S2 GRUPO

Cyber Threat Intelligence Report

TRENDS Q2 2023

Lab52

Content

Executive summary

This report summarises the activity recorded by the Lab52 cyber intelligence team, with a special analysis of the most significant events detected during the second quarter of 2023.

Quarterly trends

Geopolitical context

During the quarter the following developments are worthy of note:

The Russian-Ukrainian conflict has been continued by the Ukrainian counteroffensive, the results of which seem to be leading to a stalemate in the conflict. In statements published in May, UN Secretary-General António Guterres said that it is not yet possible to negotiate peace as both Russia and Ukraine believe they have a chance of winning. He also said there was little chance of nuclear escalation.

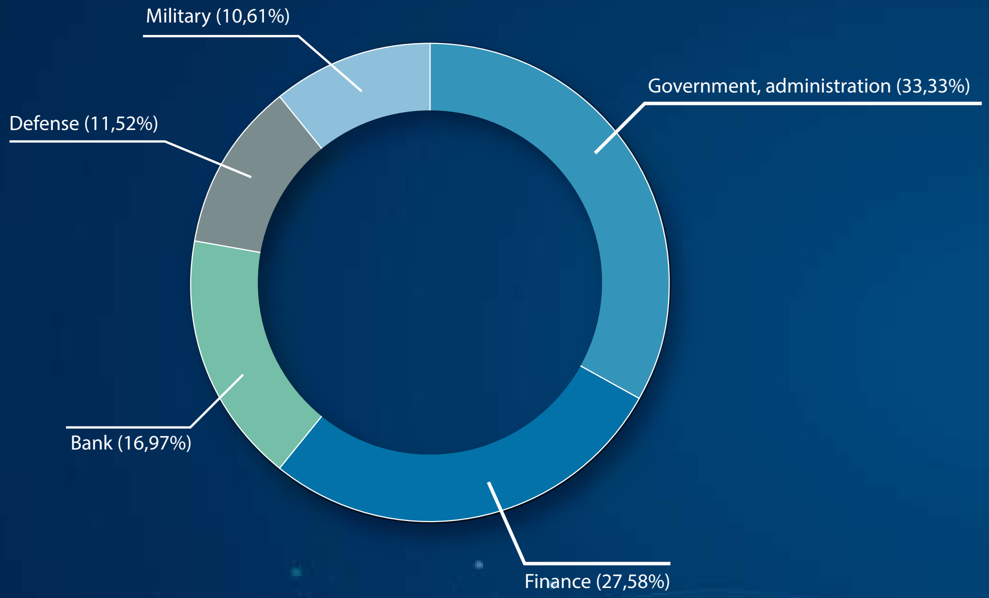
However, on 23 June Yevgeny Prigozhin, head of the Wagner Group, launched an armed rebellion on 23 June to 'force a change of leadership within the Russian defense ministry'. Prigozhin accused the ministry of launching an attack on a Wagner camp in the rear, thereby making an anti-Russian appeal. From Moscow, Vladimir Putin called what happened in the town of Rostov, a city of one million people where the population put up no resistance, "treason". The Kremlin and the leader of the Wagner group agreed that Prigozhin would leave Russia to settle in Belarus within 24 hours. In addition, it gave Wagner members three options: return to their families, exile in Belarus, or integration into the Russian army.

As for the economic effects of the conflict, the International Monetary Fund's (IMF) World Economic Outlook forecasts higher food and energy prices if the war escalates. Not only could this affect food prices, but Ukrainian grain exports are affecting Europe's less favored economies.

Finally, it is also worth noting the coup in Sudan in mid-April. Paramilitaries seized the presidential palace in Khartoum, the Sudanese capital's airport, and the airfields of Al Obeid and Marawi, a town close to Egypt. Rapid Support Forces (RSF) attacked several army camps throughout the country. Both sides agreed to a seven-day ceasefire starting on Thursday 4 May. The UN estimates that in less than a month 100,000 refugees have fled to other countries.

