Telefónica Tech

Security Status Report 2024 H2

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

telefonicatech.com

Índex

EXECUTIVE OVERVIEW

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

Two major news items stood out during the second half of 2024. On July 19, a worldwide technology outage occurred. Around 8.5 million Windows systems started rebooting with blue screens, over and over again, with no remote remedy to fix them. The headlines went ahead: a bug at Microsoft. However, shortly after, CrowdStrike admitted that its Falcon product had suffered from a faulty update that, when executed in the kernel, caused this serious error.

This incident went beyond the one-off problem that occurred that day. It raised serious questions about the responsibility of a cyber security vendor in Windows: how could a bug in a single product paralyze half the world? How far could Windows be held responsible for allowing unvalidated content to run in the kernel environment? Shortly after the incident, the accusations and even lawsuits for losses began.

As a consequence, the positive thing is that Microsoft itself is considering restructuring its own EDR integration system, so that this cannot happen. After all, the dichotomy is clear: Crowdstrike wanted to upgrade fast to protect more, but fast and good are often opposing characteristics.

We will see direct consequences of this problem in the years to come, both in the design of Windows itself and in the design of EDRs.

On the other hand, Ivanti, Cisco, Fortinet, PaloAlto... companies that protect the perimeters of millions of companies have once again suffered very serious vulnerabilities, much more frequently than desired. Ivanti, in particular, has suffered a series of disastrous 0-days throughout the second half of the year, most of them found, (as the term 0-day itself indicates) while being exploited by attackers.

These two outstanding observations during the half year should make us reflect on the problems arising from the protection systems themselves, which deserve special attention. It will not be possible to prevent them from being breached, but at least a more secure management is possible, allowing prior bastioning and a rapid response in the event of an incident.

In the end, it all comes down to the eternal question: who watches the watcher?

Whether you are an amateur or a professional, it is important to be able to keep up with relevant cyber security news: what is the most relevant thing going on? What is the current landscape? This report will provide the reader with a tool to understand the state of security from different perspectives and will also provide insight into its current state and project possible trends in the short term. The information gathered is based in large part on the compilation and synthesis of internal data, contrasted with public information from sources we consider to be of quality.
Here we go!

HIGHLIGHTS OF THE SECOND HALF OF 2024

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

JULY

- **CrowdStrike Falcon EDR**: A faulty update of CrowdStrike affected more than 8 million Windows systems. The incident caused quite a stir both in worldwide operations and in media reports of all kinds. From a global attack to failure at Microsoft itself (since it manifested itself with the famous blue screen). CrowdStrike Falcon is a company-focused EDR, so the incident brought down essential IT systems globally.
- **Major vulnerability in a WordPress plugin**: The WPScan team discovered a major vulnerability in a **popular WordPress plugin called Profile Builder** and its commercial version, Profile Builder Pro. The vulnerability **allowed malicious actors to gain admin access without having any account on the site**.
- Telephone fraud group arrested: **Spanish and Portuguese security forces arrested 54 individuals suspected of stealing 2.5 million euros from elderly people using telephone scams**. The group operated by contacting victims by telephone and posing as bank employees. They convinced users to reveal bank credentials or hand over their savings to a courier who showed up at their door. The stolen money was then laundered through the group's network of bank accounts.
- **ServiceNow vulnerability**: CISA and several security companies warned that two ServiceNow vulnerabilities that were reported by AssetNote on July 11 are being actively exploited, including the critical vulnerability CVE-2024-4879. **These vulnerabilities allow attackers to access databases and exfiltrate data, as well as read arbitrary files**. The researchers warn of between 13,000 and 42,000 vulnerable ServiceNow instances spanning both private and public sectors.
- **Bottleneck in NIST vulnerability processing and enrichment**. The National Vulnerability Database (**NVD**) has been accumulating a significant backlog since February and, although the hiring of a new vendor was announced in May, the *backlog* has continued to grow to more than **17,000 unprocessed vulnerabilities**. This **impacts vulnerability management in the global cybersecurity community**, which relies heavily on this information **to help inform customers on which bugs to fix first**.
- **The U.S. cyber security agency, CISA, issued an advisory detailing,** among others, a set of exploits of the Honeywell ControlEdge Virtual UOC industrial controller. This system is a Linux-based virtual machine that eliminates the need for a physical controller. An attacker could take full control of the controller and access to the entire OT network where the controller is located.

AUGUST

- Exploit for RCE vulnerability in Windows: A Proof-of-concept (PoC) code was published this month on GitHub for **the remote code execution vulnerability in the Windows TCP/IP stack**, **affecting IPv6-enabled systems**. Identified as CVE-2024-38063 and with a **CVSSv3 of 9.8** according to Microsoft, it **allowed attackers to exploit Windows 10, 11 and Server systems without requiring user interaction by sending specially crafted IPv6 packets** that trigger a buffer overflow.
- **Generation of QRs with Unicode**: Attackers create an innovative method to create QRs with Unicode characters to fool email protection systems. Unicode characters allow the sequencing of black-on-white "block" characters of different sizes that, perfectly aligned, will form a QR perfectly identifiable by any camera. **However, for the mail analysis system, it will no longer be neither a URL nor an image, but text again, and it will be, for now, impossible for it to deduce that a QR code is hidden in this combination of "blocks"**.
- On the one hand, **Digicert** is forced to revoke more than 83,000 certificates of almost 7,000 customers within hours due to a security check failure. On the other hand**, it has had to postpone the revocation and extend the deadline for accepting exceptions in critical infrastructures**.
- AMD *Sinkclose* Attack: Security researchers discover a security flaw in AMD processors, called Sinkclose, with identifier CVE-2023-31315. This vulnerability affects almost the entire line of AMD CPUs since 2006. The vulnerability allows attackers to execute malicious code in the chip's privileged System Management Mode. Although initial access is required, *Sinkclose* allows the installation of deep-rooted *malware* that can survive OS reinstallation and be extremely difficult to remove.
- **Pavel Durov, CEO and founder of Telegram arrested in France**: French authorities detain Telegram CEO and founder. Durov was arrested in an **investigation related to the lack of content moderation on Telegram**. The popular instant messaging service is increasingly being used for criminal activity: stolen personal data, stolen cards, *malware* and other illegal content.
- Researchers at the University of California have discovered a vulnerability in Shimano's wireless bicycle shifter. It is not complex and can be performed at a distance of up to 9 meters. The attacker takes full control of the shifter: he/she can change gears or lock the shifter in a particular gear.

SEPTEMBER

- **Pager explosions in Lebanon**: Thousands of people were injured after pagers, allegedly used by Hezbollah members, exploded. Subsequent reports seem to indicate that this was not the case and that the reality was that a shipment of pagers was intercepted, and explosive charges were added that could be detonated remotely.
- **MC2 Data Leak**: The MC2 Data background check service **exposed** a database server containing the personal data of more than **100 million U.S. citizens**. CyberNews reports that the 2.2TB database contains extremely sensitive information, ranging from **names to property records, employment details, and legal documents.**
- Compromised Kia cars: A team of security researchers found a **vulnerability in Kia's web portal that allowed them to take control of millions of the company's cars**. The researchers built a custom tool that gave them control over key car functions. This included the **ability to unlock doors, sound the horn**

or start the engine. The research team notified Kia about the flaw in June, and the company patched its web portal in August.

- Critical Linux vulnerability in the Common UNIX Printing System (CUPS): this vulnerability allowed attackers to execute commands on a target computer via malicious print jobs. The vulnerability requires specific conditions to be exploited. Likewise, Akamai has discovered that the CUPS system can be abused to launch large-scale DDoS attacks. An attacker can send a single packet to a CUPS server that will amplify and relay it to a desired target.
- Kemp Technologies fixes a major vulnerability in its *LoadMaster* load balancing appliances that can allow malicious actors to execute malicious code on the appliance. Identified as CVE-2024-7591, the vulnerability is an input validation error in the device's management panel and can allow malicious actors to execute operating system commands. Kemp released a security update last week and encouraged customers to update before the vulnerability is exploited in the environment. **It received a severity score of 10/10 due to its ease of exploitation.**
- **Australia introduces *anti-doxxing* law**: Australia's Attorney General introduces a bill that will prohibit the publication of personal information online, also known as *doxxing*. The proposed law amends the Australian Privacy Act 1988 and imposes a prison sentence of up to seven years for offenders. This government also plans to introduce novel legislation to introduce a minimum age for the use of social networking sites.
- The U.S. cyber security agency, CISA, has reissued an announcement warning of the relative ease with which industrial systems can be successfully attacked, in addition to their simplicity. This announcement was preceded by the cyberattack on the Arkansas City water plant, population 12,000. The plant had to revert to manual operations after losing control of its systems.

