how we perceived the change in the global axis of cyber-attacks depending on the location of the attackable assets. The project required us to change the location (at a logical level) of one of our nodes to the one suggested by the customer, in a central-eastern European country. In this story, we focus on one of the main attack vectors, because of its simplicity and cost-effectiveness: brute-force access against RDP.

Below is a comparison between access attempts to the engineering bay (the industrial system's control PC) of the node while it was deployed in Spain and during its (temporary) stay in France. The lists have been compiled for 7 days and the 10 highest values are shown by number of attempts.

SPAIN	FRANCE
scada1\ad	scada1
scada1\us	administr
administr	hello
hello	scada1\ad
scada1\sc	user cont
admin	usercontr

user	user.cont
raquel	u.control
david	domain
laura	test

There are a number of things that are striking about the TOP 10:

- The similarity is striking. Thirty per cent of the passwords attempted are identical but in different orders.
- 40% have a certain relationship or similarity between them.
- 30% are... personal names?

Indeed, when we started going down the list, we stopped seeing "generic" passwords and started finding proper names. As soon as we located the node in France, the names started to change. Thus, from the tenth result onwards, we began to see "emanuel", "guillaume", "isabelle", etc., typical of the Gallic country. Some of them would be in the TOP 10 were it not for the results showing different iterations between "user" and "control".

We cannot give you specific data about the country where our client asked to locate the node, but we can tell you that the first four names we found were the four most used names in that country, according to their own "INE" (National Statistics Institute) as we officially consulted the country's organism to support our theory.

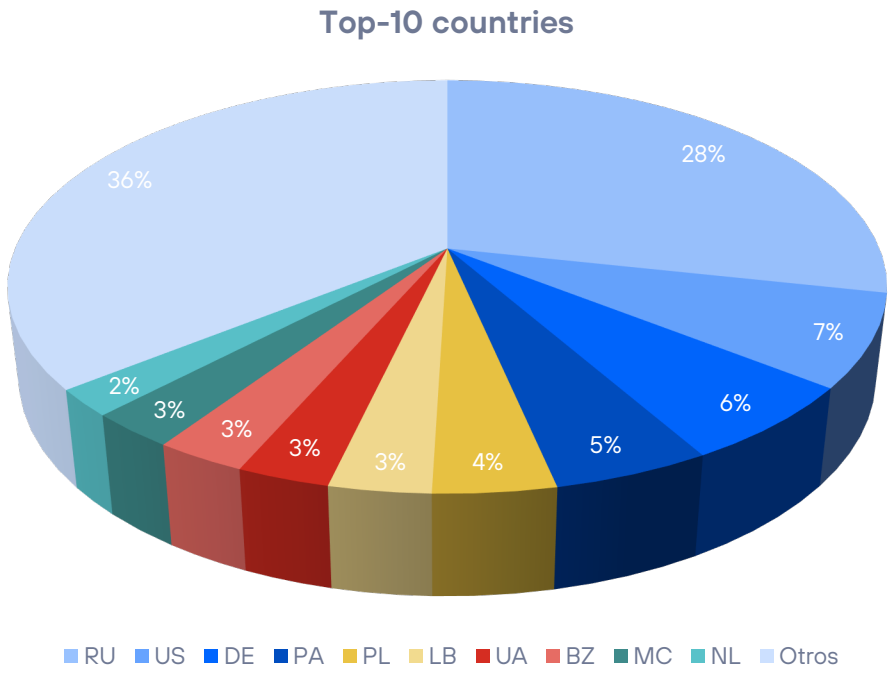
This type of circumstance, besides being very curious, hints at something we have highlighted in other reports. The attacker knows very well what he is doing, against whom he is doing it and where his target is. In fact, although the engineering bay is still a PC, the access attempts show that the attackers were very clear that it was an embedded element of an industrial system. These are advantages of using real industrial systems.

As you scroll down the list of access attempts, you also start to see default credentials for various industrial and IIoT (Industrial IoT) devices that are not present in our industrial system. This gives us a very clear indication of the attackers' TTPs at a general level: automated reconnaissance tasks largely, but not mostly, first go through a system identification (OT-IIoT) and then a generic brute-force attack. They don't go as far as digging into what kind of system they have encountered. Probably because **they are so successful that they don't need to improve the effectiveness and efficiency of their automated systems**. And that's... scary.

