CTI-TEND-JUL-2024

2024 Mid-Year Cyber Threat Report

Cyber Threat Intelligence

INDEX

1. Introduction

1.1. Scope of the report

This report aims to provide a detailed overview of relevant trends and developments in the field of Threat Intelligence during the first half of 2024. It will analyse emerging threats, relevant Malicious Actors, prominent campaigns, and critical vulnerabilities identified in this period, in order to provide an in-depth understanding of the current cybersecurity landscape.

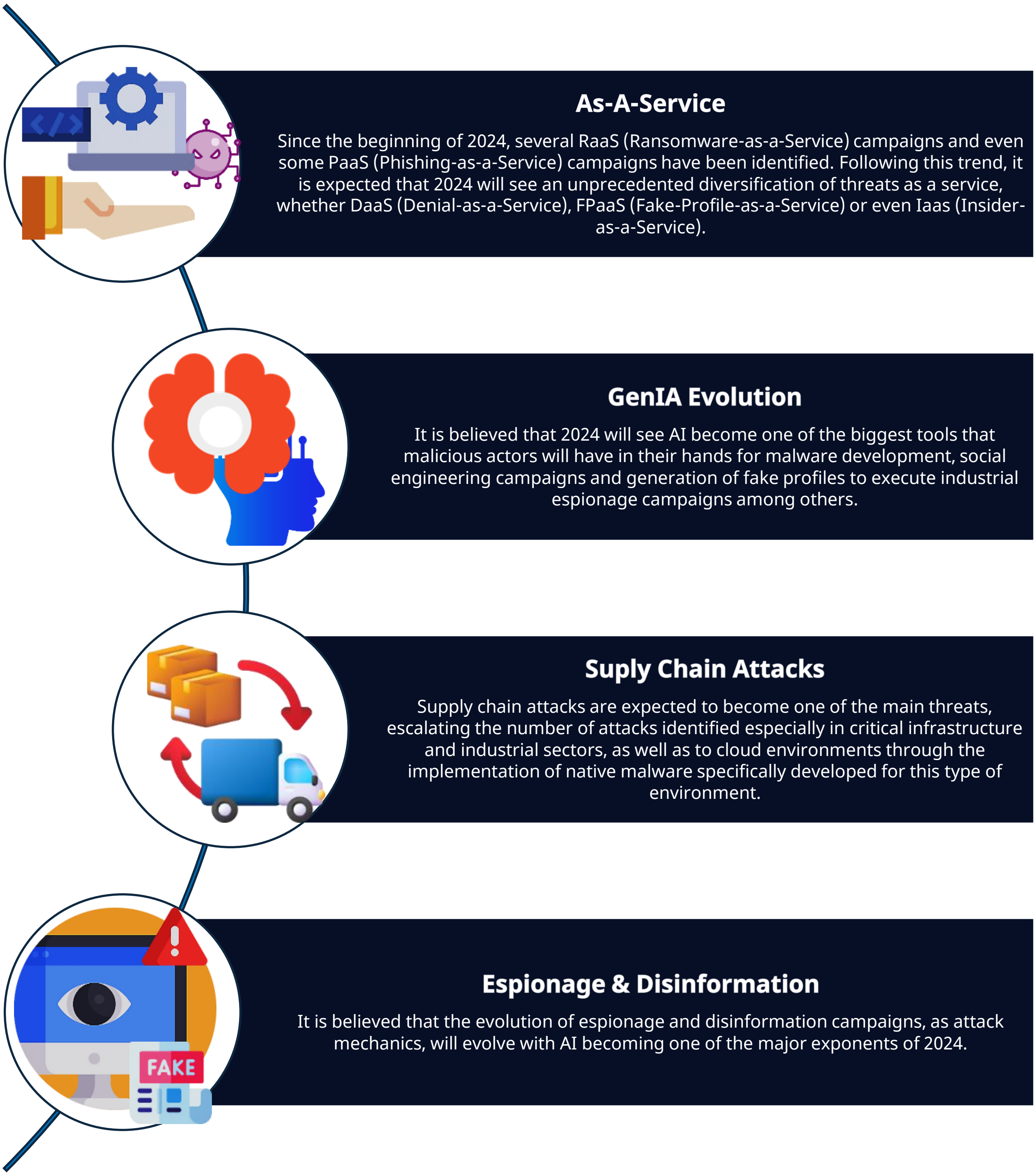
1.2. Geographical and Timeline Scope of the Report

The scope of this document focuses on Cyber Threat Intelligence trends in a global geographical scope, analysing trends occurring across the entire threat landscape in the first half of the year 2024 (January to June).

Global Threat Landscape

2. Global Threat Landscape

The evolution of the cybersecurity landscape has taken on a new stream, mainly linked to new emerging technologies and the power in the development of **Generative Artificial Intelligences (GEN-IA)**. **NTT DATA's Cyber Threat Intelligence team** has identified **four key points for 2024:**



As-A-Service

Since the beginning of 2024, several RaaS (Ransomware-as-a-Service) campaigns and even some PaaS (Phishing-as-a-Service) campaigns have been identified. Following this trend, it is expected that 2024 will see an unprecedented diversification of threats as a service, whether DaaS (Denial-as-a-Service), FPaaS (Fake-Profile-as-a-Service) or even Iaas (Insider-as-a-Service).

GenIA Evolution

It is believed that 2024 will see AI become one of the biggest tools that malicious actors will have in their hands for malware development, social engineering campaigns and generation of fake profiles to execute industrial espionage campaigns among others.

Suply Chain Attacks

Supply chain attacks are expected to become one of the main threats, escalating the number of attacks identified especially in critical infrastructure and industrial sectors, as well as to cloud environments through the implementation of native malware specifically developed for this type of environment.

Espionage & Disinformation

It is believed that the evolution of espionage and disinformation campaigns, as attack mechanics, will evolve with AI becoming one of the major exponents of 2024.

FIGURE 1 - MAIN THREAT TRENDS

2.1. Main global threats

Moving on to the main threats to be faced in the first half of 2024, **NTT DATA's Cyber Threat Intelligence** team has established a threat ranking, highlighting the **top 5 attacks with the highest number of unique registrations** for the first half of 2024:

1. **Data Leak**
   - Increase in 2024 vs. 2023: **30%**
   - Registered attacks: **2.3 million**
2. **DDoS**
   - Increase in 2024 vs. 2023: **25%**
   - Registered attacks: **1.8 million**
3. **Phishing and Vishing**
   - Increase in 2024 vs. 2023: **18%**
   - Registered attacks: **1.45 million**
4. **Ransomware**
   - Increase in 2024 vs. 2023: **20%**
   - Registered attacks: **623,000**
5. **Defacement**
   - Increase in 2024 vs. 2023: **10%**
   - Registered attacks: **150,000**

According to the contrasting data recorded in the internal monitoring tools of **NTT DATA's Cyber Threat Intelligence** team and the data collected from verified external sources, an **overall percentage increase of 39%** in the number of attacks expected for the second half of the year has been established, and it can be inferred that by the second half of 2024, the numbers will increase to almost double the number of attacks recorded compared to 2023, if they continue to have a linear ratio:

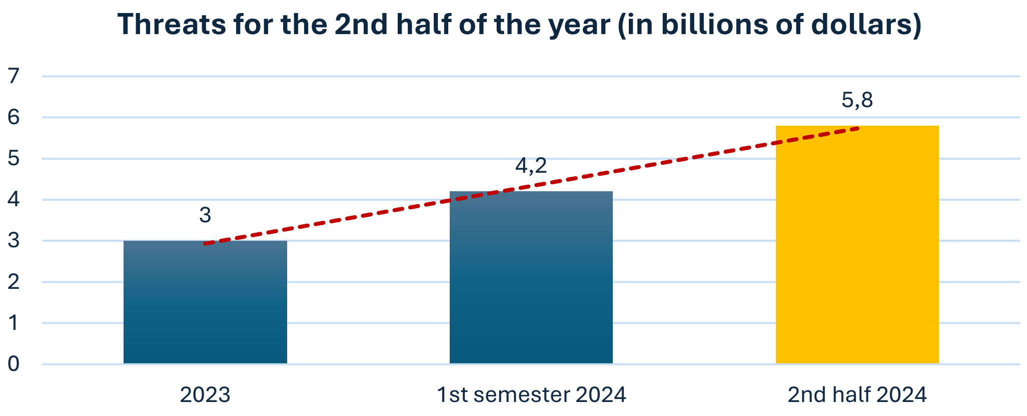
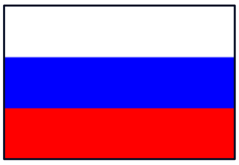
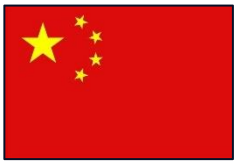


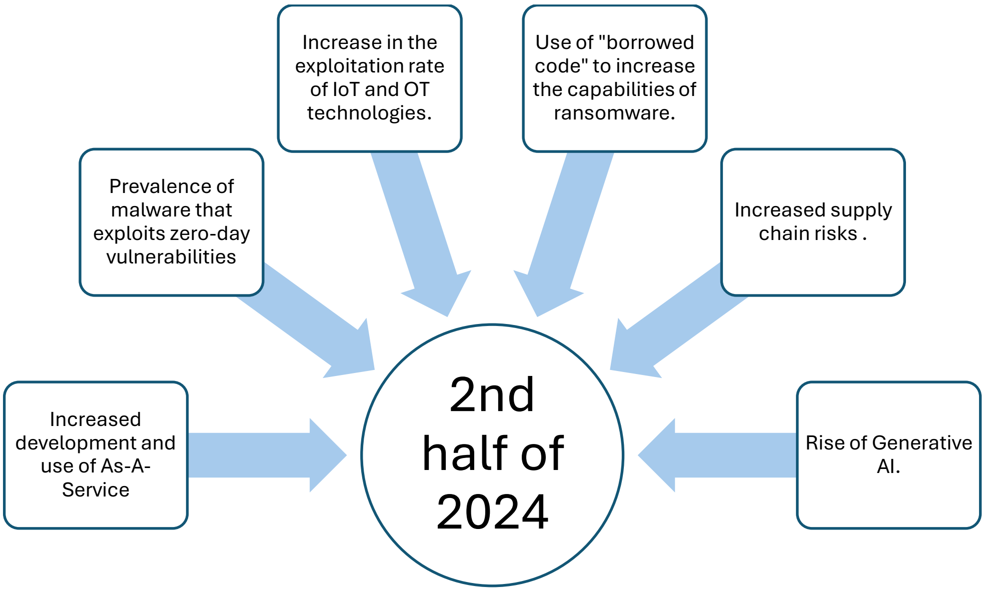
TABLE 1 - THREAT OUTLOOK FOR THE 2ND HALF OF THE YEAR

Regarding the geographic distribution of these threats, it has been estimated that the 3 most active countries with the highest attribution rate, involving all types of attacks, are:





The trend of the threats detected in the first half of the year suggests that they will continue to continue to gain strength for the second half of 2024, where the following threats can be highlighted:



2nd half of 2024

Increase in the exploitation rate of IoT and OT technologies.