OCTOBER

- Of course, attackers will use AI to make their social engineering attacks more realistic. But also, in a much simpler and cheaper way, as a social engineering claim in itself. That's what the FIN7 group thought and, after many years preparing sophisticated campaigns, found an interesting formula to infect their victims. It has been made public that FIN7 is using at least seven websites advertising AI nude generators as a lure to trick victims into getting infected with *malware*. It is offering a free trial of AI nude generator software containing a version of NetSupport RAT.
- A **vulnerability affecting many thousands of traffic lights in the Netherlands** is defected **and will require manual replacement as the only possibility for remediation**, a high-cost project, which the Dutch government has estimated will take six years until 2030.
- The EU Council approved the Cyber Resilience Act. The new law introduces minimum cybersecurity requirements for digital products sold in the EU. Under the new rules, vendors must provide free and automatic security updates, support products for at least five years and manage a vulnerability disclosure program. Companies must also notify the EU cyber security agency when a vulnerability is exploited in their products. **Products that meet the CRA's minimum requirements will be able to place the CE mark on their product label.**
- New ***Passkey* Migration** Specification: The **FIDO Alliance** is publishing a new specification for a new technology that will allow users to easily move passkeys between platforms and vendors.

Currently, when a user wants to transfer credentials from one credential manager to another, the transfer is usually done in an insecure and unclear manner.

- **CISA Bad Practices Guide**: In an unusual twist (usually highlighting and recommending good practices), CISA publishes a "guide" to the most common bad practices that software vendors are still incurring, in the hope that companies will feel pressure and start adopting a Security by Design approach.
- New **DDoS record blocked by Cloudflare**: During a distributed denial-of-service campaign targeting organizations in the financial services, internet and telecommunications sectors, volumetric attacks peaked at 3.8 terabits per second, the largest publicly recorded to date. The assault consisted of a "month-long onslaught" of more than 100 DDoS attacks. **Cloudflare mitigated all DDoS attacks autonomously and noted that the one that peaked at 3.8 Tbps lasted 65 seconds**.
- A report published by OpenAI reveals that the artificial intelligence company has disrupted more than 20 cyber operations since the beginning of the year, including the activities of Iranian and Chinese state-sponsored APT-Groups. The groups were detected in several attacks on water plants in Iran and the US.According to OpenAI, the associated accounts used ChatGPT to perform reconnaissance, but also to assist them with vulnerability exploitation, detection evasion and post-compromise activity

NOVEMBER

- **Google AI finds a vulnerability in SQLite**: Google with its Big Sleep AI system finds its first valid vulnerability in a real-world project: the SQLite database engine. The vulnerability was described as a buffer overflow. The problem was found in a development version of the database and was fixed before the vulnerable code was shipped to consumers.
- **Security breach at Finastra**: Finastra, a supplier to 45 of the world's 50 largest banks, acknowledges an incident. An attacker accessed and stole a large batch of the fintech company's internal files. The company says the attacker did not deploy *malware* or tamper with customer files. The company's data was put up for sale on a popular dark web forum.
- **Secret iPhone reset feature**: Apple has added a secret feature that restarts iPhones that have not been unlocked for a period of time. Resets put devices into a state where the phone's data is more difficult to obtain. The feature was added in iOS version 18.1, This feature was discovered by law enforcement after the iPhones of detained suspects mysteriously rebooted while in custody. Read more here.
- New **Android scam detection goes live**: Google is rolling out a new security feature in Android that listens to on calls and warns of potential scams. The feature was announced earlier this year at the Google I/O conference. At the same time, O2 has developed an Artificial Intelligence system to waste the time of scammers....
- Palo Alto fixes two 0-day vulnerabilities in its NGFW firewalls. The first, identified as CVE-2024-0012, CVSSv4 of 9.3 according to the vendor, is an authentication bypass flaw that allows attackers to gain administrative privileges. The second is a bug that allows privilege escalation to *root*.
- **Major authentication vulnerability in a WordPress plugin**: Security researchers discover a vulnerability in a **WordPress security plugin installed on more than 4 million websites**. The bug

is an authentication omission in ***Really Simple Security*** and **allows attackers to access any account on a WordPress site, including the admin account**, due to an error in handling an invalid login *nonce* in the 2FA procedure. Wordfence researchers described the bug as **"one of the most serious vulnerabilities" they have reported in the company's 12-year history**.

- **Japan**'s Consumer Affairs Center **has urged citizens to plan for their "digital end of life,"** recommending that they share access to devices, maintain password lists and **designate digital heirs** to manage subscriptions.
- A 59-year-old U.S. citizen was sentenced to 4 years in prison for conspiracy and espionage. Ping Li, from Florida, sent information to the Ministry of State Security (China) while working for companies such as Verizon and Infosys. According to the conviction, Li shared information about Chinese dissidents, members of religious groups of interest in China and US-based NGOs. He also shared training information (Verizon and cyber security) and information about the Solarwinds cyberattack.

DECEMBER

- **Windows hacking**: A team of software crackers claims to have cracked "*almost the entire Windows and Office software license protection scheme*". This group claims that their circumvention method can **work natively** without the need for third-party software. The group has tested the technique to activate licenses for Microsoft Office, Windows 7, Windows 8, all editions of Windows Server and security updates. **If confirmed, the technique is set to trigger a new boom in Windows piracy**
- Blockchain attack: new attack affecting the open-source library 'solana-web3.js'. The *javascript* library is used to write decentralized applications on the Solana *blockchain*. The backdoor was introduced in a commit after gaining access to the repository through social engineering, was active for 5 hours and was hidden in a new addToQueue function that sent the **user's private key** in seemingly harmless headers to a server controlled by the attacker.
- Apache Struts 2 vulnerability: In 2017, a serious vulnerability in the aforementioned software allowed executing Struts commands with just an http request without being authenticated. This December, a **new critical vulnerability has been patched. It would allow any type of file to be uploaded to the server, resulting in remote execution of arbitrary code through a *webshell***. The flaw has the CVE-2024-53677 and a score of 9.8/10.
- **Lawsuits to improve safety:** There has been a boom in the use of the U.S. *False Claims Act*, a regulation dating back to the American Civil War, to **make large sums of money by suing companies that fail to meet safety obligations set forth in federal government contracts**. Encouraging these lawsuits is a government strategy to discourage negligent security practices.
- **New NATO Cyber Center**: NATO will combine three cyber branches into a new **cyber coordination center**. The new NATO Integrated Cyber Defense Center will be launched in **2028 and will be located in Mons, Belgium**. It will unify the roles of the NATO Cyber Security Center, the NATO Cyber Operations Center and the alliance's Cyber Threat Analysis Branch.
- Brute force against Microsoft Azure MFA. Researchers at Oasis Security discovered a vulnerability in one of the MFA methods for Microsoft Azure. That endpoint did not correctly implement ***rate-limiting*** and the authentication period lasted a full three minutes instead of the recommended 30 seconds. An attacker could therefore quickly perform many simultaneous authentication attempts to enumerate the entire 6-digit MFA slot and gain access.

- Romania's National Cybersecurity Directorate stated that the "Lynx" ransomware gang attacked Eléctrica Group, one of the country's largest electricity providers. It also revealed that more than 85,000 cyberattacks were recorded against the country's electoral infrastructure between the election period of November 19-25.

MOBILE

Apple iOS

The new security enhancements in iOS 18

As usual in the second half of the year, Apple released version 18 of its mobile operating system, iOS, in September. Let's take a look at its improvements in the security aspect.

The first one that catches the eye is the ability to lock apps and use Face ID (facial recognition) for unlocking.

An additional security measure that enhances the privacy of applications to prevent snooping on them when our terminal is unlocked and used by third parties.

Users of iOS 18 will be able to record their phone calls as an option. If they do so, the iPhone will notify the other party that the call is being recorded. This feature, for legal reasons, will not be available in all countries.

In addition to the recording, a transcript of the conversation can be obtained directly in the Notes application.

The granularity of access to contacts by applications has been improved. Previously only two options were allowed with respect to this permission: either access was prevented, or full access was given to the contact list.

Starting with iOS 18, it will be possible to make a selection of contacts allowed for access by an app requesting such permission.

Access and privacy permissions have also been improved with respect to Bluetooth. In this sense, Bluetooth access is limited and displayed to the user to avoid abusive uses after pairing between devices and applications.

An application is introduced to manage passwords with the ability to synchronize between devices and even share passwords with our contacts or family.

Vulnerabilities and versions released in the second half of 2024

Despite a relatively quiet start to the summer at Apple headquarters, new updates were released on July 29 for virtually the entire range of the Californian firm's top-of-the-line products.

iOS, twice over, saw version 16.7 updated with revision 16.7.9 while branch 17 moved up to 17.6.

Between the two update packages, a total of 42 vulnerabilities have been fixed with a varied impact, ranging from information leaks to denial of service.

Shortly after, on August 7, a small update is released for the two branches: 16.7.10 and 17.6.1, but they do not include any security updates.

We must go back almost to the end of the summer, on September 16, to receive the major revision 17.7 with, precisely, 17 patched vulnerabilities.