Analysis of incidents in the quarter

In terms of sectoral impact, public administration, as well as governments, have been the most affected during the period.While last month there was an increase in belligerence between countries since the defense and military sectors were in the top three positions, this month the financial sector and the banking sector are in the top positions.

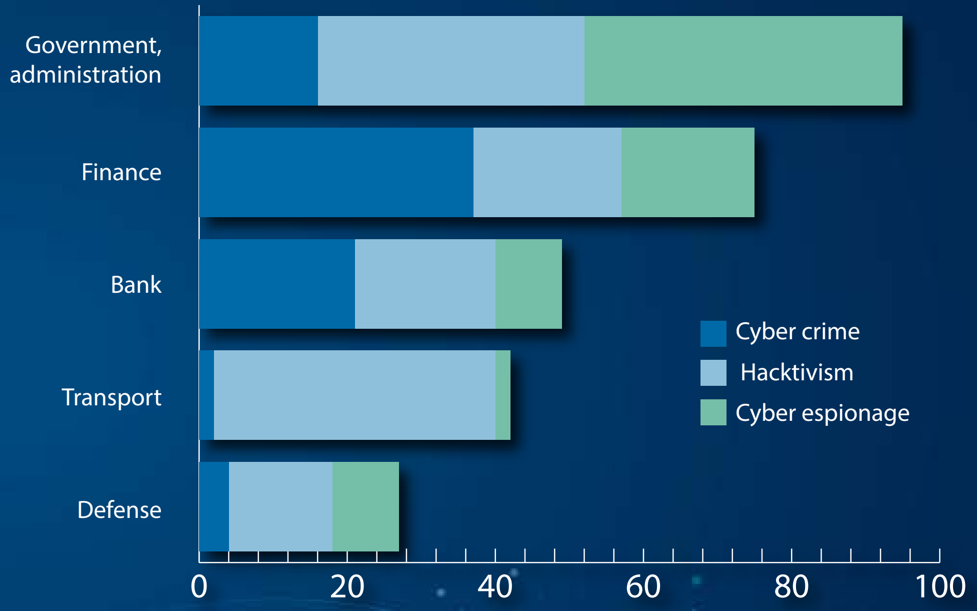


Sectoral distribution.

Cyber espionage focuses on the most strategic sectors, such as government, defence, military, and electricity. A similar distribution can also be found in the field of cyber warfare, affecting the industrial sector and transport.

A decrease in attacks against Ukraine's critical infrastructure has been observed, which is evidence of a new trend in the conflict, especially in the cyber sphere.

A broadening of cybercrime targets has also been found, mainly affecting the financial, banking, and governmental sectors.



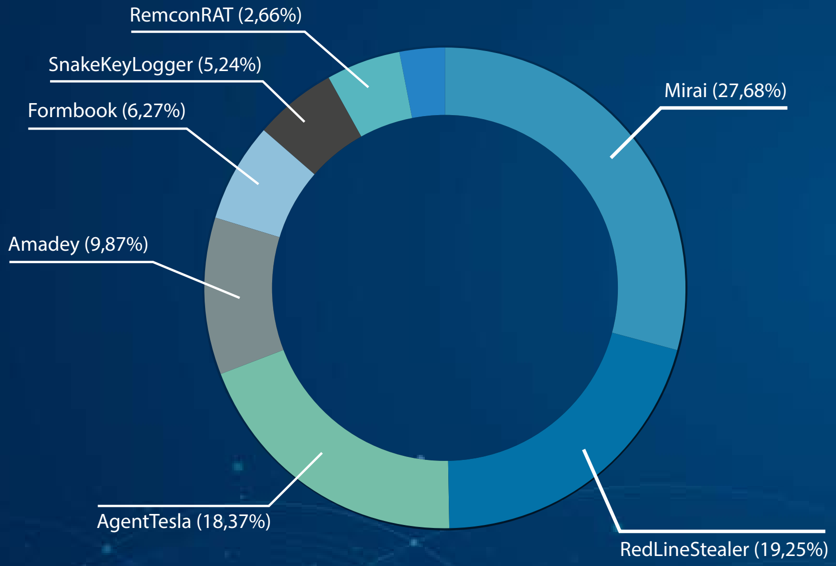
Sector and campaign type.