Use of "borrowed code" to increase the capabilities of ransomware.

Prevalence of malware that exploits zero-day vulnerabilities

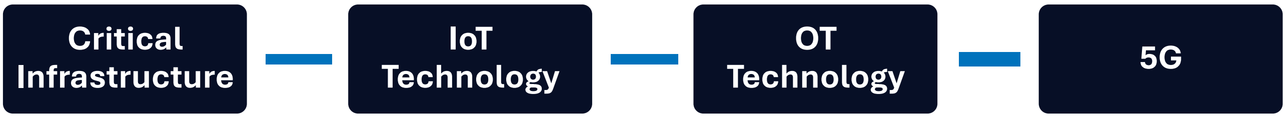
Increased supply chain risks .

Increased development and use of As-A-Service

Rise of Generative AI.

FIGURE 2 - MAIN THREATS IDENTIFIED

Among the threats mentioned, in the first half of the year, the four most threatened technological fronts have been identified as follows:



Critical Infrastructure

IoT Technology

OT Technology

5G

FIGURE 3 - MAIN RISK TECHNOLOGIES IDENTIFIED

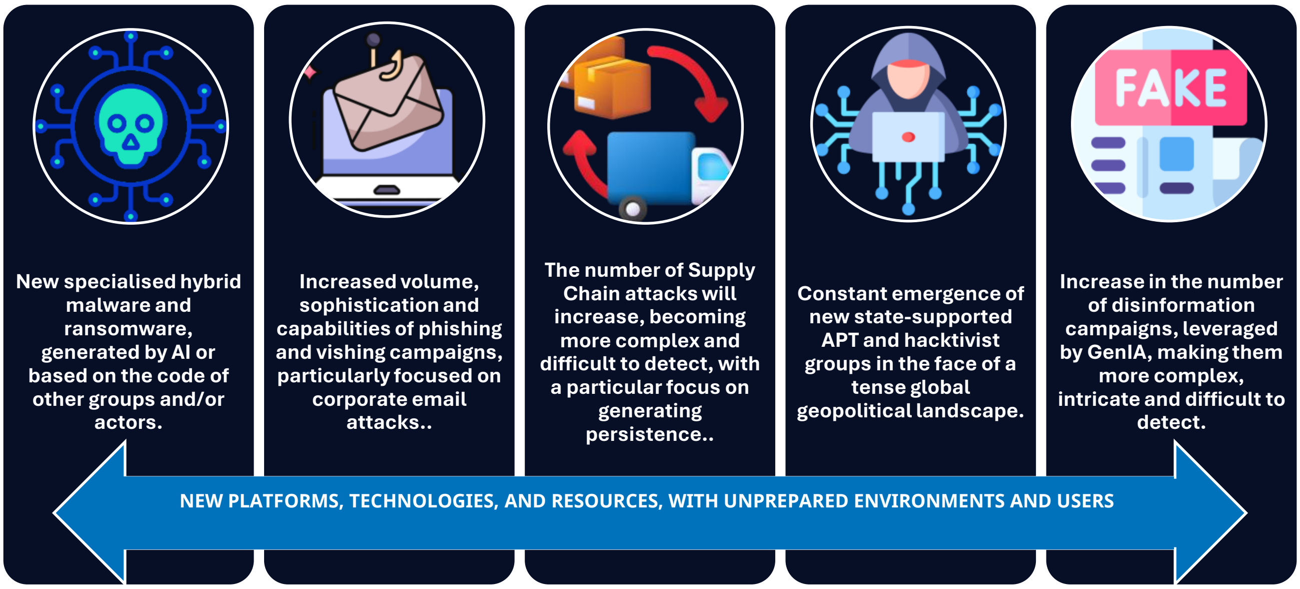
Specialised attacks, sophistication and the number of Techniques and Tactics are increasing and evolving, aligning with new emerging technologies, device interconnectivity and Generative AI. In addition, it can be concluded that attacks directed against **NATO** and **BRICS**[1] countries have increased, mainly due to the recent events concerning the conflicts in Palestine and Iran, as well as the events in Russia and Ukraine.

Countries belonging to **NATO** have accumulated about **36% of the recorded attacks** (1,500 direct attacks), while countries belonging to the **BRICS have settled at 28%** (1,200 direct attacks), with **ransomware and DDoS standing out** as the main attack typologies.

[1] BRICS+, formerly BRICS, is an association, group and political and economic forum of emerging countries, which has become an alternative international space to the G7, made up of developed countries. It was initially formed by **Brazil, Russia, India, China and South Africa**, and was created in 2010 after the incorporation of South Africa to the already existing BRIC organisation.

2.2. Emerging trends

In terms of emerging trends in general, **NTT DATA's Cyber Threat Intelligence** team has detected a series of behavioural patterns among malicious actors that allow us to speculate on what to expect in the second half of the year:



New specialised hybrid malware and ransomware, generated by AI or based on the code of other groups and/or actors.

Increased volume, sophistication and capabilities of phishing and vishing campaigns, particularly focused on corporate email attacks..

The number of Supply Chain attacks will increase, becoming more complex and difficult to detect, with a particular focus on generating persistence..

Constant emergence of new state-supported APT and hacktivist groups in the face of a tense global geopolitical landscape.

Increase in the number of disinformation campaigns, leveraged by GenIA, making them more complex, intricate and difficult to detect.

NEW PLATFORMS, TECHNOLOGIES, AND RESOURCES, WITH UNPREPARED ENVIRONMENTS AND USERS

FIGURE 4 - EMERGING TRENDS

Following this point and with special reference to threats related to **AI, 5G** and **IoT**, from the 2nd half of 2023 to the end of the 1st half of 2024, **there has been an increase in the use of Generative AI of 600%**, which mainly impacts **these 5 types of attack:**

Phishing & Vishing

- Estimated increase of around 70% by the 2nd half of 2024.
- Increase in the use of AI ChatBots, as well as the use of voice impersonation AI Vishing attacks.
- Rise of adversary-in-the-middle (AiTM) phishing attacks and browser-in-the-browser (BiTB) attacks.
- Increase in the number of DNS hijacking attacks for redirection to malware download websites.

Identity Theft

- Impersonation of prestigious brands with high reputation to avoid security measures.
- Use of LLM chatbots that make it possible to create more reliable communications and emails, eliminating most spelling and grammatical errors.
- Emergence of evolutionary campaigns that rely on AI ChatBots that allow to run campaigns pretending to be a technical support that will be almost impossible to detect.

Disinformation & Fake News

- Increase in the complexity sophistication of disinformation campaigns thanks to AI.
- Increase in data distribution capacity through 5G technologies, increasing the range of action of malicious groups.
- Creation of photos and videos by AI to increase the credibility of campaigns.

DDoS Evolution

- Substantial increase in the volume of these attacks, with 5.2 million HTTP DDoS attacks.
- New groups emerge, many of them state-sponsored.
- Centralisation of IoT-based DDoS attacks, taking advantage of the massification of IoT connectivity, especially in OT technologies.
- The botnet range for attack execution will increase, specialising in exploiting vulnerabilities associated with IoT devices.

Credential Stuffing

- GenIA tools that have made it possible to develop methods and techniques for bypassing standard security measures such as CAPTCHA and IP rate limiting.

A clear example of the use of AI and following the analysis of a security incident detected in this first half of the year, was a **fraud of almost $26 million** where malicious actors simulated a meeting executed with AI-generated and controlled avatars. (CNN, SCMP ,2024).