That same day, iOS 18 is released. In addition to the new features it brings, it comes with 40 security fixes. It is striking that, far from memory corruption vulnerabilities, many failures are due to security control flaws that can be evaded or logical flaws that can be exploited for a different, and malicious, purpose than the one intended.

Weeks later, a small but curious update slipped out, revision 18.0.1. Two bugs fixed: the first one is

due to the fact that it is possible to make an audio recording of seconds before the audio capture indicator (amber circle) is activated.

The second one is even more curious. It fixes a bug whereby an attacker could "listen in" to passwords stored on the device due to abusive use of the "VoiceOver" accessibility feature.

We are going to the end of October, on the 28th to be precise. That day 17.7.1 is released and it fixes 23 security flaws. 23 bugs that is almost half that iOS 18.1 fixes on the same day: up to 55 patches, nothing more and nothing less. A large batch that includes dangerous vulnerabilities fixed, such as an arbitrary code execution in the IOSMobileFrameBuffer, the component responsible for rendering the iPhone screen.

On November 19, Apple releases two minor patches: 17.7.2 and 18.1.1. Both fix the same security bugs that affect Webkit and are not only dangerous (they lead to arbitrary code execution when visiting web content) but are actively being exploited.

And we close 2024 with two major patches. On December 19, 17.7.3 is released with 26 fixes and 18.2, a major revision of version 18 containing up to 32 patched vulnerabilities.

Evolution of vulnerabilities in iOS in the second half of 2024

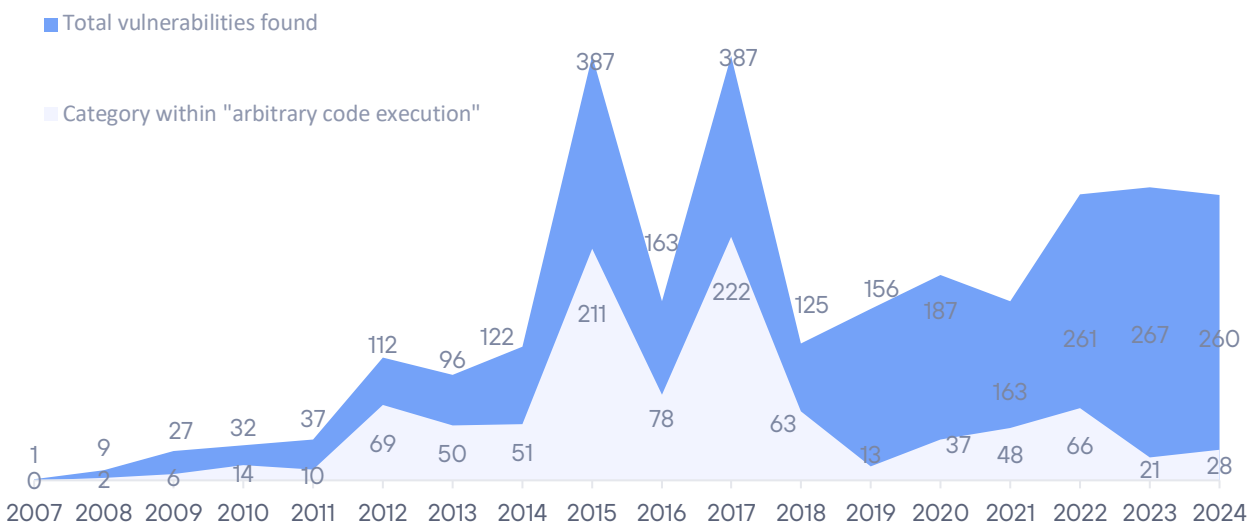
The second half of 2024 closed with 149 unique vulnerabilities patched, four considered high-risk, with the potential to execute arbitrary code.

260 vulnerabilities were corrected in total in 2024. This represents a slight decrease compared to 267 in the previous year. A similar number was found in 2022 (261).

The estimated number of high-impact vulnerabilities (arbitrary code execution) is 28, seven more than the previous year.

IOS VULNERABILITIES 2024-H2

Evolution of vulnerabilities per year



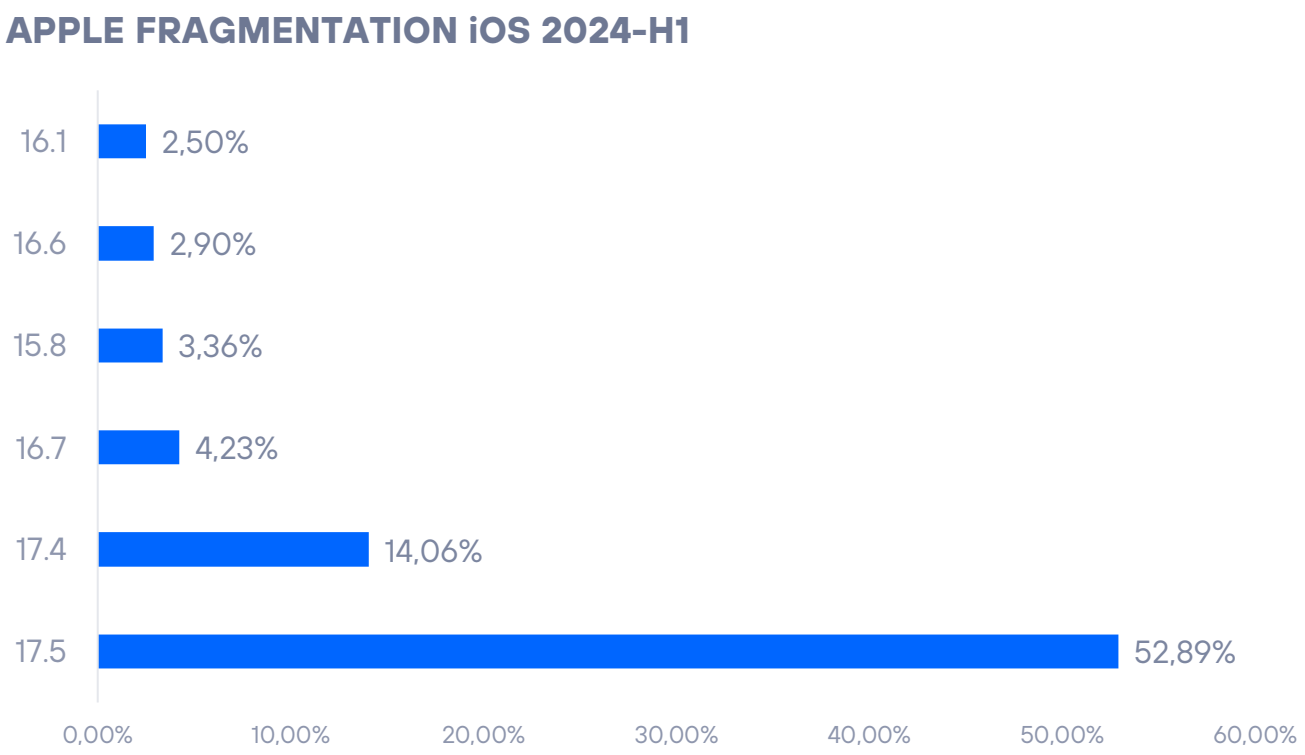
Fragmentation of versions during the first half of 2024

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

The picture of the second half of 2024 presents us with a strong presence of the new version of iOS, version 18, as usual. The release of a new version of the operating system is an event awaited by Apple users and its update, even in the first hours, is massive. It is noteworthy that even iOS 18.2, released well past the December meridian, reaches 6.57% of the mobile base.

We are left then with the released iOS 18, which has a small percentage, a 4.31% since the bulk of the 18 population is now on 18.1, with almost 50%. We add the already mentioned iOS 18.2 with 6.57% which gives us just over 60% adoption.

The previous branch, iOS 17, adds up to 10.95% of 17.6 and 3.5% of 17.5. The 16 branch survives with a modest 3.46%, limited to handsets such as iPhone 8 that are almost eight years old.



Android

New security features

Android 15 was released to the public on October 15. Let's see what new security features this new iteration of Google's mobile operating system implements.

One of the new features is the theft protection. It is interesting because it is not just a remote blocking of the terminal, which can be done from another terminal using a security check. Android implements a system that detects the physical theft of the terminal "live". That is, someone steals the terminal and runs away. In such a scenario, the system will detect that something unusual is going on and lock the handset to prevent tampering.

In addition to physically, it also has a heuristic that tries to find out if the mobile is being manipulated to access information or change its characteristics: manipulation of the SIM, repeated failed access to passwords, changes in certain configuration parameters or if the terminal is disconnected from networks (mobile or wifi known) etc. In such cases, the terminal will also be blocked.

Regarding privacy, a new feature called "private space" has been implemented, which consists in the creation on demand of a group of applications that we want to hide from view. Not only will the application icon be hidden, but also its notifications or their settings. In addition, we can hide our own private space from the view of others. All this is designed for if the terminal is used discretionary by third parties or is unlocked.