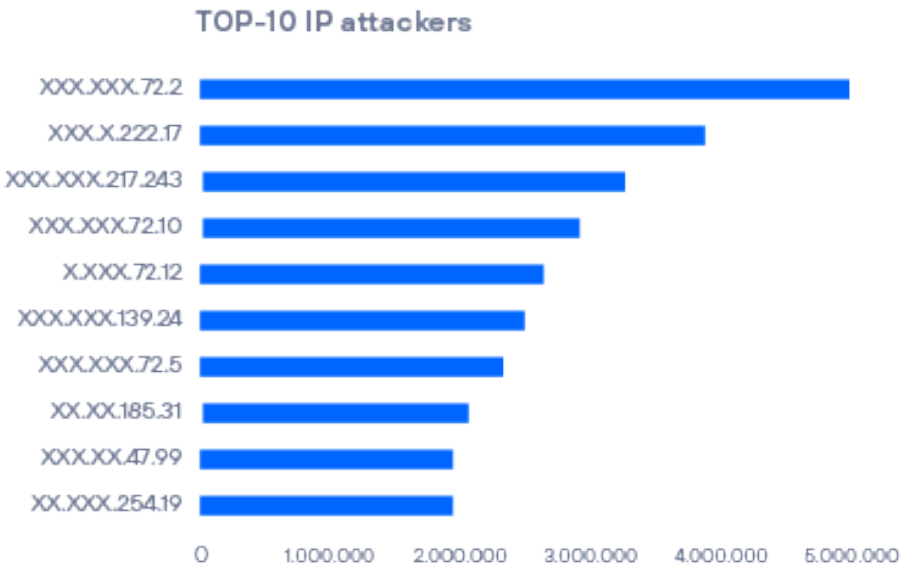
And now, we turn to the general statistics of the information recorded. In the second half of 2022, **more than 291 million cybersecurity events were detected**. This is a decrease compared to the data recorded in H1 2022 and 30% less compared to the same period last year.

Even so, the total number of events detected in 2022 was more than 706 million, higher than in 2021.

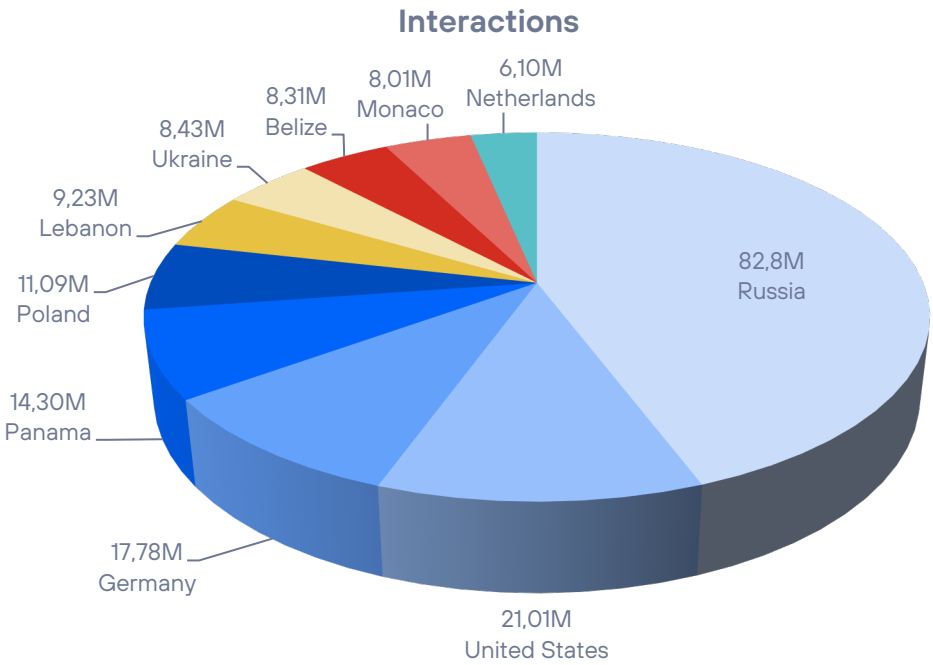
The distribution by country is as follows:



Let's now look at the ten IP addresses with the most interaction with the Aristeo system. 70% come from various Eastern European countries. Not a single IP address belongs to a country outside the European geographical location. This is especially striking because it is common for IP addresses from such important nodes for internet traffic as the United States.



Below, we can see how the countries with the greatest presence in our Aristeo are distributed. The entry of Belize in this list in the previous semester was already striking, but the presence of Lebanon is not far behind in the ranking of surprises either (or not so much, when all the data is available).



INDICATOR-BASED THREAT ASSESMENT

We have conducted, in collaboration with **Maltiverse**, a ranking study of the indicators of compromise detected on their platform. This is to indicate interesting attributes of maliciousness detected in IP addresses, domain names and URLs over the last six months..

What kind of maliciousness do the URLs studied involve?

Out of more than 650,000 urls studied, almost 66% were malware download points. In other words, once the URL was visited, the resource obtained was malware: either a Trojan, exploit or any binary classified as such.

Following malware, **which is always closely related to URLs, is phishing**, which accounts for 30%. These are URLs that at some point have been related to phishing. A URL that sent the victim to a forged site in the hope that they would hand over their credentials, financial passwords or similar deception.

URL	
Malware download	66%
Phishing	30%
Beacons	4%

The rest of the URLs fit into the concept of malware-related infrastructure. For example, almost 4% of the URLs belonged to beacons of the Cobalt Strike pentesting framework. They would fall under the heading of malware hosting, but with a more specific use.

What can we find regarding the registration of domains associated with malicious activity?