Malware trends

In terms of malware seen in the quarter, Mirai has become the most detected malware during the period, surpassing RedLine Stealer.

In addition to the proliferation due to the interest of hacktivist groups in the botnet, it is also due to the appearance of the CVE-2023-1389 vulnerability in the TP-Link Archer router, which expanded the number of potential botnet devices.

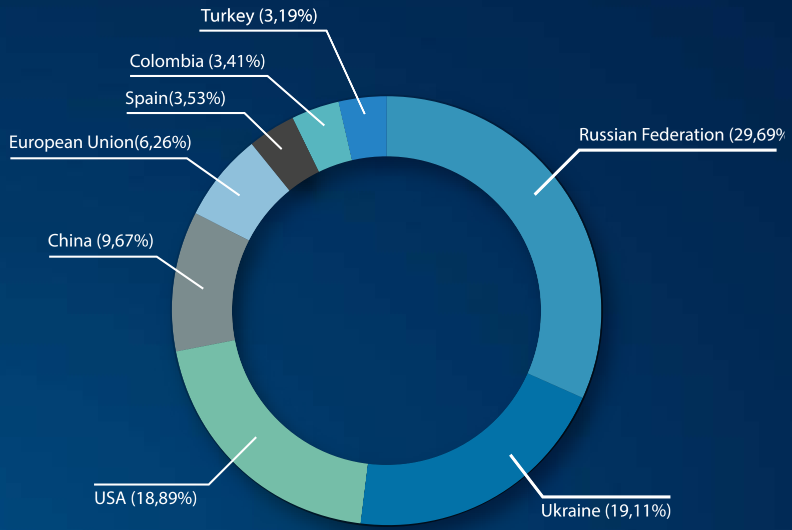
AgentTesla and Amadey remain in the top positions, in contrast to SnakeKeylogger and GCleaner, which have slipped down the rankings.



Malware trends Q2 2023.

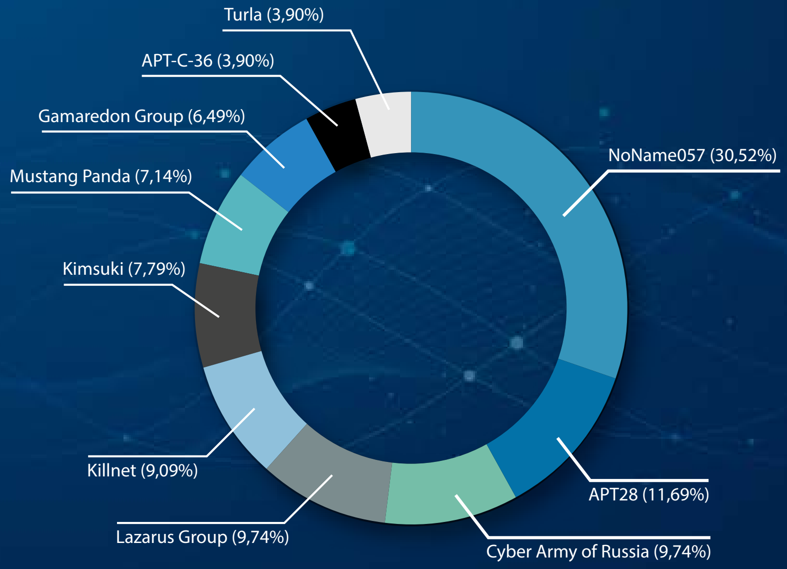
As mentioned in the previous section, Russia's internal instability, as well as the participation of countries allied to Ukraine in the conflict, the calculation of geopolitical risk places the Urals country in first position, followed by Ukraine and the United States.