2.3. Significant data leaks or sales in underground markets

In the first half of the year, **NTT DATA's Cyber Threat Intelligence** team has estimated a total of almost **10,000 confirmed incidents**, in which approximately **35 billion data and records** have been affected:

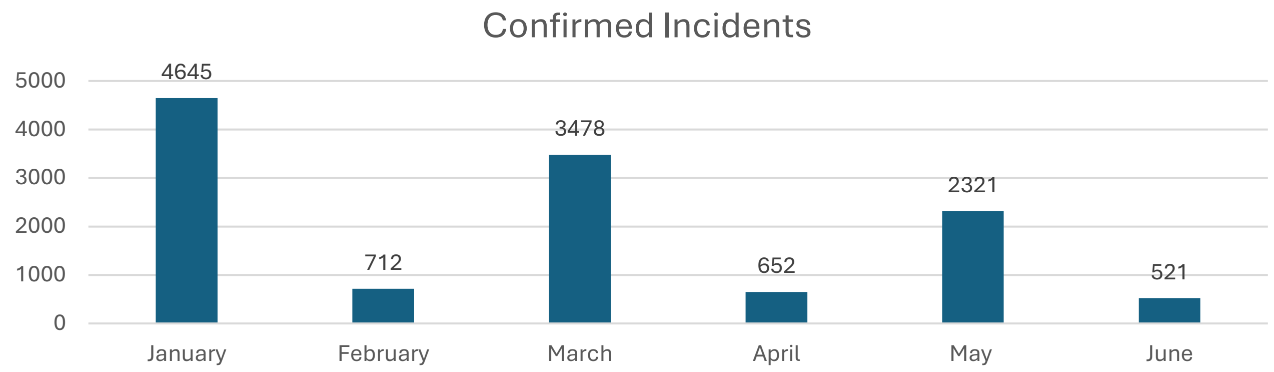


TABLE 2 - CONFIRMED INCIDENTS

The most prominent data breaches of the last 6 months are:

MONTH	ORGANISATION	COUNTRY	SECTOR	COUNT OF LEAKED DATA
JANUARY	MOAB	Global	Multiple	± 26.000.000.000
	Indian Mobile Network	India	Telecommunication & Technology	± 750.000.000
	IPL Consulting	Russia	Telecommunication & Technology	Desc. [± 60 TB of data]
FEBRUARY	Zenlayer	United States	Telecommunication & Technology	± 384.658.212
	MRA	United States	Commercial & Professional Services	Desc. [± 3 TB of data]
	Optum	United States	Healthcare	Desc. [± 6 TB of data]
MARCH	AMMEGA	Denmark	Manufacturing	Desc. [± 3 TB of data]
	916 Google Firebase	United States	Multiple	± 124.605.664
	NHS Dumfries & Galloway	United Kingdom	Healthcare	Desc. [± 3 TB of data]
APRIL	Discord	United States	Entertainment & Media	± 4.186.879.104
	iSharingSoft	United States	Telecommunication & Technology	± 35.000.000
	Baidu, Honor, Huawei, iFlytek, OPPO, Samsung, Tencent, Vivo & Xiaomi	China	Telecommunication & Technology	± 1.000.000.000
MAY	KyungChang's	China	Industry	Desc. [± 1.6 TB of data]
	Landmark Life	United States	Insurance	Desc. [± 2.4 TB of data]
	99 Digital	United States	Telecommunication & Technology	Desc. [± 5.2 TB of data]
JUNE	Ticketmaster	Multiple	Entertainment & Media	± 560.000.000
	Tea Group	United States	Commercial & Professional Services	Desc. [± 1 TB of data]

TABLE 3 - MAIN DATA GAPS FOR THE 1ST HALF OF 2024

2.4. Global statistics on security incidents, types of attacks and malicious actors involved

With reference to global trends in security incidents, **NTT DATA's Cyber Threat Intelligence** team has established a ranking of the **most relevant security incidents during the first half of 2024**, according to their impact:

INCIDENT	AFFECTED COUNTRY	ATTRIBUTION GROUP	ATTRIBUTION COUNTRY	INFORMATION OF INTEREST
Breach of Microsoft executive accounts (January 2024)	United States	Midnight Blizzard (NOBELIUM)	Russia	A breach of **Microsoft** executive accounts that affected several U.S. government agencies. This breach involved unauthorised access to high-profile accounts within **Microsoft**, allowing attackers to obtain privileged and potentially sensitive information.
MITRE attack (January 2024)	United States	UNC5221	China	**Mitre Corporation** was the victim of a massive cyber-attack that disabled its activities in January. The attackers exploited two Zero-Day vulnerabilities in Ivanti Connect Secure security devices, which allowed them to access Mitre's research and development network, known as NERVE.
Ivanti VPN Compromise (February 2024)	United States	APT 29 (Cozy Bear)	Russia	**Ivanti's VPNs** were targeted in a widespread compromise that significantly **affected several U.S. government agencies**, allowing the attackers to gain unauthorised access to internal networks. This not only compromised the confidentiality of sensitive data, but also exposed the agencies to operational and national security risks. The vulnerabilities exploited were part of a series of flaws that had not been adequately patched.
Diversified attack against the U.S. healthcare sector (February 2024)	United States	ALPHV/BlackCat	Russia	**UnitedHealth Group** and **Change Healthcare** reported being victims of a cyberattack that compromised sensitive data of millions of patients, who had personal and financial data compromised.
Massive attack on Fujitsu Infrastructure (March 2024)	Japan	Unknown	Unknown	In March, **Fujitsu** confirmed it had been the victim of a cyber-attack that affected several of its global operations, compromising critical data and systems.
Dell Customer Data Breach (May 2024)	Worldwide	A BreachForum user named Menelik	Unknown	**Dell** warned its customers of a data breach after a threat actor claimed to have stolen information on approximately 49 million customers, as the computer maker began sending data breach notifications via email to its customers.
Attack on Ticketmaster/Live Nation (May 2024)	Worldwide	ShinyHunters	Unknown	The cybercriminal group **ShinyHunters** shared details of an alleged attack on **Ticketmaster** and **Live Nation** and offered the data for sale for a price of $500,000. The data was for sale on a popular hacking forum and ShinyHunters claimed to have a 1.3 terabyte database with information on some 560 million users including names, addresses, emails, and phone numbers.
Snowflake Data Breach (June 2024)	United States	UNC5537	Unknown	**Snowflake,** a cloud data storage platform, was the victim of widespread data theft attacks targeting its customers that compromised the information of several organisations.

TABLE 4 - MAIN INCIDENTS FOR THE FIRST HALF OF 2024

Threat trends by sector

3. Threat trends by sector

3.1. Most common types of attacks in each sector

According to the analysis and detections carried out by the **NTT DATA's Cyber Threat Intelligence** team, during the first half of the year the main threats are well defined and delimited, being able to highlight 3 types of attack:

- **Ransomware**
- **DDoS**
- **Phishing**

The 5 sectors most affected globally by this type of cyber-attacks are:

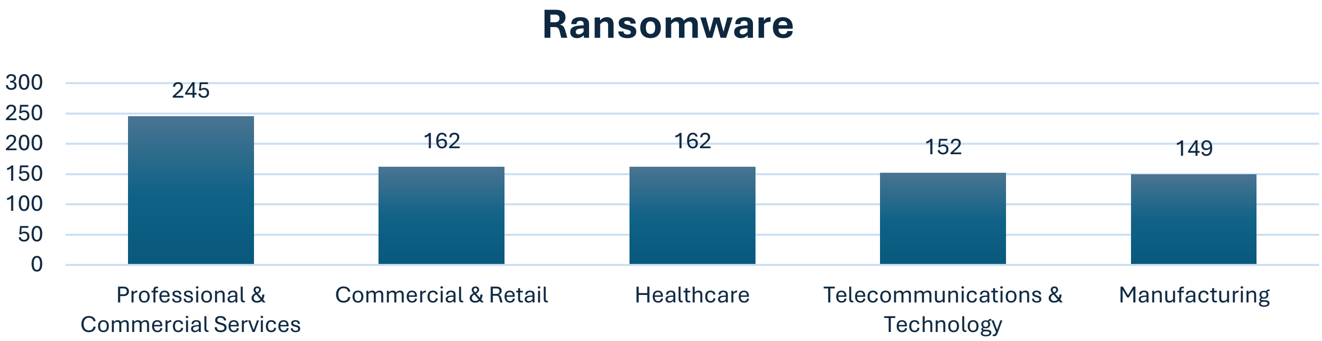


TABLE 5 - 5 SECTORS MOST AFFECTED BY RANSOMWARE ATTACKS

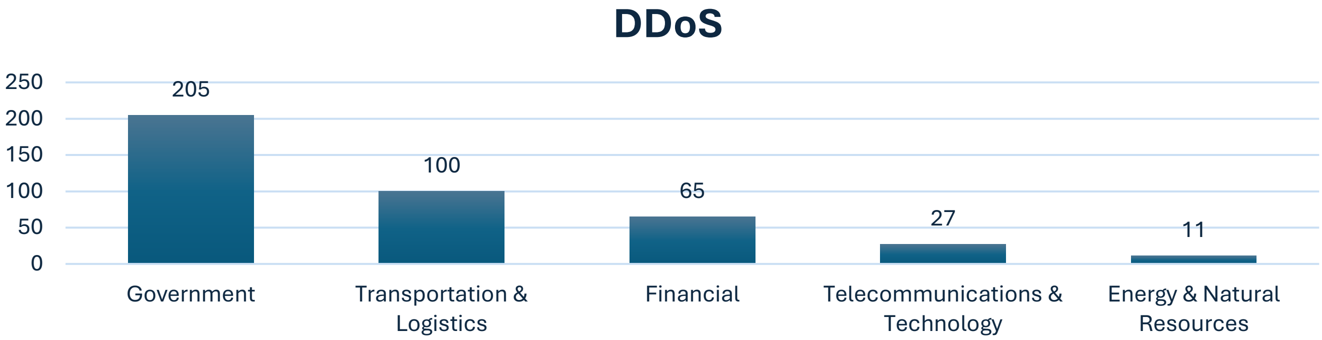


TABLE 6 - 5 SECTORS MOST AFFECTED BY DDOS ATTACKS

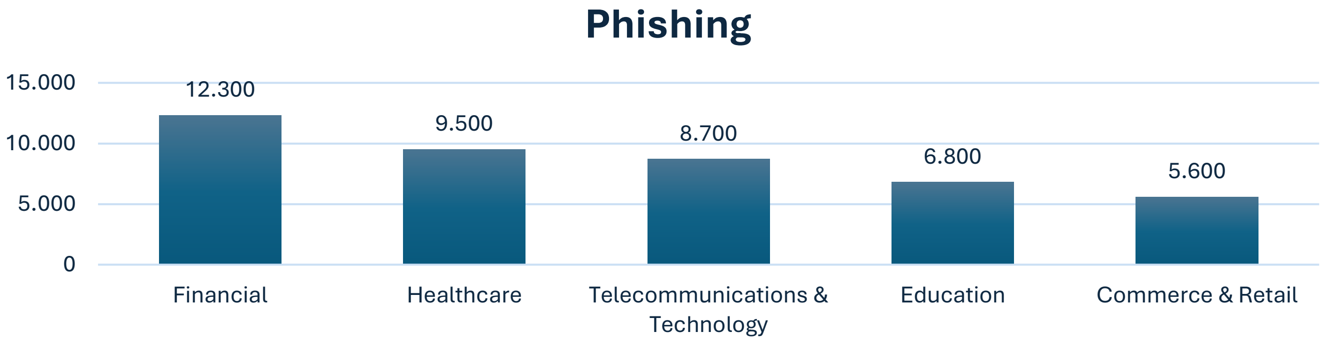


TABLE 7 - 5 SECTORS MOST AFFECTED BY PHISHING ATTACKS

Following the trend observed during the first half of the year, attacks targeting the professional and business services, government and financial sectors were the three most targeted sectors in their respective categories, followed by retail, transportation and logistics and healthcare sectors.