There are key moments in the life of a malicious domain, for example: when it appears in an infrastructure and is not registered; when it is registered but not active; and finally, when it is active and provides some malicious capability. **Almost 72% of the domains detected or involved in infection campaigns were active at the time of detection**.

Most of the domains have been used for operations related to phishing attacks or campaigns. **Some 40% of the domains were involved in spoofing sites to steal credentials**.

Almost 30% of the domains studied belonged to bot control centres. The control centre is the server to which infected nodes or systems go to obtain orders to coordinate joint actions, among other operations

DOMAINS	
Bots	29%
Distribución malware	26%
Phishing	39%
Otros	6%

Where malicious IP addresses are geolocated?

The final destination of the traffic produced by a malware architecture will always be an IP address. Whether directly, by indicating the IP address itself in the URL, or through domain resolution, we will always come across a server hosted somewhere that responds on a specific IP address.

Since IP addresses are linked to their networks and these have a physical location, it is quite easy to draw conclusions about the geopositional distribution of IP addresses on which malicious activity has been detected.

Out of a total of more than 450,000 IP addresses collected, the top 10 countries with the most IP addresses appearing in these positions are:

IP COUNTRIES	
United States	18,08%
India	10,90%
China	10,32%
Taiwan	4,48%
Russia	3,67%
Germany	3,33%
Brazil	3,05%
Vietnam	2,34%
Pakistan	2,27%

Thailand	2,26%
Other	39,30%

This group represents 60% of the total, while the rest, 40%, hold percentages that are not significant or less than 2%.

Typology

Although the same IP address can have more than one classification (i.e., the same IP address can contain, for example, a spam system and later or concurrently serve as a C2).

Slightly more than 68% of detections are IP addresses that are considered bots. In other words, infected machines or systems. A bot is a malware-infected computer under the control of a botnet. The use to which this botnet can be put is discretionary: from mining cryptocurrency, attacking a target with mass requests to create a denial of service, or simply hosting malware or phishing for further attacks.

Some 20% of IPs have been seen performing some form of brute force against authentication systems. This is, for example, making thousands of requests with username and password combinations against an SSH server. If one of these combinations is accepted by the server, it would mean the compromise of the server or at least access with the credentials and permissions granted by the hijacked account. It is a clear exploitation of a simple and expensive oversight: changing default credentials or weak passwords to more robust ones.

About 8% of these IPs have been categorised as malware distributors. That is, they host malware available for download by victims who have been infected. When it comes to infections, it is common that the victim is first infected by a downloader that, once inside the system, downloads the final malware. These IPs have been observed hosting malware or being part of download points.

Almost 3% of the IPs are involved in a case of SPAM or, in other words, mass distribution of unsolicited mail. In other words, at some point, 7% of IP addresses have been classified as mail servers. A tireless and always profitable evil for criminal organisations. In addition to being one of the main vectors through which malware enters.

IP	
Bots	69,00%
Brute force	20,00%
Malware download	8,00%
SPAM	3,00%

any given time serve as a point of downloading malware, hosting phishing, or sending unsolicited emails or equally: spam along a timeline. In other words, an infected node or machine is in the end a multi-purpose service under the control of a criminal organisation that decides, depending on the needs of the organisation, to which it dedicates the systems under its control.

SUMMARY

Overall increase in the number of vulnerabilities fixed in iPhone. From 125 in 2018 to 261 in all of 2022. The number of serious bugs also increases to 66. On Android, on the other hand, the trend is stable, with similar numbers since 2021 at around 500 bugs. 2022 has been one of the years with the lowest number of critical vulnerabilities.

Regarding Apple's transparency report, we must talk about data from the first half of 2021 (the last one published by the company). It is interesting to note that Germany is the country that has made the most requests for device information, while by far the United States is the country that has made the most requests for account information. As usual, China is the country with the most requests to remove apps from the market.

Microsoft, Google, and Oracle are the companies with the most bugs fixed, as usual, although sometimes swapping order. Jenkins ranked fourth in the previous six months for the first time and remains there. It is closely followed by Apple.

Regarding OT security, we show how attackers are very aware of where potential victim machines are located and use country-specific idiosyncrasies. For example, in the use of proper names for brute force, they consider usage statistics to maximise the likelihood of success.

We inaugurate in this report the collaboration with Maltiverse. We can conclude from their systems that most of the infrastructure considered malicious is used to download malware (66%) and that the majority of malicious domains are also related to bot control centres (30%). Most of the infrastructure tends to be located in the US. This may be related to the abuse of legitimate infrastructure that is fashionable among attackers, precisely to avoid being blocked by security measures.

USEFUL LINKS

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

IDENTITY

How to protect your social media accounts

Are we really shopping " securely " on the internet?

CRIPTOGRAPHY

Google takes a step to improve Certificate Transparency's ecosystem: No dependence on Google

MALWARE

DGA o no DGA, esa es la cuestión

Name the malware you have, and I'll tell you which botnet you belong to

Understanding the dynamics of Ransomware security incidents