It is also worth noting Turkey's appearance among the countries with the highest risk. This is due to its leading role in negotiating Sweden's NATO membership.



Risk by country.

Of all the events processed by the Lab52 team, more than seven thousand Indicators of Compromise have been generated and added to S2 Grupo's intelligence database. The following groups have been identified as the most active during the period:



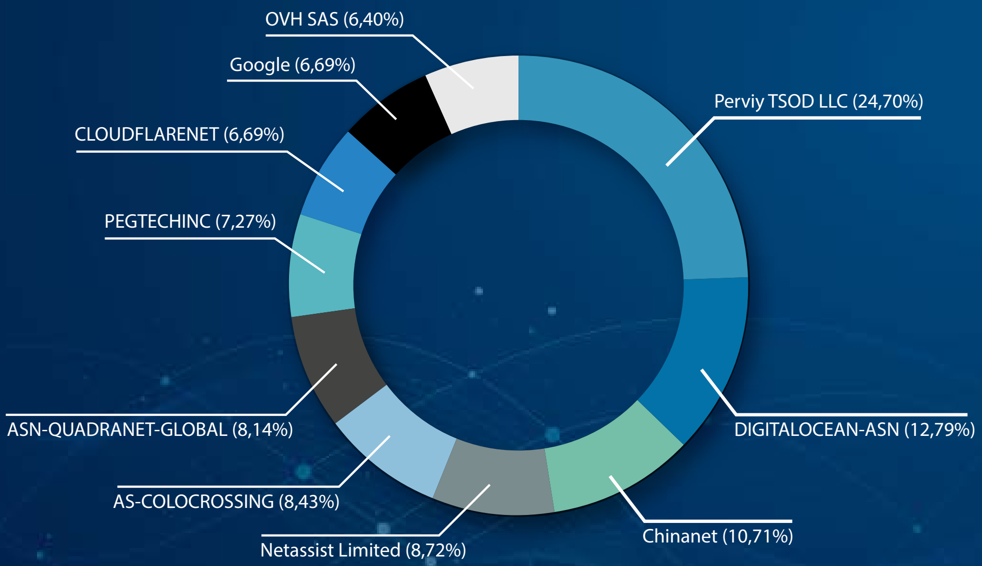
Top Threats-based IoC processed.

Again, actors of pro-Russian origin were the most active in the period, especially those with hacktivist motivations. As many as six groups in the Top 10 are aligned with Russian activities.

Among the remaining groups, both Lazarus and Mustang Panda continue to appear, expanding both in several different capabilities and targets.

Infrastructure analysis

The provider occupying the first position is Perviy TSOD, a service provider located in Russia, and which has been especially used in the period by Lazarus. Again, the second place is held by DIGITALOCEAN followed by Chinanet, both providers have already been mentioned in previous reports as they are widely used by all types of actors.



Number of registrations per ASN 2Q.

Campaigns associated with state interests

China’s reaction to the AUKUS treaty. Mustang Panda campaign against Australia

Lab52 notified its clients about the increased tension in the Indo-Pacific area following the signing of the AUKUS treaty, where the strategic alliance between Australia, the United Kingdom, and the United States on submarine technologies could upset France as well as China or Russia. This hypothesis was confirmed by a sample of Mustang Panda, a group associated with China, which targeted Australian personnel.

- Some of the techniques recently observed by Mustang Panda include the following:
- Use of spoofed files with biographies of diplomatic personnel.
- Modified the usual execution chain via RAR files, using mshta.exe and wscript.exe for PlugX dropping, including new artifacts such as TONEINS, TONESHELL, and PUBLOAD.
- PlugX backdoor deployment
- Exfiltration via unusual protocols such as MQTT

Groups using TTP associated with APT29

Lab52 has detected a campaign from an unknown actor targeting Chinese-speaking personnel. The malicious document employs social engineering techniques pretending to be the CV of a professional in finance, specifically in banking software development.