Continuing with the security chapter, version 15 implements an advanced feature to hide certain applications when sharing the screen. For instance, certain notifications will not be visible in screen sharing and, in fact, only the application to be shared will be visible and not the entire system. In addition, if the system detects that a password, credit card or login data is going to be displayed, it will be hidden and will not be visible while using the screen sharing function.

Closing the security chapter, Android 15 implements improvements in the password manager, new security features available in the API for programmers, robustness of some "Intents" and improvements in the privacy of some features.

Vulnerabilities

Android releases a set of patches every month, usually during the first week. In this second half of 2024, six bulletins have been published with the following distribution of vulnerabilities for each month:

Month	CVEs	Critical or CER
July	16	2
August	40	2
September	35	2
October	24	1
November	38	2
December	14	1

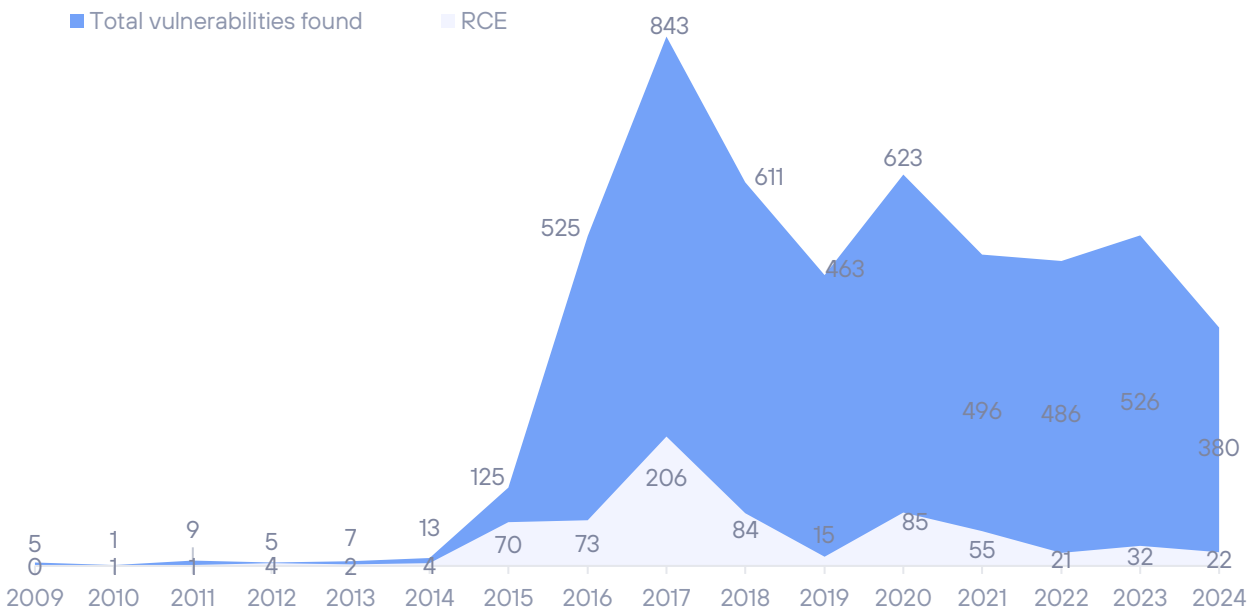
However, some CVEs may not have associated impact information as of the date of publication of this report, so the number of CVEs may subsequently be higher than indicated.

In total, 167 patches in this six-month period (the previous six-month period was 213); 10 of them considered critical (12 in the previous six-month period). This makes a total of 380 vulnerabilities patched in 2024.

It should be noted that many of these flaws 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.

ANDORID VULNERABILITIES 2024-H2

Evolution of vulnerabilities per year



Fragmentation in systems

The latest release from Statcounter as of the date of this report indicates that the most deployed version of Android is Android 14, with a share that exceeds last semester's 25.64% with 36.95%, followed by Android 13 with a share of 18.81%, down from 22.29%.

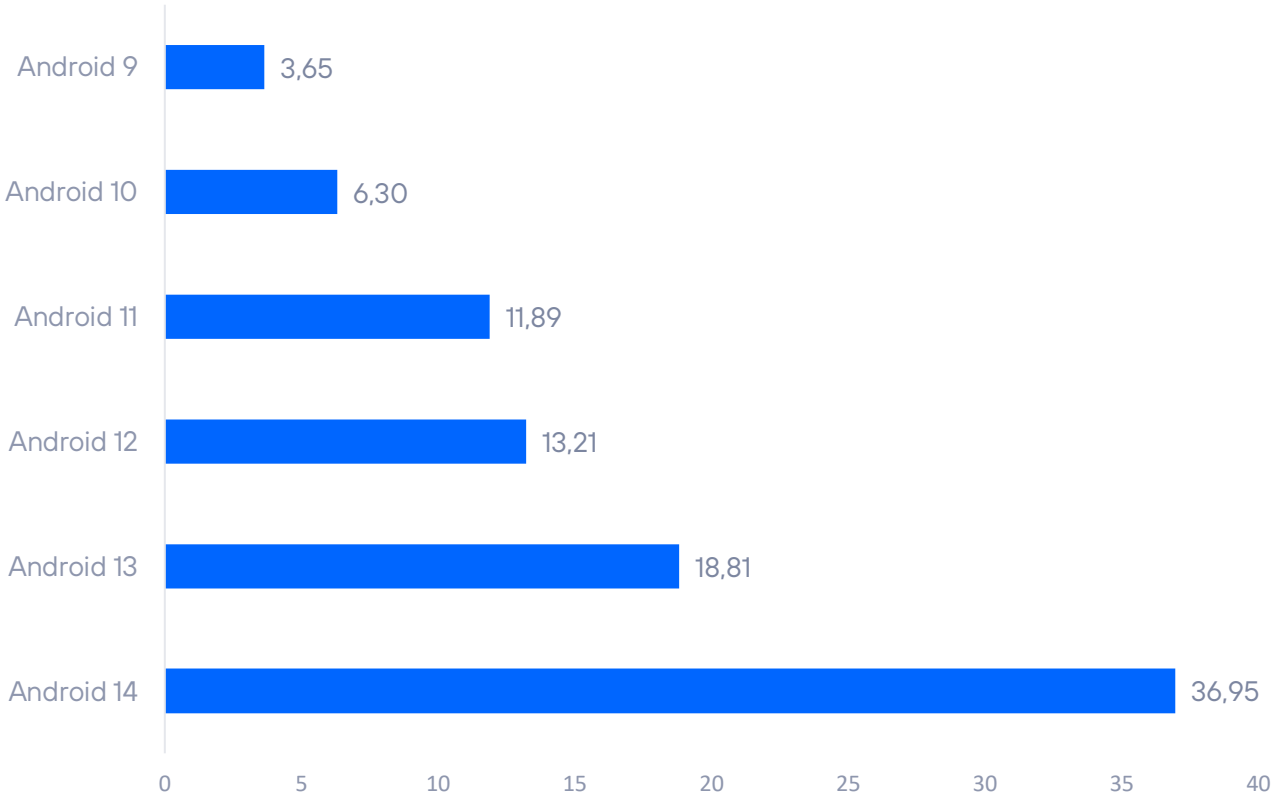
Android 15 has not yet had a noticeable effect on the number of Android 15 mobile devices. We will have to wait for the next edition of this report to assess the situation. Even the increase in figures for the previous version, version 14, which has even grown in penetration, is notable.

It falls within the norm, since a new version, released in late summer, takes time to gain a foothold. In addition to the fact that the counting of numbers also means that the display window for new models takes a long time to appear.

Android versions prior to version 12 (including the system that appeared in September 2020) are no longer supported for updates. Even so, they have remarkable figures: Android 11 with 11.89%, Android 10 with 6.30% and closing the queue, Android 9 with 3.65%.

There is an unaccounted 10% that may be consolidated by even older versions, but they no longer fall into the pigeonhole for classification. We would be talking about almost 25% of terminals with unsupported operating systems, which makes them exposed to vulnerabilities and their exploitation.

ANDROID FRAGMENTATION 2024-H2



It is common in the Android system, where there are markets that due to economic difficulties have terminals that are out of coverage age. The very wide range of phones, both economic and high range models, make the Android ecosystem rich in fragmentation and different deadlines and stages of recycling

SIGNIFICANT VULNERABILITIES

In this section we will discuss what we consider to be some of the most notable vulnerabilities in the second half of 2024.