After conducting an analysis of the attacks and the data collected, **NTT DATA's Cyber Threat Intelligence** team has reached the following conclusions:

The malicious actors/groups that focus their activity on ransomware have focused their attacks on the commercial and professional sectors, mainly targeting SMEs, as they are companies with a high rate of security breaches, in many cases lacking in the basic application of cybersecurity principles and unable to invest large amounts of capital in keeping their systems and networks secure by incorporating optimised measures.

Denial-of-service attacks are observed to be directed against government institutions and critical infrastructure and have multiplied, mainly due to current international conflicts and the rise of state-sponsored groups.

Phishing attacks continue to focus on sectors such as finance and healthcare for two reasons: financial gain and data value. In the case of the financial sector, they focus on impersonating banks or payment platforms, seeking to obtain user data and credentials.

3.2. Identification of the most vulnerable and targeted sectors

The **Government sector** and **the services sector** has suffered a significant hit, placing it at the top of the attacked industries, followed by the **transportation, information technology (IT)** and **commerce sectors**, indicating an alarming vulnerability in sectors that are critical to the functioning of society.

However, it is the substantial year-on-year increase in attacks on **government administrations** that underscores a strategic shift in target preference by cybercriminals and state-sponsored groups, mainly due to the current international conflicts, allowing us to hypothesize about the possible political and geostrategic motivations behind these attacks.

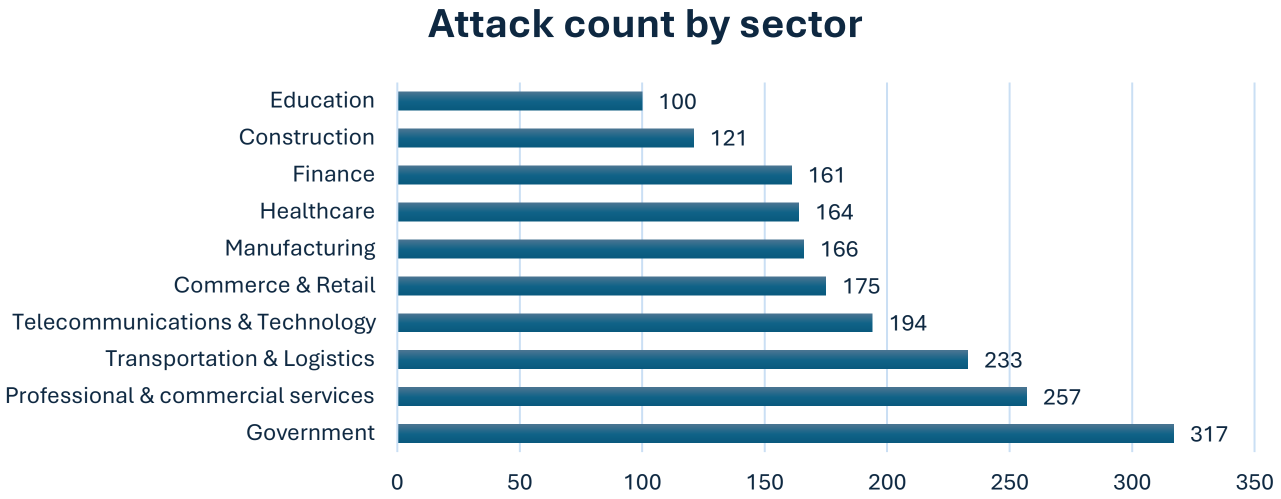


TABLE 8 - COUNT OF ATTACKS BY SECTOR

Furthermore, in the first half of 2024, **North America was the region most affected** by ransomware attacks, followed by **Europe** and the **Asia-Pacific region.**

The largest increase in reported attacks compared to the first half of 2023 was observed in **Europe**, with a **significant increase of 64%.** This significant increase could be attributed to factors such as **increased digitisation of services and regulatory environments** that may make organisations more vulnerable or visible targets, coupled as previously indicated with international conflicts. In contrast, **North America experienced a 16% increase**, indicating a sustained focus by attackers in this region.

Finally, it is interesting to note **the increase in attacks against the manufacturing, education, and healthcare sectors**, which have seen a significant increase as a target for malicious actors and groups. This is mainly due to the expansion of IoT devices for monitoring OT systems and also due to the value of the data they control, which is very profitable as a commodity in forums and underground markets.

Threat Actors

4. Threat Actors

In the following section, an analysis is made of the threat actors with the highest activity during the first half of 2024 as well as the new threat actors appearing for the first time in the global landscape, identifying the motivations, skills, resources, and contexts that identify them.

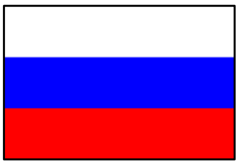
4.1. State-sponsored Threat Actors

In the first half of 2024, **Advanced Persistent Threat (APT)** groups in various regions of the world, such as **China, North Korea, Iran,** and **Russia**, showed an increase in dynamic and innovative cyber activities.

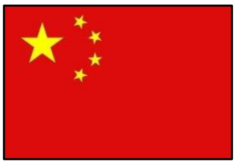
- **State of Iran:** Malicious actors such as ***Homeland Justice*** and ***Mint Sandstorm*** intensified their espionage efforts by targeting government and academic institutions in the West and Middle East with sophisticated phishing attacks and sophisticated malware, such as ***MediaPI*** and ***MischiefTut***. In addition, malicious actor ***Charming Kitten*** advanced with their social engineering tactics through a counterfeit webinar platform, and malicious actor ***Tortoiseshell*** intensified its focus on the aerospace and defence sectors in the Middle East, illustrating a broad and strategic enhancement of Iran's cyber capabilities.
- **State of Russia:** Malicious actors such as ***APT29*** accessed high-value targets such as *Microsoft*, compromising corporate emails and source code repositories. This malicious actor also shifted its attention to European policy domains, attacking German political parties by exploiting a recently developed **WINELOADER** backdoor. Meanwhile, malicious actor ***Gamaredon*** maintained its sophisticated attacks against the Ukrainian military, and ***APT28*** exploited vulnerabilities in Ubiquiti ***EdgeRouter*** routers to create extensive botnets, demonstrating Russia's adaptability and strategic depth in cyber operations.
- **State of China:** Malicious actors, such as ***Earth Lusca***, which leveraged geopolitical tensions with Taiwan by increasing targeted phishing campaigns; ***Evasive Panda*** exploited the Tibetan diaspora during the Monlam Festival with Trojanised software; and ***Earth Krahang*** conducted comprehensive attacks against global government entities. These operations exploited vulnerabilities and leveraged compromised systems for extensive intelligence gathering, underscoring the strategic and aggressive pursuit of intelligence by Chinese state-sponsored threat actors.
- **North Korean State:** The ***Kimsuky*** malicious actor expanded its reach across the APAC region using sophisticated malware deployment techniques to maintain covert access and create supply chain attack opportunities using PyPI software repositories. At the same time, the ***Lazarus Group*** malicious actor exploited a new vulnerability in the Windows kernel to enhance its ***FudModule rootkit***, facilitating deep system manipulation and evasion of advanced security measures.

In the first half of 2024, the APT landscape showed intensified efforts by Iranian, Russian, Chinese, and North Korean malicious actors.

Iranian groups such as **Homeland Justice** and **Mint Sandstorm** intensified their operations with sophisticated attacks against domestic and academic targets.



Russian entities such as **Nobelium** and **Gamaredon** were versed in using their enhanced tactics against high-value corporate and military targets.



Chinese malicious actors, including **Earth Lusca** and **Evasive Panda**, took advantage of geopolitical events in the Asian region to deploy advanced multi-stage malware, expanding their espionage footprint globally.

North Korean groups such as **Kimsuky** and **Lazarus** demonstrated enhanced capabilities in multi-stage attacks, focusing on supply chain attacks and exploitation of zero-day vulnerabilities.

State-sponsored cyberattacks have experienced a significant increase, evidencing the growing sophistication and frequency of these threats globally. The following graph illustrates the percentages of attacks attributed to various government-backed malicious actors, highlighting the emerging trends and the most active actors in this period.