It is interesting to note that the infection chain has similarities to the one implemented by APT29 over the last few months, however, it has considerable differences. Despite using the Appvisvsubsystems64.dll side-loading DLL with the legitimate WinWord binary or the deployment of Cobalt Strike at the end of the infection, it uses a .bat file and stores the files in a different folder than usual, which seems to point to a different group.

Lazarus activity

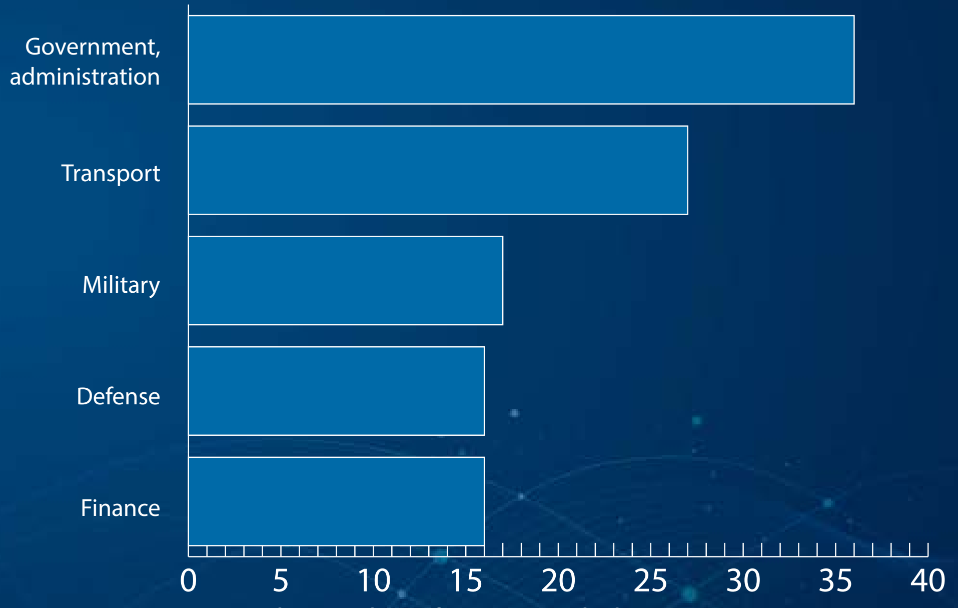
Among the APT groups' activity during the quarter, Lazarus stands out for the number of campaigns seen. Among the targets, various typologies can be observed, from the National Institute of Virology in India to companies dedicated to the defense sector, using means such as the exploitation of IIS servers or malware for macOS devices.

Among the TTPs observed are the following:

- Use of phishing DOC documents containing VBA macros for EarlyRat infection.
- Modified TightVNC software to spoof VNC software related to the communications provider to induce users to run the malware.
- Exploitation of the notepad++ color picker plugin to create additional malware "diagn.dll".
- Both client and server use RC4 and BASE64 encryption to transmit communication information.

Hacktivism

Hacktivist campaigns during the period have increased considerably, however, it is striking that the target has changed considerably in the month of June. Usually, the main targets of these campaigns were Ukraine and other geographically close countries that actively supported their cause. However, during June the main country targeted was Sweden, followed by Denmark, the Netherlands, and Switzerland. Although countries that have been involved in the conflict through support for Ukraine have been targeted by denial-of-service campaigns, they were not the main targets, indicating a change in trend in the behavior of hacktivist groups.



The number of DDoS attacks by sector.

As can be seen, the main targets of denial-of-service attacks have been those associated with government and administration, as well as the transport and military sectors. All the targets have in common that they are strategic sectors of the various countries that, in one way or another, have supported the Ukrainian cause.

Deep web

Several major leaks have been detected in the analysis of Deep Web publications carried out by the Lab52 team.