CVE ID	OBJECTIVE	DESCRIPTION	SCORING
CVE-2024-6385,	Gitlab	A bug in Gitlab allows running jobs as another user.	9,6
CVE-2024-20401	Cisco	Code execution through a "path traversal" problem	9,8
CVE-2024-4879	ServiceNow	Through the chaining of several failures, full control of the system could be obtained.	9.3
CVE-2024-29847	Ivanti	A problem in deserialization allows code execution	10
CVE-2024-6678	Gitlab	A bug in Gitlab allows running jobs as another user.	9,9
CVE-2024-8963	Ivanti	Path Traversal in Ivanti CSA allows an unauthenticated remote attacker to access restricted functionality.	9.4
CVE-2024-7593	Ivanti	Authentication failure allows unrestricted access to administration panel	9.8
CVE-2024-38812 **CVE-2024-38813**	VMware vCenter	Execution of code with the concatenation of two vulnerabilities.	9.8
CVE-2024-29824	Ivanti	SQL injection in Endpoint Manager	9.6
CVE-2024-23113	Fortinet	Code execution in FortiOS	9.8
CVE-2024-9486	Kubernetes	SSH failure allows unauthenticated access to virtual machines	9.8

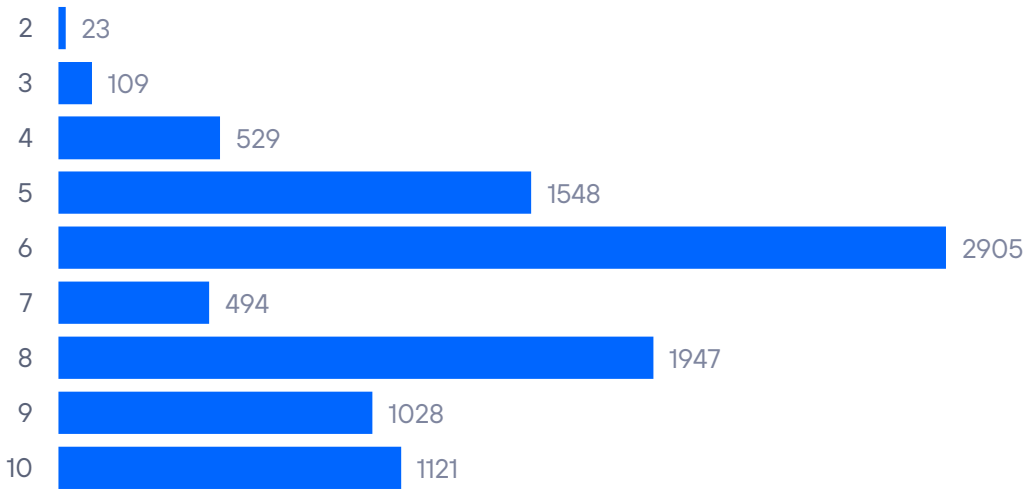
CVE-2024-47575	Fortinet	FortinetManager API problem allows code execution	9.8
CVE-2024-20418	Cisco	Code execution in Ultra-Reliable Wireless Backhaul (URWB) access points.	10
CVE-2024-0012.	PaloAlto	An authentication bypass in Palo Alto Networks PAN-OS software allows an unauthenticated attacker with network access to the management web interface.	9.8
CVE-2024-11639	Ivanti	Administrative access to the Ïvanti CSA Console	10
CVE-2024-53677	Apache Struts	A path traversal bug allows arbitrary file uploads and code execution.	9.6
CVE-2023-34990,	FortiNet	Code execution in FortiVLM	9.8
CVE-2024-34026	OpenPLC	A specially crafted Ethernet/IP request can cause remote code execution. An attacker can send a series of requests to trigger this vulnerability.	9.8
CVE-2024-4708	mySCADA	mySCADA myPRO uses a hard-coded password that could allow an attacker to remotely execute code on the affected device.	9.3
CVE-2024-8956	ValueHD cameras	PT30X-SDI/NDI-xx PTZOptics cameras prior to firmware 6.3.40 are vulnerable to an insufficient authentication issue. The camera does not properly enforce authentication when sending requests without the HTTP "Authorization" header. A remote, unauthenticated attacker can leak sensitive data and update individual configuration values or overwrite the entire file.	9.1
CVE-2024-8497	Franklin Fueling Systems	Franklin Fueling Systems TS-550 EVO versions prior to 2.26.4.8967 have an arbitrarily readable file that could allow an attacker to obtain administrator credentials.	8.7
CVE-2024-8630	Console for tanks at Sibylla service stations	A successful SQL injection could result in an attacker obtaining device information from the database, deleting credentials or potentially gaining administrator access.	9.4

Vulnerabilities in figures

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

RISK OF VULNERABILITIES

Distribution of vulnerabilities by risk

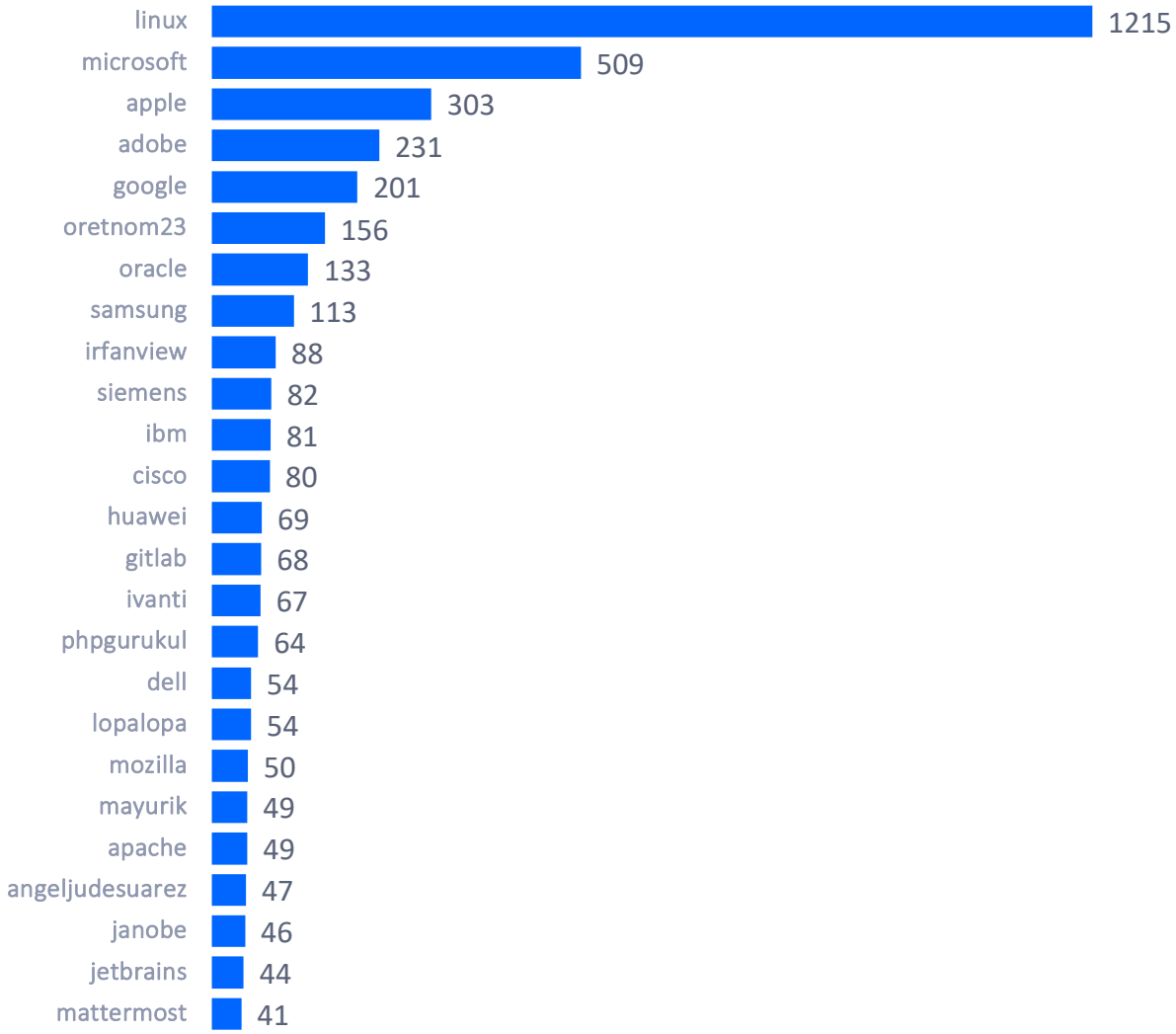


Top 25 companies with the most accumulated CVEs

During the second half of 2024, Linux led by far in the number of known vulnerabilities, followed by Microsoft and Apple. In general, it is common for Microsoft, Adobe, Google and Oracle to always be among the top in number of vulnerabilities. We have not found a specific public reason why so many CVEs associated with Linux have been reported in this half year.

VULNERABILITIES BY MANUFACTER

Top 25 manufacters by accumulated CVE



APT OPERATIONS, ORGANIZED GROUPS, AND ASSOCIATED MALWARE

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

We must point out that the attribution of this type of operation, as well as the composition, origin and ideology of the organized 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 the actors may use means to manipulate information in such a way as to conceal their true origin and intentions. It is even possible that in certain cases they may act with the modus operandi of other groups to divert attention or harm the latter.