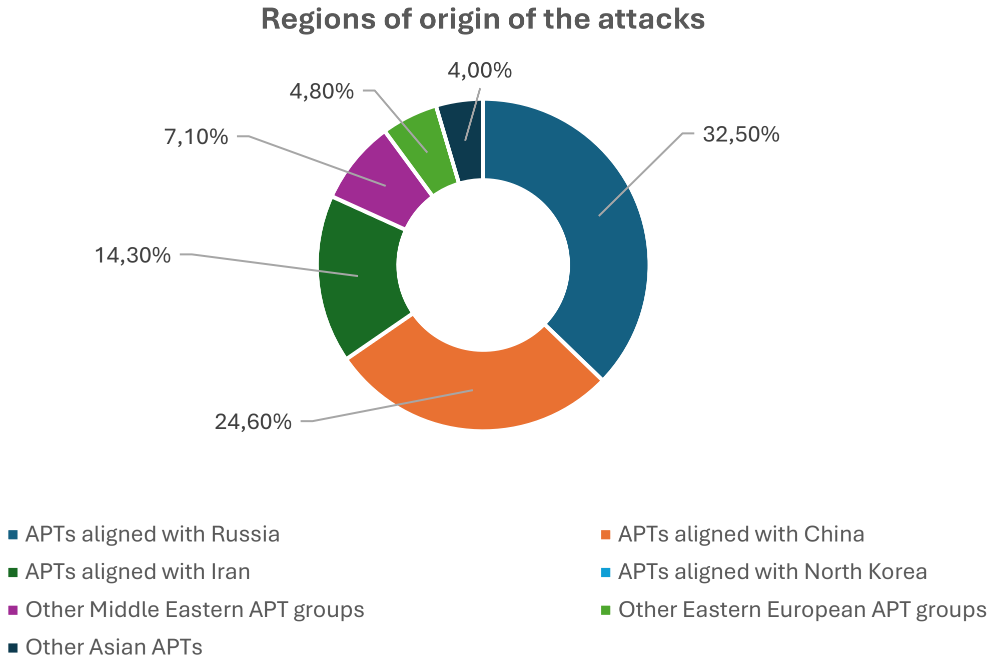


TABLE 9 - PERCENTAGES OF ATTACKS BY MALICIOUS ACTORS SPONSORED BY STATES

4.2. Ransomware groups

The year 2024 started with a vastly different picture than 2023, while the numbers spiked in Q4 2023 with 1309 cases, in Q1 2024, the ransomware industry was down to 1048 cases. This is a **22% decrease in ransomware** attacks compared to Q4 2023.

NTT DATA's Cyber Threat Intelligence team estimates that the two reasons for this decline could be the **intervention of law enforcement**, as observed with the **LockBit** and **BlackCat** malicious actors, and the **decrease in ransom payments**, which led ransomware groups to withdraw and look for alternative sources of revenue.

Below is the evolution of ransomware attacks in the first half of 2024:

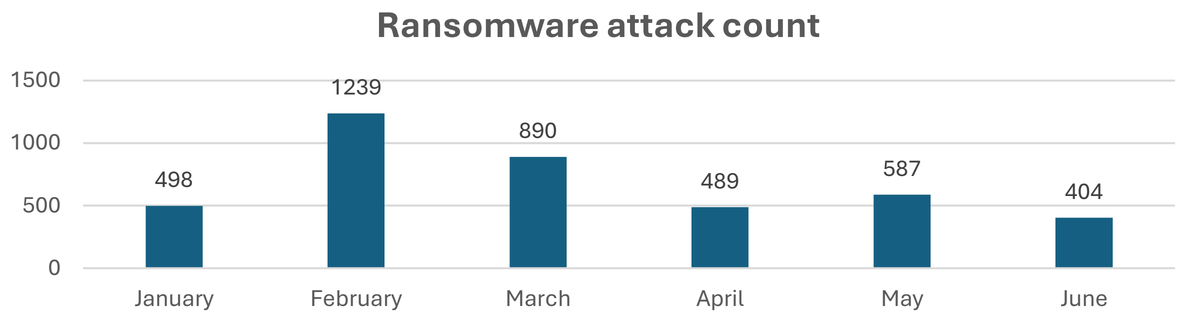


TABLE 10 - COUNT OF RANSOMWARE ATTACKS

The following chart shows the most active ransomware groups during the first half of 2024:

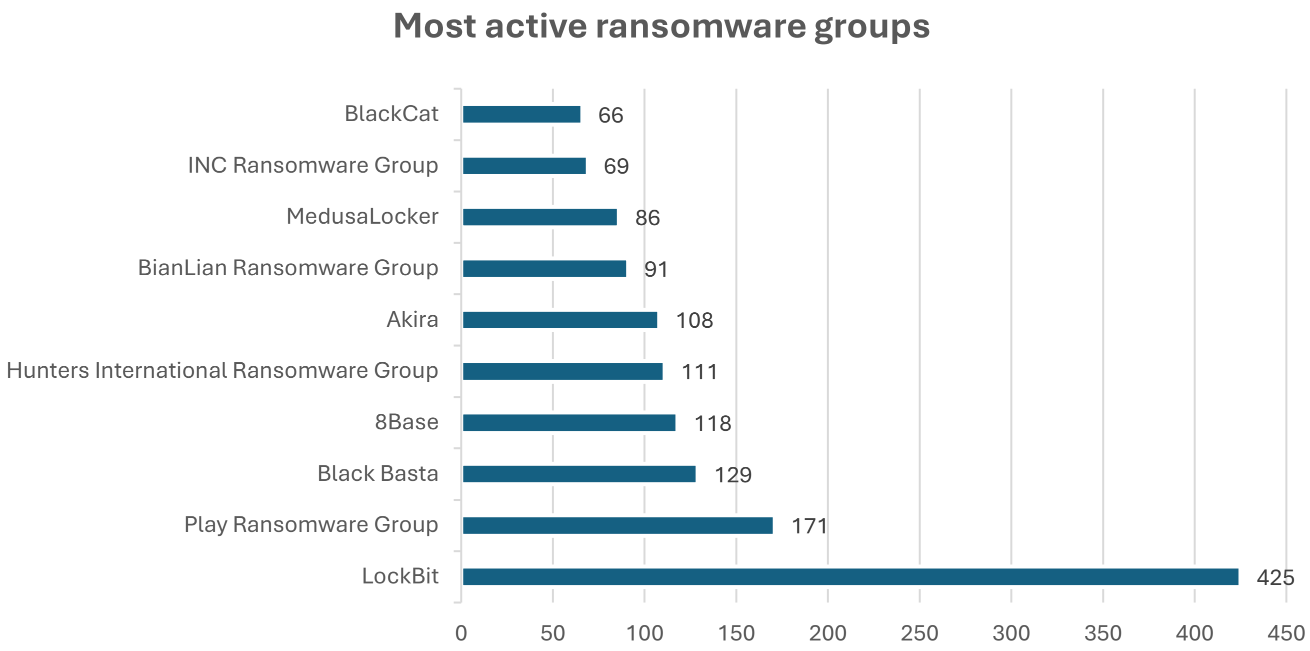


TABLE 11 - MOST ACTIVE RANSOMWARE GROUPS

4.3. New Malicious Actors

During the first half of 2024, new malicious actors have been identified who, although they may appear novel in this environment, are sometimes backed by large malicious groups. This means they do not go unnoticed and must be taken into account due to the significant capabilities they may demonstrate.

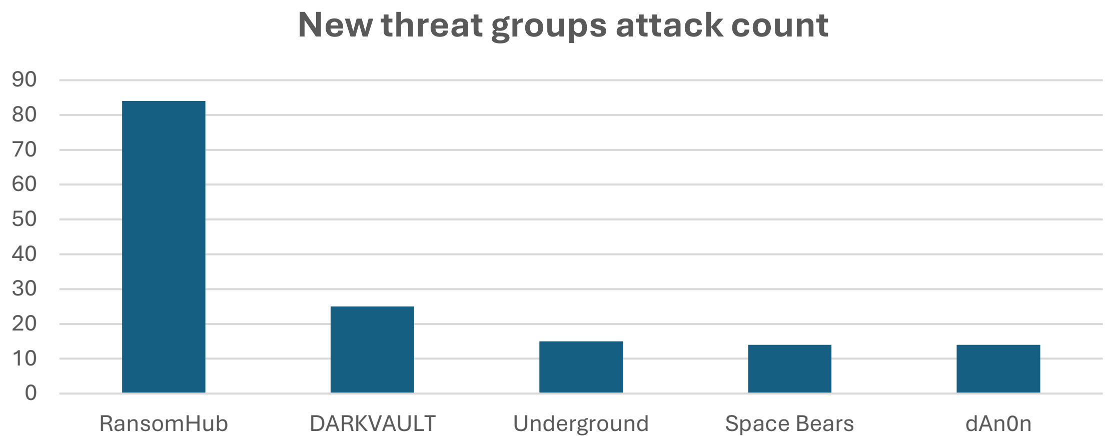


TABLE 12 - COUNT OF ATTACKS BY NEW THREAT GROUPS

RansomHub

RansomHub is a new ransomware group that has come to prominence in 2024 for its claims backed by data leaks. This group allegedly composed of hackers from various parts of the world **pursues financial targets and refrains from attacking nations such as Cuba, North Korea, and China, as well as non-profit organisations.** Despite its global focus, its operations are reminiscent of traditional Russian ransomware groups, sharing similarities in the companies attacked and in its stance toward nations allied to Russia. RansomHub operates as a Ransomware-as-a-Service (RaaS) group, collaborating with affiliates and setting strict guidelines for them. Affiliates must comply with the set agreements, and any non-compliance results in a ban and termination of the collaboration. The group claims that it will provide a free decryptor to victims if the affiliate fails to do so after receiving payment or if it targets a banned organisation. RansomHub recruits affiliates from the **RAMP** forum and uses rewritten **ESXi ransomware** strains in **Golang**, capable of encrypting data before exfiltrating it.