Italiamilitare.it

A user has been detected on a Deep Web forum posting a database of “italiamilitare.it”, a shop selling surplus products belonging to the Italian army. The exfiltrated database has a size of more than 350,000 lines and contains both names and emails of the shop’s customers and contacts.

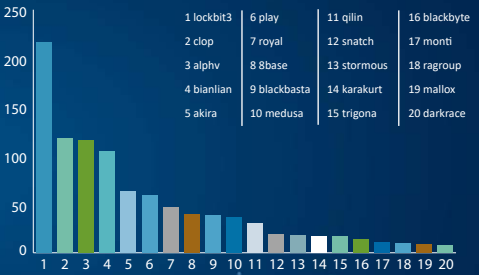
Maxar Technologies

A sale of access to a satellite operated by Maxar Technologies has been detected. This company specializes in the development of earth observation satellites, radar, and in-orbit services and satellite products.

Cybercrime

Ransomware

A total of 1065 data breach incidents by ransomware groups were detected during the second quarter of 2023. They were distributed as follows:

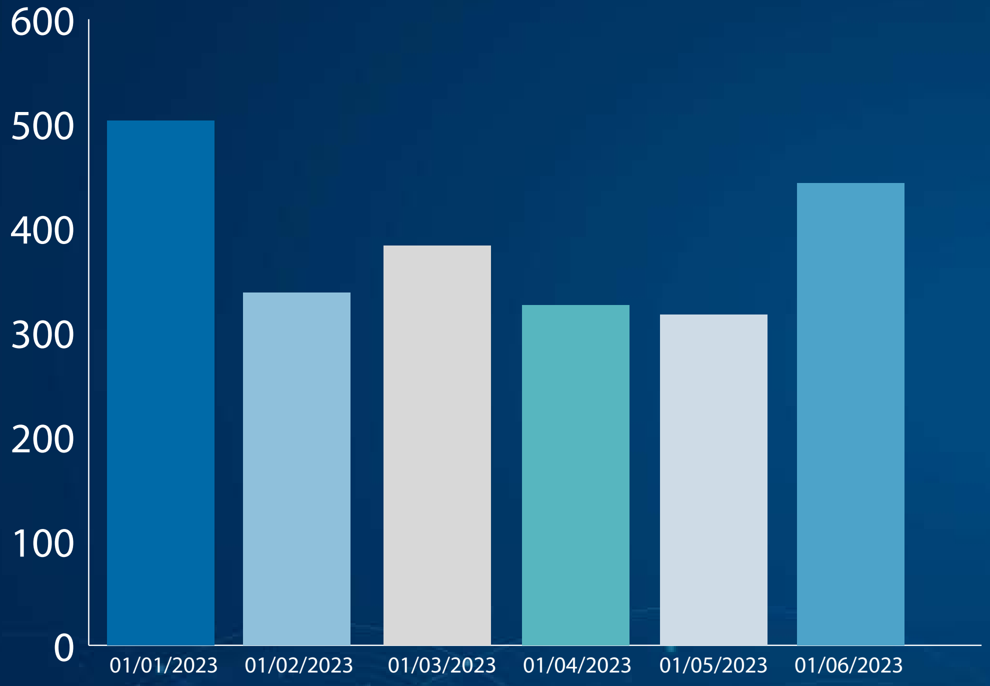


Number of attacks registered by ransomware family.

It is worth highlighting the large number of attacks carried out by the Cl0p group, despite having practically no activity in the months of April and May, during June it has very actively exploited the MOVEit vulnerability, as it has carried out a very aggressive campaign of compromises to organizations of all kinds. Using the exploitation of the previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software’s managed file transfer (MFT) software called MOVEit Transfer. This has made Cl0p the highest impact group of the month with a total of 89 victims, including Shell, BBC, Sony, and PWC.