Remarkable APT activity detected during the second half of 2024

Venomous Bear - No honor among APT-Groups

Also known as "Turla", this group has been active for at least 20 years and is backed by the FSB, according to the US DOJ (enough acronyms in one sentence). Although they have been "disbanded" several times, they are more resilient than the systems they attack.

In this case, they have been seen attacking targets in Ukraine, but using platforms and positions deployed by other groups. For example, by the Pakistani "Mythic Leopard". Apparently, the bear accessed networks already controlled by the Leopard in Afghanistan and India and modified their C2 servers to use them for its wanderings.

It does not appear that the Pakistani group is the only one to have been poisoned by this bear.

Some claim that they are responsible for the Moonlight Maze espionage campaign (and corresponding breach), which would place their existence at least as far back as 1996.

More information: https://www.bleepingcomputer.com/news/security/russian-hackers-hijack-pakistani-hackers-servers-for-their-own-attacks/

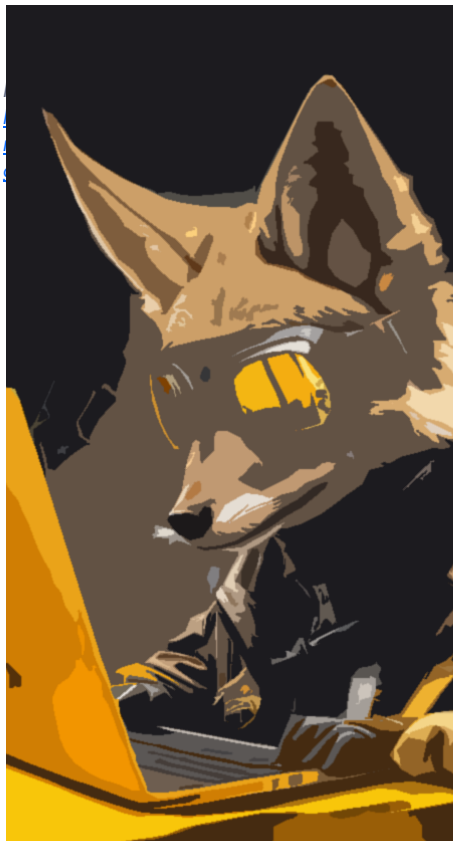
Golden Jackal - Breaking the laws of physics

We have already discussed this group in the report for the first half of 2023. Several We Live Security researchers have detected the jackal bypassing the supposedly infallible "Airgap" of several European government systems.

Their preferred target is still information: e-mail addresses, encryption keys, files... However, the researchers did not reveal who exactly was their target.

We are not going to describe how these attacks are prepared and executed to breach isolated networks, because it would take us 52 pages, but let's just say that it is not exactly simple and in many cases requires negligence or collaboration on the part of the potential victims.

It is still not possible to relate this group to a specific country, although they still use some expressions that remind us of our friend the bear above...



More information: https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/

Kimsuky

Kimsuky - Back to the studios

This North Korean group has been linked to several attacks targeting South Korean university professors and researchers.

Always related to Spear Phishing and social engineering, they were detected when they made a mistake (probably) in the exfiltration of the information. Thanks to this, it was possible to know what their TTPs were.

One of them is the execution of their work with obfuscated tools to fly under the radar of hosting companies. Prominent among their tools is the use of a webshell called "GreenDinosaur" to operate on the host they have taken over.

Considering that their business is the theft of research information (nuclear, pharmaceutical, medical...), when they are detected in connection with financial crimes it is because that is their way of financing the rest of their work.

More information: https://thehackernews.com/2024/08/university-professors-targeted-by-north.html

Sandman - The sand is everywhere

- *Sleep with one eye open*
- *Holding your pillow tightly..*

Since the sandman has learned to sneak into your systems by exploiting the tunnels of Vistual Studio Code, Microsoft's source code editor.

It appears that this group, linked to China, has been caught hacking into European IT service providers using VSCode to persistently maintain their access. And we say "allegedly" because the perpetrator of this activity is not certain.

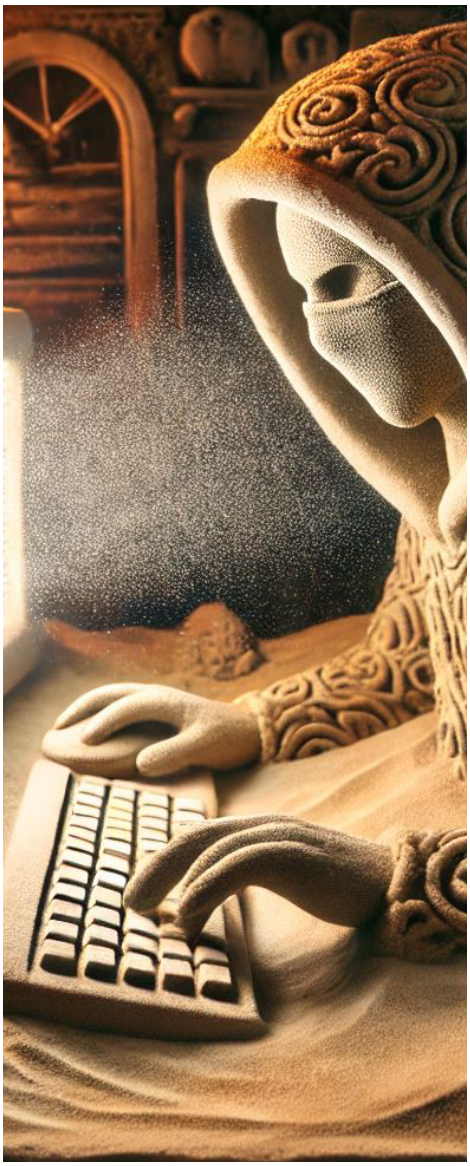
These tunnels are established through Azure with executables signed by Microsoft and serve to work securely (...) on remote systems.

Apparently, the input vector is a typical SQLi exploit. Once access is established, they deploy a webshell and ... play.

When deploying VSCode and configuring the tunnels they do nothing "illegitimate" so security tools do not detect malicious activity.

This tactic is not new, but it is rare. In September of this year, the Chinese group "Mustang Panda" was detected employing the same strategy.

Same panda, but different collar? We'll see.



More information at: https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/

OT THREAT ANALYSIS

The following information comes from the OT threat capture and analysis system, Aristeo. **It** incorporates a network of **decoys, made of real industrial hardware,** which appear to be industrial systems in real production. **They behave as such**, but are extracting all the information about the threats accessing the system.

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

Information analysis

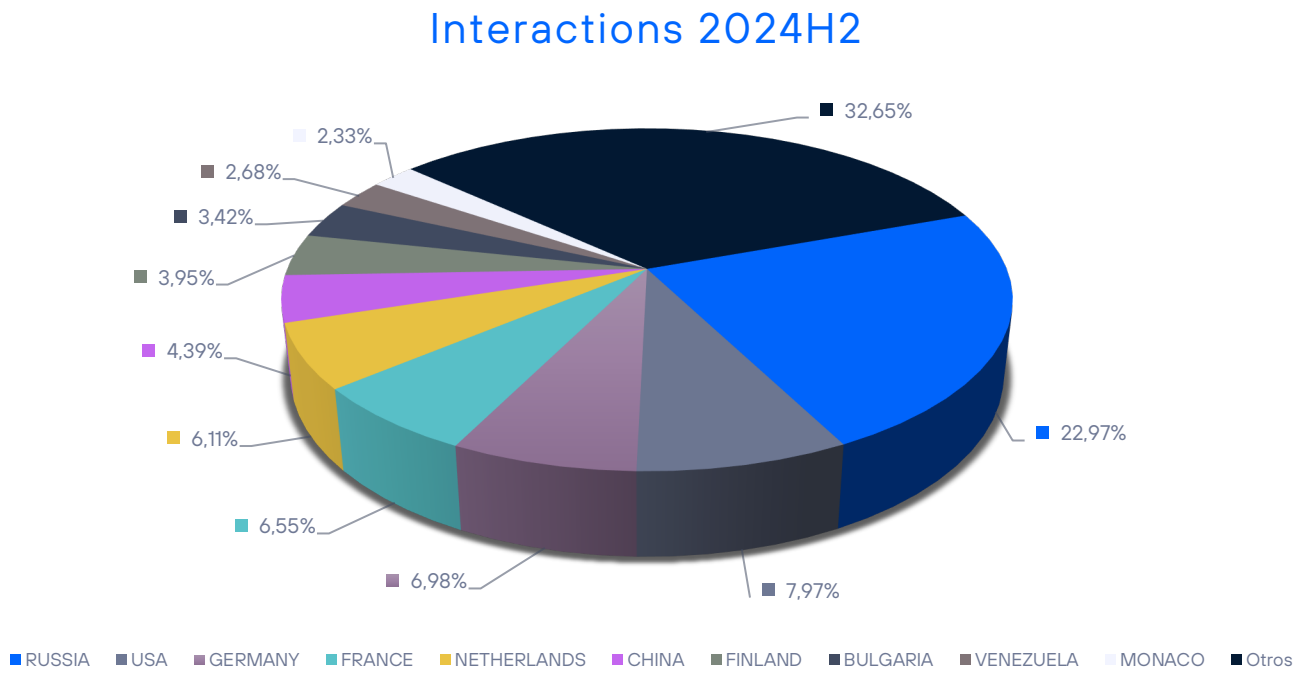
This semester we have implemented Aristeo "2.0" for data analysis for this report. Therefore, we will briefly explain the improvements introduced, instead of commenting on a specific case detected in recent months.