DARKVAULT

DarkVault is a self-proclaimed online community and a unique ransomware group that engages in various illegal activities such as, doxing, website defacement, malware creation, scams, spamming and fraud. Although some reports suggest that DarkVault could be part of **LockBit** or affiliated with this group due to the similarity of its data leakage site (DLS) to that of **LockBit 3.0**, there is no conclusive evidence of this relationship. The group has two main pages: one for posting victims of alleged ransomware attacks or data exfiltration and another detailing their illegal activities. However, outside of the published victims, its DLS and Telegram channel lack additional information.

Underground

Underground Team is a new ransomware group that encrypts files on affected machines, and although the ransomware they use encrypts files, the extensions of the affected files remain unchanged. The ransomware group has its negotiation site on the TOR network, where victims can talk to the attacker about ransomware details. The URL of the TOR site is included in the ransom note **"!!!readme!!!!.txt"** along with additional information about where the attacker claims to have exfiltrated the information and the type of information. The ransom note also claims that the attacker will release the stolen data unless the ransom is paid within three days. The attacker also claims to be willing to help victims improve their network security.

Space Bears

SpaceBears is a new group in the trend of data brokers, which has gained prominence recently. The group is suspected to be located in Moscow, Russia and has claimed several high-profile cyberattacks, showcasing alleged advanced tactics. On its data leak site (DLS), **SpaceBears** lists companies that have leaked sensitive data, including login credentials, intellectual property, and personal and financial data. These groups use a strategy of extortion, pressuring insurance companies and worrying customers to gain revenue from the compromised data. The group offers instructions in its DLS for those who believe their data has been compromised, stating that, after receiving payment, they will remove the post, delete the data from their servers and provide a decryption tool for the "encrypted" files. They also offer guidance on how to prevent future similar attacks.

dAn0n

In April 2024, the **dAn0n Hacker Group** emerged, which, although labelled by some sources as a ransomware group, appears to operate more as a data broker. They have announced multiple victims from March through the end of May, and their data breach sites on Clearnet and TOR are active. Sources indicate that dAn0n engages in both data brokering and ransomware attacks, using phishing emails for initial access and deploying custom ransomware and obfuscated scripts to execute their payload. They employ privilege escalation and defence evasion tactics to maintain persistence and avoid detection. However, so far, no concrete evidence of ransomware or specific techniques have been found to support these claims.

Techniques, Tactics and Procedures (TTPs)

5. Techniques, Tactics and Procedures (TTPs)

5.1. Description of the most common TTPs used by cybercriminals

While the TTPs of some threat actors remain constant over time, social engineering remains the preferred means of gaining access to a target organisation or compromising an individual's device. Likewise, other groups have renewed their tools and expanded the scope of their activities. These periodic semi-annual reviews are intended to highlight the most significant and commonly used techniques related to APT groups.

MITRE ATT&CK ID	DESCRIPTION
T1566 - Phishing	Adversaries can send phishing messages to gain access to victims' systems. All forms of phishing are social engineering that are sent electronically. Phishing can be targeted, known as spear phishing. In spear phishing, the adversary targets a specific person, company, or industry. More generally, adversaries can conduct non-targeted phishing, such as mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, usually to execute malicious code on victims' systems. **Mitigation:** • Antivirus can automatically quarantine suspicious files. • Perform audits or analysis of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. • Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity. • Determine whether certain websites or attachment types (e.g., .scar, .exe, .pif, .cpl, etc.) that can be used • Use email authentication and anti-spoofing mechanisms to filter messages based on sender domain validity (using SPF) and message integrity (using DKIM) controls. • Users can be trained to identify social engineering techniques and phishing emails. **References:** • https://cybersecuritynews.com/facebook-ad-phishing-attack/ • https://cybersecuritynews.com/greatness-paas-tool-microsoft-365/ • https://cybersecuritynews.com/telegram-know-secure-messaging/ • https://gbhackers.com/cryptochameleon-kit/ • https://gbhackers.com/flyingyeti-winrar-vulnerability-malware-attacks
T1059 - Command and script interpreter	Adversaries can abuse command interpreters and scripts to execute commands, scripts, or binary files. These interfaces and languages provide ways to interact with computer systems and are a common feature on many different platforms. **Mitigation:** • An antivirus can be used to automatically quarantine suspicious files. • On Windows 10, enable attack surface reduction (ASR) rules to prevent Visual Basic and JavaScript scripts from executing potentially malicious downloaded content. • When possible, only allow signed scripts to execute. • Disable or remove unnecessary or unused interpreters or shells. • Use application control where appropriate. For example, the restricted language mode of PowerShell can be used to restrict access to sensitive or dangerous language elements, such as those used to execute arbitrary Windows files or APIs (e.g., Add-Type). • When PowerShell is required, consider restricting the PowerShell execution policy to administrators.

	• Script blocking extensions can help prevent the execution of scripts and HTA files that may be commonly used during the exploitation process. **References:** • https://cybersecuritynews.com/poc-exploit-fortisiem/ • https://cybersecuritynews.com/tp-link-archer-c5400x-router-flaw-remote-hack/ • https://cybersecuritynews.com/winrar-flaw-deceive-users/ • https://gbhackers.com/hackers-microsoft-access-malware/ • https://gbhackers.com/social-engineering-black-basta-ransomware
T1203 – Exploitation for customer execution	Adversaries can exploit software vulnerabilities in client applications to execute code. Vulnerabilities may exist in software due to unsecure coding practices that can lead to unforeseen behaviour, exploiting certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Often, the most valuable exploits for an offensive toolkit are those that can be used to gain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to work with, so they are a useful target for exploit research and development because they are so useful. **Mitigation:** • Isolated browser environments can be used to mitigate some of the impact of exploitation but escapes from isolated environments may still exist. Other types of virtualisations and application micro-segmentation can also mitigate the impact of client-side exploitation. Risks of additional exploits and implementation weaknesses may still exist. Security applications that look for behaviour used during exploitation, such as Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET), can be used to mitigate some exploit behaviours. Control flow integrity checking is another way to identify and potentially stop the occurrence of a software exploit. • Many of these protections depend on the architecture and binary of the target application for compatibility. **References:** • https://cybersecuritynews.com/chrome-security-update-125/ • https://cybersecuritynews.com/hackers-advertising-pulse-connect/
T1219 - Remote access tools	An adversary can use legitimate desktop support and remote access software to establish an interactive command and control channel to attack systems within networks. These services, such as VNC, Team Viewer, AnyDesk, ScreenConnect, LogMein, AmmyyAdmin, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be enabled by application control within a targeted environment. **Mitigation:** • Properly configure firewalls, application firewalls and proxy servers to limit outbound traffic to sites and services used by remote access tools. • Network intrusion prevention and detection systems that use network signatures can also prevent traffic to these services. • Use application whitelisting to mitigate the use and installation of unapproved software. **References:** • https://attack.mitre.org/techniques/T1219/ • https://gbhackers.com/fbi-cisa-warns-alphv-blackcat-ransomware/ • https://gbhackers.com/hijacking-connectwise-screenconnect-server/ • https://packetstormsecurity.com/news/view/35567/ConnectWise-Exploit-Could-SpurRansomware-Free-For-All.html • https://services.google.com/fh/files/misc/connectwise-screenconnect-remediationhardening-guide.pdf • https://thehackernews.com/2024/02/fbi-warns-us-healthcare-sector-of.html
T1486 – Encrypted data for impact	Adversaries can encrypt data on target systems or on a large number of systems on a network to disrupt the availability of system and network resources. They may attempt to make stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This can be done to extract monetary compensation from a victim in exchange for a

	decryption or decryption key (ransomware) or to make data permanently inaccessible in cases where the key is not saved or transmitted. **Mitigation** • Consider implementing IT disaster recovery plans that contain procedures for making and periodically testing data backups that can be used to restore the organisation's data. • In some cases, the means to decrypt files affected by a ransomware campaign are made public. Research trusted sources for public releases of decryption tools/keys to reverse the effects of ransomware. • Identify potentially malicious software and audit or block software by using whitelisting tools such as AppLocker or software restriction policies where appropriate. • Execution consists of techniques that result in the execution of adversary-controlled code on a local or remote system. Techniques that execute malicious code are often combined with techniques from all other tactics to achieve broader goals, such as exploring a network or stealing data. For example, an adversary could use a remote access tool to execute a PowerShell script that performs remote system discovery. **References:** • https://attack.mitre.org/techniques/T1486/ • https://gbhackers.com/black-basta-ransomware-decryptor/ • https://gbhackers.com/hackers-hijacking-ms-sql-servers/ • https://gbhackers.com/kasseika-ransomware-kill-antivirus/ • https://gbhackers.com/phobos-ransomware-office-document/ • https://packetstormsecurity.com/news/view/35385/Babuk-Tortilla-Ransomware-DecryptedAfter-Hackers-Arrest.html

TABLE 13 - MOST USED TTPS BY MALICIOUS ACTORS

As malicious actors continue to adopt more stealthy and innovative attack methods, **active use of approximately two-thirds of the techniques in the MITRE ATT&CK framework is observed**. Among these, defence evasion and process injection emerge as predominant tactics.

Phishing maintained its position as the top initial access vector in a variety of threat incident types, with phishing email compromise standing out in particular.

In addition, during 2024, there was an **increase in attacks that began with social engineering techniques.** There was also an increase in incidents initiated by Threat Actors exploiting public applications, such as Cisco's Adaptive Security Appliance (ASA) virtual private networks and ScreenConnect remote management tools. **Attacks targeting known vulnerabilities showed a higher probability of culminating in ransomware incidents.**

Vulnerabilities

6. Vulnerabilities

The following section contains an analysis of the main vulnerabilities published during the first half of the year 2024, detailing those that have had the greatest impact on information systems.

6.1. Trend analysis

In terms of criticality, CVEs classified as **critical** and **high** represent a significant part of the total, resulting in an **increase in remote code execution attacks, denial of service or privilege escalation.**

Organisations and public institutions are expected to respond quickly to these threats by applying the solutions offered by the providers of the technologies concerned.