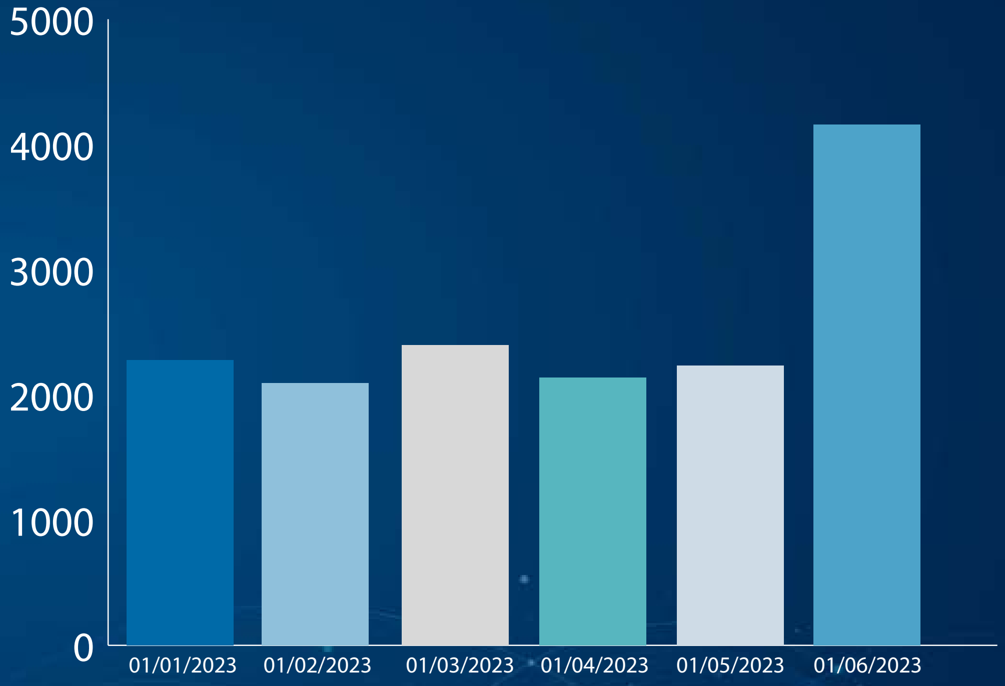
Vulnerabilities

The number of vulnerabilities during the period has increased, especially in December, as can be seen in the graph below:



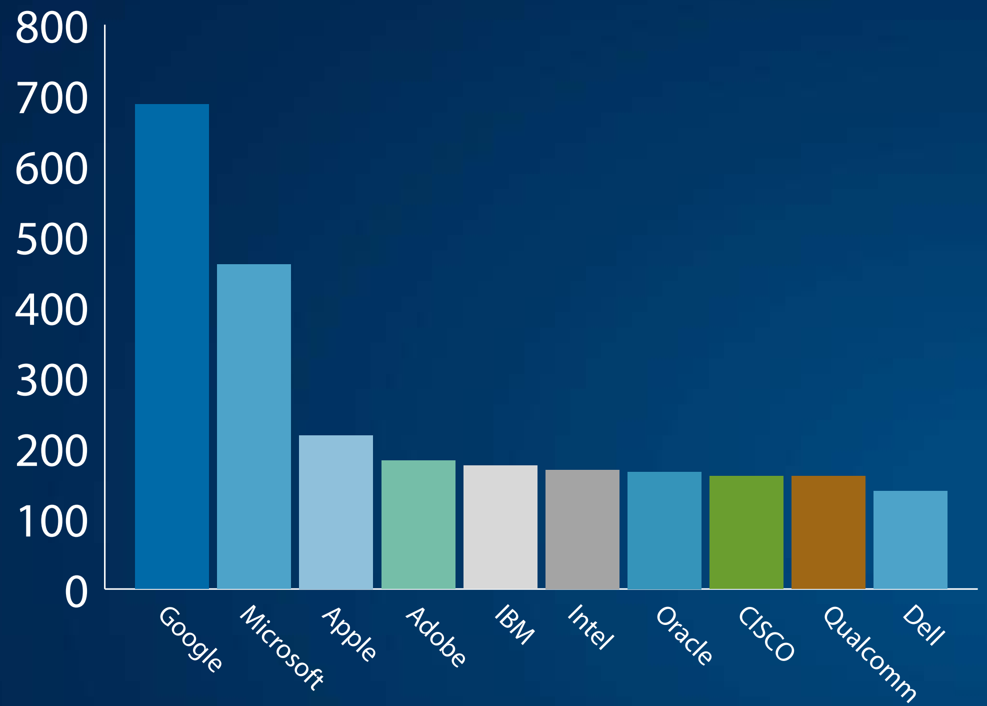
Number of vulnerabilities per month.