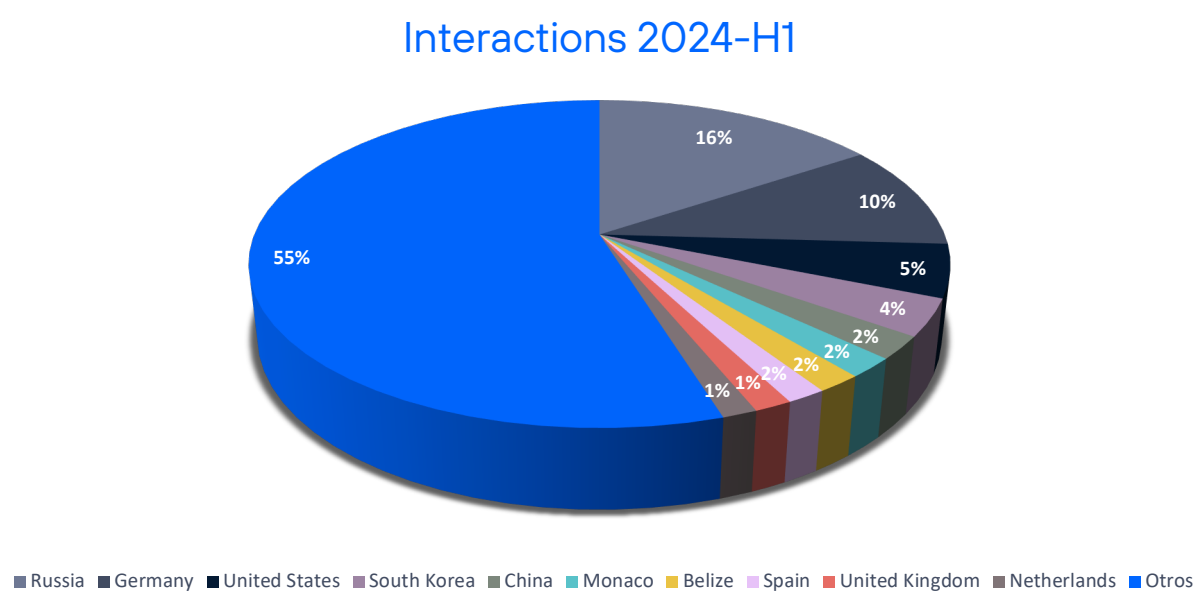
- Association of events and actions in complex events: this leads to a decrease in the total number of events. Less activity is counted, even though the same (or more) activity is recorded. For example, 100 RDP access attempts to a control PC from the same IP in a short period of time are counted as "1" (RDP bruteforce) instead of counting the number of RDP access attempts, 100. It is true that the "coarse" measure is lost, but at the end of the day the important thing is not the global data (which, of course, we keep and can deal with) since an automated system can make 100 or 1000 attempts in an attack and in reality it is still the same attacker executing the same action with the same TTP (tactics, techniques and procedures) and the same IoA and IoC.
- Identification of "gray" interactions: Aristeo already differentiated in a binary way between legitimate and non-legitimate activity (black/white). Now, it is able to identify those interactions that need not be malicious per se but are not legitimate or solicited either. Traffic generated by metasearch engines or corporate security services, for example. This differentiation makes it possible to continue to archive "gray" information to work with, but to focus the activity of Aristeo and the analysts on events that do not come from these types of services or institutions, but from genuine attackers.
- More granularity in the information that already exists, which equals more information to deal with: the ability to discern activity by its origins or to group it together also makes it possible to work better with the information that was being generated and to generate more of it. Aristeo can now more easily identify cyber security events as they occur and place them in a context understandable to an analyst, such as MITRE's **Enterprise and ICS matrices**
- Improved reading of activity across the network: Aristeo had a bias towards activity received in Spain, due to the fact that its lures are mostly positioned in its country of birth. We have introduced changes to record more information across the globe, which means more depth and breadth in recording attacker activity.

We turn to the general statistics of the recorded information. In the second half of 2024, **more than 333 million cyber security events** were detected**, but with the new version, in which events are grouped into more complex ones, the figure decreases. We would therefore be talking about more than 27 million complex events in the six-month period with the new counting system**. Comparing the figures obtained with the same version, this represents a rise compared to the data recorded in the first half of 2024, 313 million, and a small rise compared to the second quarter of 2023,

when some 322 million events were recorded. However, the figures remain in very similar ranges, so it could be said that the situation remains stable.

The distribution by country is as follows:

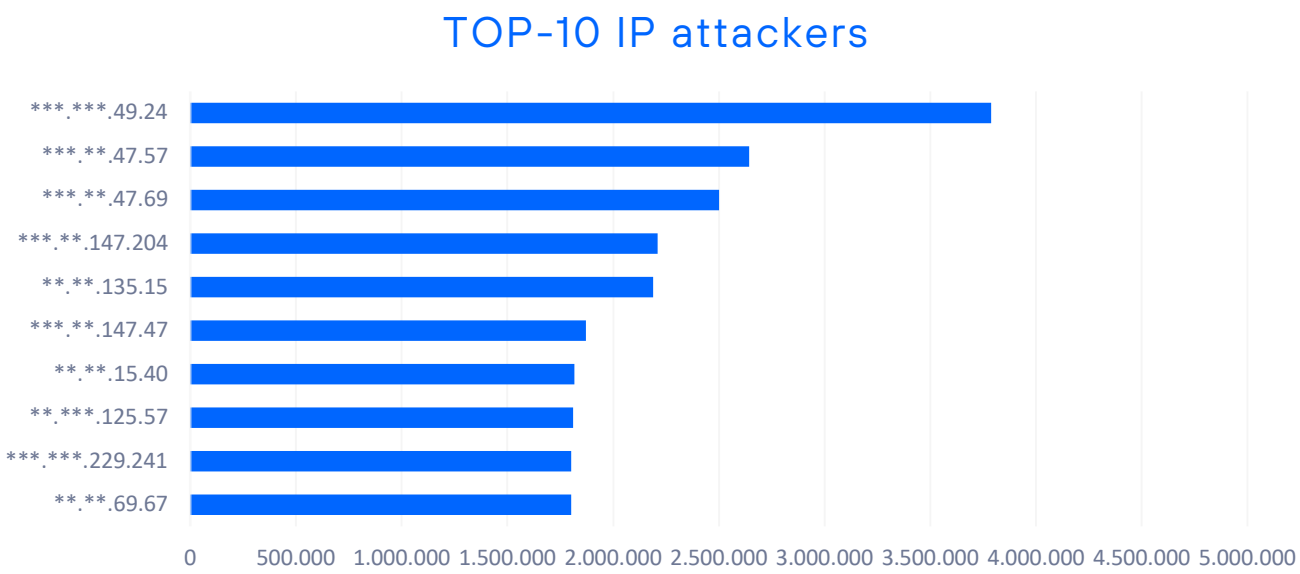




As can be seen, despite having increased the breadth of the Aristeo network, the countries with the most interactions towards the decoys are still old acquaintances. Although there may be a slight variation in the countries registered, if we look at the history of all the semesters (and with access to all the data we have) we

can conclude that the situation is very similar. Especially if, in addition to the countries, we look at the regions of the world they occupy.

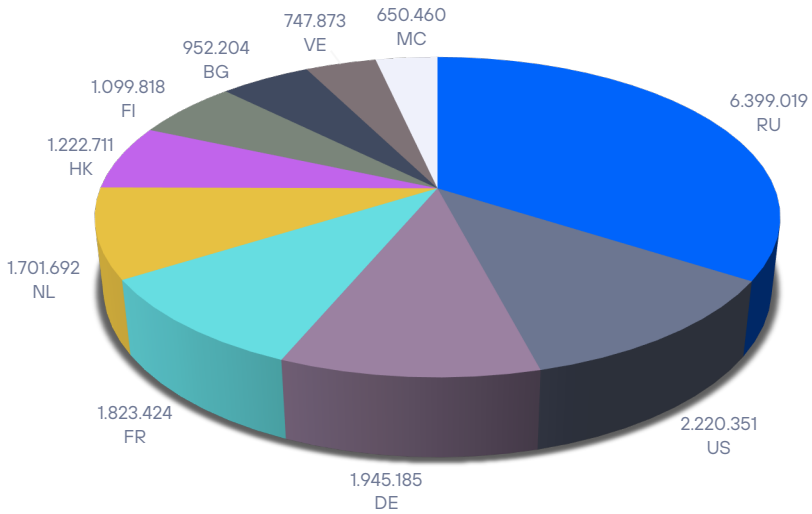
Now, let's take a look at the top ten IP addresses with the most interaction with the Aristeo system. In this semester, as in the previous one, the vast majority of IP addresses in this Top 10 come from central-north-eastern Europe. However, the number is not 85% as in the previous semester. In this case, the IP address with the most activity is not European, and other addresses that are not European also slip into the Top 10. This is probably also related to the greater breadth of Aristeo's network. By positioning it better in relation to the world, we have managed to capture more accurate information in reference to the world panorama.