As can be seen below, the **medium** criticality vulnerabilities stand out above the rest, but this should not divert attention from the **high** and **critical** vulnerabilities identified, as these are the ones that can have the greatest negative impact on an organisation or system.

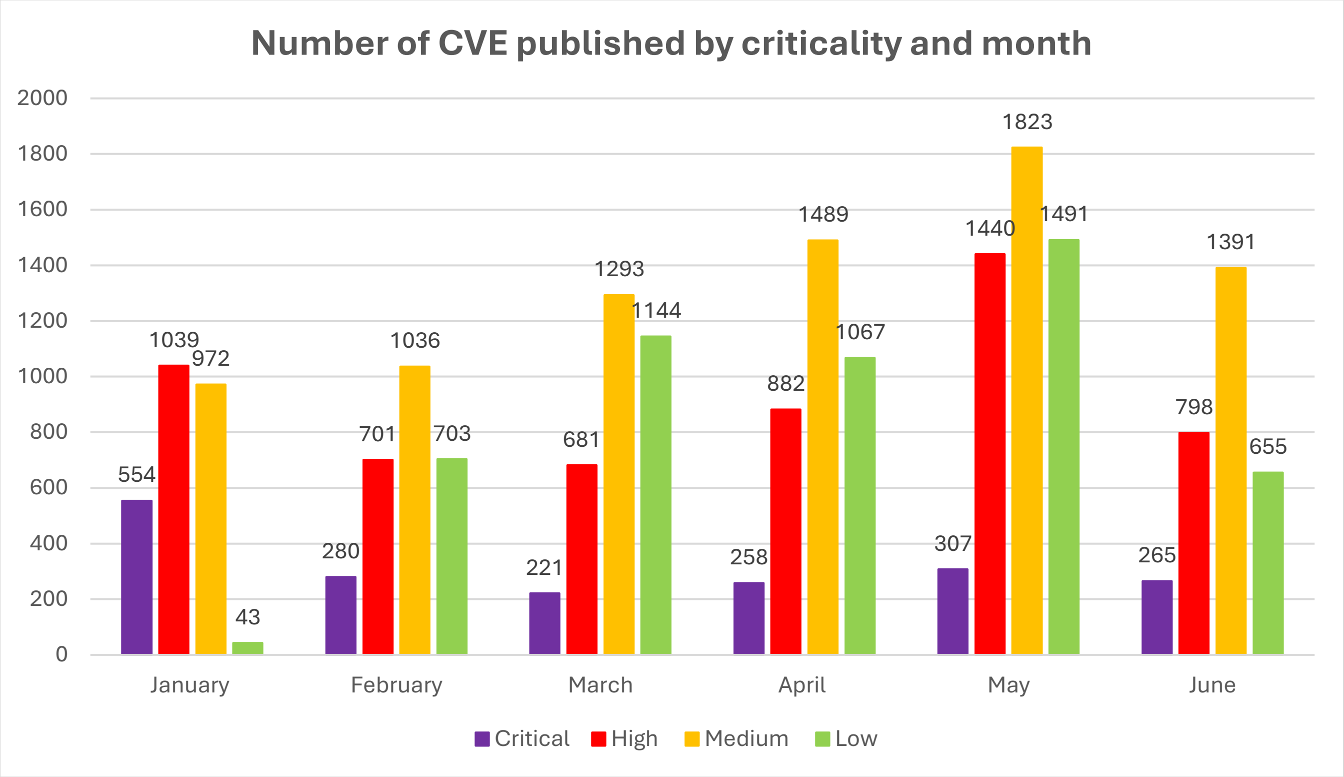


TABLE 14 - CVE COUNT BY CRITICALITY AND MONTH

There is a strong predominance in the publication of vulnerabilities related to **Cross-Site-Scripting (XSS)**. This is a cause for concern because it is one of the highest risk vulnerabilities for an application, since exploiting this type of vulnerability could lead to obtaining session cookies, identity spoofing, malicious redirects, access to sensitive information, undesired actions, among others.

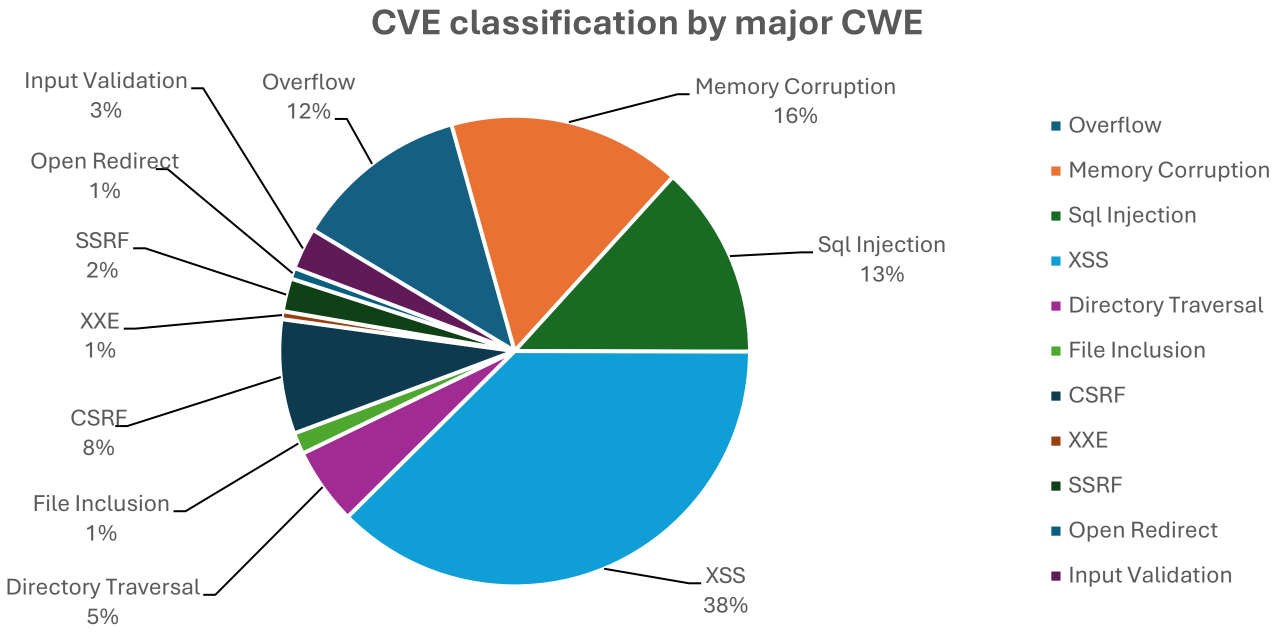


TABLE 15 - CLASSIFICATION OF CVE BY MAIN CWE (COMMON WEAKNESS ENUMERATION)

6.2. Most critical vulnerabilities

The following is a list of vulnerabilities published during 2024 that have been deemed most critical according to their CVSS v3:

CVE	CVSS v3	DESCRIPTION (SCOPE)	AFFECTED SOFTWARE	EXPLOITS AND PATCHES
		JANUARY		
CVE-2024-23897	9.8 – Critical	Vulnerability that allows unauthenticated **attackers to read arbitrary files** in the Jenkins driver file system.	**Jenkins** 2.441 and earlier. **LTS** 2.426.2 and earlier.	35 exploits. 2 patches.
CVE-2024-0204	9.8 – Critical	Omitting authentication **allows an unauthorised user to create an administrator** user through the administration portal.	**Fortra** GoAnywhere MFT prior to 7.4.1.	9 exploits. 1 patch.
CVE-2024-21887	9.1 – Critical	Command injection vulnerability in web components that allows an authenticated administrator to send specially crafted requests and **execute arbitrary commands** on the device.	**Ivanti Connect Secure** (9.x, 22.x) and **Ivanti Policy Secure** (9.x, 22.x).	0-Day. 10 exploits. 2 patches.
		FEBRUARY		
CVE-2024-21762	9.8 – Critical	An out-of-bounds script that allows an attacker to **execute unauthorised code or commands through specifically crafted requests.**	**Fortinet**: **FortiOS** versions 7.4.0 a 7.4.2, 7.2.0 a 7.2.6, 7.0.0 a 7.0.13, 6.4.0 a 6.4.14, 6.2.0 a 6.2.15, 6.0.0 a 6.0.17. **FortiProxy** versions 7.4.0 a 7.4.2, 7.2.0 a 7.2.8, 7.0.0 a 7.0.14, 2.0.0 a 2.0.13, 1.2.0 a 1.2.13, 1.1.0 a 1.1.6, 1.0.0 a 1.0.7.	0-Day. 8 exploits. 2 patches.
CVE-2024-1709	9.8 – Critical	**Authentication bypass vulnerability** using an alternate path or channel, which may **allow an attacker direct access to confidential information or critical systems.**	**ConnectWise ScreenConnect** 23.9.7 and earlier.	0-Day. 17 exploits. 4 patches.
		MARCH		
CVE-2023-48788	9.8 – Critical	An incorrect neutralisation of special elements used in a **SQL command** ('SQL injection') that **allows an attacker to execute unauthorised code or commands** through specially crafted packets.	**Fortinet FortiClientEMS** version 7.2.0 to 7.2.2 and 7.0.1 to 7.0.10.	2 exploits. 1 patch.
CVE-2024-27198	9.8 – Critical	Vulnerability that **allows bypassing authentication to perform administration actions.**	**JetBrains:** CI/CD Server **(TeamCity)**, version 2023.11.4 and earlier.	13 exploits. 1 patch.
		APRIL		
CVE-2024-3400	10 – Critical	**Arbitrary file creation vulnerability in the GlobalProtect function** that allows injection of commands with **root privileges** into the firewall.	**Palo Alto Networks**: Some specific versions of **PAN-OS** 11.1, 11.o and 10.2.	0-Day. 42 exploits. 4 patches.
CVE-2024-4040	10 – Critical	Server-side template injection vulnerability that allows unauthenticated remote attackers to **read files from the file system outside the VFS Sandbox**, bypass authentication to gain administrative access and perform remote code execution on the server.	**CrushFTP** on all versions prior to 10.7.1 and 11.1.0.	0-Day. 15 exploits. 4 patches.
CVE-2024-3273 CVE-2024-3272	9.8 – Critical	An unknown function in the **/cgi-bin/nas_sharing.cgi file of the HTTP GET Request Handler component is affected.** Manipulation of the argument system leads to **command injection**. It is possible to launch the **attack remotely.**	**D-Link DNS-320L, DNS-325, DNS-327L** and **DNS-340L** up to 20240403.	11 exploits. 1 patch.