However, considering only critical vulnerabilities, there has been a decrease compared to the rest of the year.



The number of critical vulnerabilities per month.

The top 10 companies affected by critical vulnerabilities during the period are:



Percentage of vulnerabilities by vendor in 2Q.

The following vulnerabilities are considered the most notable during the period:

CVE-2023-34362 - MOVEit Transfer

In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5) and 2023.0.1 (15.0.1), an SQL injection vulnerability has been found in the MOVEit Transfer web application that allows an unauthenticated attacker to gain access to the MOVEit Transfer database. Depending on the database engine used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker could be able to infer information about the structure and content of the database and execute SQL statements that alter or delete items in the database. The vulnerability, rated 9.8, is being exploited by groups such as Cl0p.

CVE-2023-27997 - Fortinet FortiOS/FortiProxy

This vulnerability allows a remote attacker to execute arbitrary code or commands via specifically crafted requests. This vulnerability is also classified as critical with a value of 9.8 and has been actively exploited by different types of groups. Among them are the Volt Typhoon group associated with the Chinese government or the Nokoyawa ransomware group.

CVE-2023-1389 - TP-Link Archer AX21

A vulnerability affecting the TP-Link Archer A21 (AX1800) Wi-Fi router that has been implemented in recent versions of the Mirai IoT botnet, to carry out denial of service attacks.

CVE-2023-27350 - PaperCut NG PaperCut NG is software that allows organizations to manage the printing process. The vulnerability makes it easy for an unauthenticated remote attacker to execute arbitrary code in the context of SYSTEM. This vulnerability is being exploited by the Bl00dy Ransomware group.

CVE-2023-2868 - Barracuda Email Security Gateway

A remote command injection vulnerability exists in the Barracuda Email Security Gateway product (appliance only) affecting versions 5.1.3.001-9.2.0.006. The vulnerability stems from incomplete input validation of a user-supplied TAR file concerning the names of the files contained in the archive. As a result, a remote attacker can specifically format these filenames in a particular way that will result in the remote execution of a system command via the Perl qx operator with the privileges of the Email Security Gateway product.

CVE-2023-32373 – Apple

Use-after-free vulnerability in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, Safari 16.5, tvOS 16.5, iOS 16.5 and iPadOS 16.5. This vulnerability allows maliciously crafted web content to lead to code execution.

Findings

The number of critical vulnerabilities that appeared during the period was substantially higher than in the previous period, especially in those technologies with the largest market share, such as Fortinet. These vulnerabilities, both zero-day and day-one, are being implemented very quickly by APT actors, but also by ransomware groups.

The conflict between Russia and Ukraine continues to be the main motivation for cyberattacks, as seen in the activity of the groups, with NoName057, APT28, and the Cyber Army of Russia carrying out attacks with great assiduity.

The information published in this report has been generated from both publicly available and private data collected by Lab52, as part of the cyber intelligence service provided by S2 Grupo.

S2 GRUPO
Anticipando un mundo
ciberseguro

MADRID	SANTIAGO DE CHILE
BARCELONA	C.D. MÉXICO
VALENCIA CERT	BOGOTÁ
VALENCIA HQ	BRUSELAS
SEVILLA	LISBOA
SAN SEBASTIÁN	RÓTERDAM

Síguenos en: • @s2grupo • s2grupo.es