A decrease in the total number of events represented by the Top 10 IP addresses can also be observed. This also has to do with the higher registration capacity. By registering more IP addresses, with a similar number of interactions, the total is divided among more actors and the Top 10 loses representativeness.

Below, we see how the *top 10* of the registered countries are distributed. This semester, Spain disappears as a country (from the Top-10 but remains in the Top-30). Once again, the fact of delocalizing more Aristeo implies less focus on a specific point of the world geography and more use with respect to the rest.

Top 10 countries



It can also be seen that the number of events is much lower than last semester. The reason is, let's remember, that events are now grouped into complex events and therefore the figures are different because they do not measure the same thing.

This section closes the analysis with Aristeo version 1.0. Next semester we will add the graphics of version 2.0.

STUDY OF THREATS 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.

A total of 359,529 IP addresses, 73,838 domains and 565,583 URLs were studied for the different IOCs involved.

What type of maliciousness do the URLs studied involve?

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

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

It is important to determine what is at the end of the URL and categorize it properly to know what type of threat we are dealing with. This is precisely what we have asked to the Maltiverse database and we have found these results in the top 10:

Malware Download	442300	78,20%
Phishing	114590	20,26%
Strela Stealer	3300	0,58%
Lumma Stealer	1952	0,35%
FAKESUPDATES	1057	0,19%
malware	907	0,16%
Mozi	621	0,11%

DCRat	604	0,11%
Coper	476	0,08%
NetSupportManager RAT	390	0,07%

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 cybersecurity regarding what awaits us at the end of a URL, it is precisely these two major categories

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

Special mention should be made of a malware that has hit countries such as Spain, Ukraine, and Germany in particular at the end of 2024: Strela Stealer. As we will see in the domains section, it has made headlines in the specialized press and its effects have been seen and felt.

Strela uses phishing as a vector through emails impersonating banking services, among other disguises. A malware download is performed through this phishing, curiously, digitally signed with a certificate stolen from a Brazilian company.

Apart from the generic categories, the rest is distributed, as we can see, among the most widespread malware families. Infrastructure that serves as a download point, to capture orders and even to temporarily deposit stolen information.

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

This edition we have consulted with Maltiverse to find out which domains appear most frequently in the URLs studied.

It is interesting to note which services, mostly legitimate, are the most employed by malware writers and their associated campaigns.

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

pages.dev	6663	1,18%
github.io	5788	1,02%
vercel.app	5676	1,00%
farpetor.shop	4882	0,86%

lameshamer.shop	4882	0,86%
geriguna.shop	4882	0,86%
gerlia.shop	4882	0,86%
gloomcutter.shop	4882	0,86%
glynnorin.shop	4882	0,86%
gonnhild.shop	4882	0,86%

As usual, the first positions belong to online services that allow to host web content for free: pages.dev, github.io, vercel.app. After them, come the domains used by individual campaigns, in particular, that number (4882) is not a bug but a group of domains (a few thousand very specific ones captured in the database) that are associated with a group of campaigns related to the Strela malware, which we have already talked about before.

The spread of this malware has been particularly acute with domains of the ".shop" tld. Both indiscriminate registrations and online stores have been the target of intrusion by the criminal group following the dissemination campaigns of this malware.

Which countries are the IP addresses detected with malicious activity?

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

United States	53727	14,94%
India	49806	13,85%
China	37670	10,48%
Vietnam	22633	6,30%
Russia	13843	3,85%
Germany	11021	3,07%

South Korea	10747	2,99%
Taiwan	10536	2,93%
Pakistan	10476	2,91%
Brazil	8352	2,32%

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

What kind of maliciousness do IP addresses engage in?

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

Suspicious host	155191	43,17%
HTTP Spammer	140821	39,17%
Mail Spammer	131096	36,46%
Malicious host	91431	25,43%
SSH Attacker	45292	12,60%
Proxy	33936	9,44%
Bruteforce	31380	8,73%
Port Scanner	30032	8,35%
Host scanner	27226	7,57%
Hacking	26583	7,39%

Crowning the top 10 ranking is a general category: "Suspicious host". It is a categorization that practically overlaps half of the dataset since it is awarded whenever there are indications of suspicious activity although the operation observed from that IP address is not yet known in detail.

When a label is added later on, with the detail of why: spam, indiscriminate scans, etc., the suspicious host label is not removed as it is a further refinement. Another type of generalist labeling is found in "Malicious host". Identical meaning, although it adds a little more certainty in the preliminary diagnosis.

If we aggregate the tags by specific IP address activity, we see that SPAM, both HTTP and Mail, top the ranking with almost 80% of the tags. As a reminder, tags overlap, so the same IP can contain several of them. For example, a general "suspicious" and "HTTP Spammer", and even the same IP can be used for port scanning because it has been a detected activity at some point in time.

SSH Attacker is a unique category. It almost certainly belongs to groups of infected hosts coordinated by a Mirai-type botnet. Mass scanning for easy access via SSH (Secure Shell) has been a constant for decades on the Internet (as was Rlogin or telnet in its early days). Almost 13% of IP addresses have been observed performing attacks on SSH (mostly dictionary attacks on the login).

Similarly, "Bruteforce" refers to the continuous attempt to perform brute-force authentication (actually, again: common username and password dictionaries). This category totals almost 9%.

In another subcategory, indiscriminate scans, we find: Port and Host scanners. IP addresses that have been detected by performing mass scans on entire ranges or multiple ports on certain hosts. That is, horizontal scans looking for certain ports or vertical scans (in depth) on a group of hosts.

The category "Proxy" with almost 9.5% are systems that, either intentionally or unsuspectedly, serve as a gateway or hop to other machines to hide the origin of certain attacks or unauthorized access.

Overall, we find the "hacking" category with 7.39% closing the ranking. These are nodes that have been observed performing attacks in general, either trying to find SQL vulnerabilities or launching exploits. Often, these are vulnerability scanners used indiscriminately and, of course, without authorization.

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 since they allow them to make use of this and change the IP address if the currently active server ceases its malicious activity.

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

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

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

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

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

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

What malicious categorization do the studied domains possess?

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

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

Phishing	48753	66,03%
Metastealer	6960	9,43%
Virut	5756	7,80%
Malware download	1974	2,67%
Lumma Stealer	1810	2,45%
CryptBot	1408	1,91%
Malware	1132	1,53%
Hook	826	1,12%
Astaroth	477	0,65%
FAKEUPDATES	416	0,56%

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 in general. The rest belong to malware families that have had an impact.

CONCLUSIONS OF THE REPORT

In the second half of 2024, it is confirmed that the number of vulnerabilities allowing code execution on iPhone is higher than in 2023, although they have slowed down in the second half of the year and are finally 28. On **Android, on the contrary, both vulnerabilities in general and serious vulnerabilities in particular are considerably reduced.** While in 2023 there were 32, in 2024 there are 22 critical ones.

If Oracle, Microsoft, and Google are the companies with the most bugs fixed on a regular basis, this semester Linux is on top of the list with 1200 vulnerabilities. We were unable to find a concrete public reason for this increase in the number of fixes in the database consulted.

Rgarding Aristeo, we are launching version 2.0 with many new features that modify the formula for counting events and incidents. We are also expanding our capacity to capture data from other countries. In this semester, as in the previous one, the vast majority of IP addresses in this Top 10 come from central-north-eastern Europe. However, the number is not 85% as in the previous half year. In this case, the IP address with the most activity is not European, and other addresses that are not European also slip into the Top 10.

A rather powerful Strela Stealer malware campaign sneaks into the top 3 of malware hosted on the Internet along with the more generic "malware" and "phishing" malware.

USEFUL LINKS

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

CYBER SECURITY

Ha! Encryption fingerprinting, right?

Communication and press: media coverage of incidents and cyber attacks

Digital wallets: maximum usability, maximum security?

Digicert incident, or when a certificate revocation ends in litigation.

ARTIFICIAL INTELLIGENCE

Project Zero, vulnerability discovery using LLM models

Ethics in AI and Machine Learning: The gray areas of sensitive variables.

MALWARE

Use of Flutter in malware to make analysis more difficult