			NOTE: This vulnerability only affects products that are no longer supported by the vendor.	
MAY				
CVE-2024-4358	**9.8 – Critical**	Authentication bypass vulnerability that allows, in IIS, an unauthenticated attacker to **gain access to restricted Telerik Report Server functionality.**	**Progress Telerik Report Server,** version 2024 Q1 (10.0.24.305) and earlier.	7 exploits. 1 patch.
CVE-2024-4671	**9.6 – Critical** **NOTE:** Chromium Security Severity: High.	**Use-After-Free (UAF)** vulnerability that allows a remote attacker who has compromised the rendering process to potentially perform a sandbox escape through a crafted HTML page.	Visuals component of **Google Chrome** older than 124.0.6367.201.	0-Day. 2 patches.
JUNE				
CVE-2024-4577	**9.8 – Critical**	Vulnerability that allows a malicious user to **bypass options to the running PHP binary**, thus revealing the source code of scripts, execute arbitrary PHP code on the server, etc. **NOTE:** When using Apache and PHP-CGI on Windows, if the system is configured to use certain code pages, Windows can use the "Best-Fit" behaviour to replace characters on the command line given to Win32 API functions. The PHP CGI module may misinterpret those characters as PHP options.	**PHP:** Versions 8.1.* prior to 8.1.29. Versions 8.2.* prior to 8.2.20. Versions 8.3.* prior to 8.3.8.	46 exploits. 1 patch.
CVE-2024-5806	**9.1 – Critical**	Incorrect authentication vulnerability in Progress MOVEit Transfer (SFTP Module) can lead to Authentication Bypass.	**MOVEit Transfer:** since 2023.0.0 prior to 2023.0.11. since 2023.1.0 before 2023.1.6 from 2024.0.0.0 before 2024.0.2	2 exploits.

TABLE 16 - MOST CRITICAL VULNERABILITIES IDENTIFIED IN THE FIRST HALF OF 2024

6.3. Most Exploited Vulnerabilities

Some of the most exploited vulnerabilities by attackers throughout the semester have been the following:

CVE-2024-3094

Release date: **29/03/2024**
Affected software: **Linux XZ**
Patches: **6**
CVSS v3: **10**
Exploits: **59**
0-Day

CVE-2024-24919

Release date: **28/05/2024**
Affected software: **Check Point**
Patches: **2**
CVSS v3: **8.6**
Exploits: **50**
0-Day

CVE-2024-32002

Release date: **14/05/2024**
Affected software: **Git**
Patches: **1**
CVSS v3: **9.1**
Exploits: **49**

CVE-2024-4577

Release date: **09/06/2024**
Affected software: **PHP**
Patches: **1**
CVSS v3: **9.8**
Exploits: **47**

CVE-2024-3400

Release date: **12/04/2024**
Affected software: **PAN-OS**
Patches: **4**
CVSS v3: **10**
Exploits: **42**
0-Day

CVE-2024-23897

Release date: **24/01/2024**
Affected software: **Jenkins**
Patches: **2**
CVSS v3: **9.8**
Exploits: **35**

6.4. Detected or published 0-days

The trend of 0-Day vulnerability exploitation marks a **significant increase** compared to previous years, with active exploitation of these vulnerabilities suggesting an increase in the speed with which malicious actors exploit software weaknesses, affecting a wide range of users and organisations.

Highlights include the increase in 0-click exploits, which do not require user interaction to activate; the reuse of exploits with slight modifications (more than 40% of the 0-Day exploits discovered are variants of previously reported vulnerabilities); and the use of 0-Day exploits to increase the impact of ransomware attacks.

TECHNOLOGY AND ASSET PROVIDERS

Around **40%** of 0-Days affect **Google** in products such as Chrome, Pixel and Android devices, followed by **20% in Microsoft**, mainly in Windows operating systems and Outlook applications. The rest of the zero-day vulnerabilities are distributed among vendors such as **Apple, VMware, Adobe,** or **Apache**.

In terms of the assets affected, **mobile devices** (Pixel, Android, and iOS) are in the lead **(50%)**, while **desktop applications (20%)** and servers and the **virtualisation sector (20%)** are also on the rise, highlighting the importance of security in productivity applications and critical infrastructures.

THREAT ACTORS

The main regions affected by the exploitation of zero-day vulnerabilities are **North America, Europe and Asia**; the **Black Basta** ransomware group (Cardinal or UNC4393), State Threat Actors such as **APT29** (Russia) and **APT41** (China) focused on espionage, with strategic targets such as critical infrastructure or advanced technological sectors and groups such as Lazarus focused on financial entities and governmental organisations stand out.

Finally, it is common that the public exposure of technical details of the vulnerabilities detected, such as in events like **Pwn2Own Vancouver 2024**, encourages a rapid exploitation of these vulnerabilities and generates a greater number of attacks by Malicious Actors.

Below are some of the 0-Day highlighted for 2024:

CVE-2024-0519	**MULTIPLE 0-DAYS IN IVANTI**	**CVE-2024-29988**
Flaw in Chrome's V8 engine, exploited for remote code execution and patched by Google in January.	**CVE-2023-46805, CVE-2024-21887, CVE-2024-21893, CVE-2024-21888, CVE-2024-22024** Remote command execution, unauthenticated access to restricted resources and persistent access. CISA highlighted its exploitation for credential theft and evasion of mitigation measures.	Omission of Microsoft SmartScreen security features from exploits in compressed files.
CWE-787 CWE-125 CWE-119 BUFFER OVERFLOW	**CWE-78, CWE-918, CWE-77, CWE-287, CWE-611**	**CWE-693**

TABLE 17 - MOST EXPLOITED 0-DAY

6.5. Published security patches

Analysing the vulnerabilities by vendor, the main affected vendors are those that offer the largest number of technology products and services, with Microsoft and Google being the most affected in terms of number of published vulnerabilities.

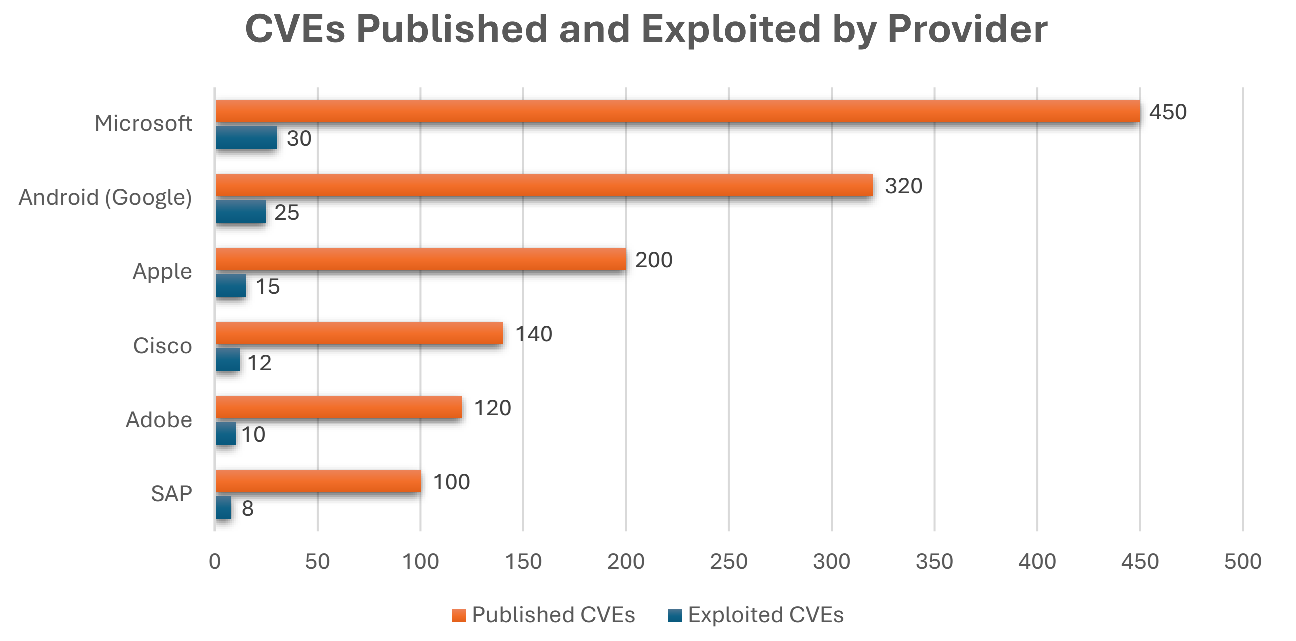


TABLE 18 - CVE PUBLISHED AND USED BY PROVIDER

The number of **security patches published** has followed an upward trend, with March being the month with the most solutions registered.

According to the vulnerabilities published by vendor, the solutions offered by **Microsoft and Google are in the lead**, addressing the need for a rapid response to mitigate attacks on affected products.

The effort made by vendors and companies to reduce security risks through the publication of security patches and the application of frequent updates can be seen.

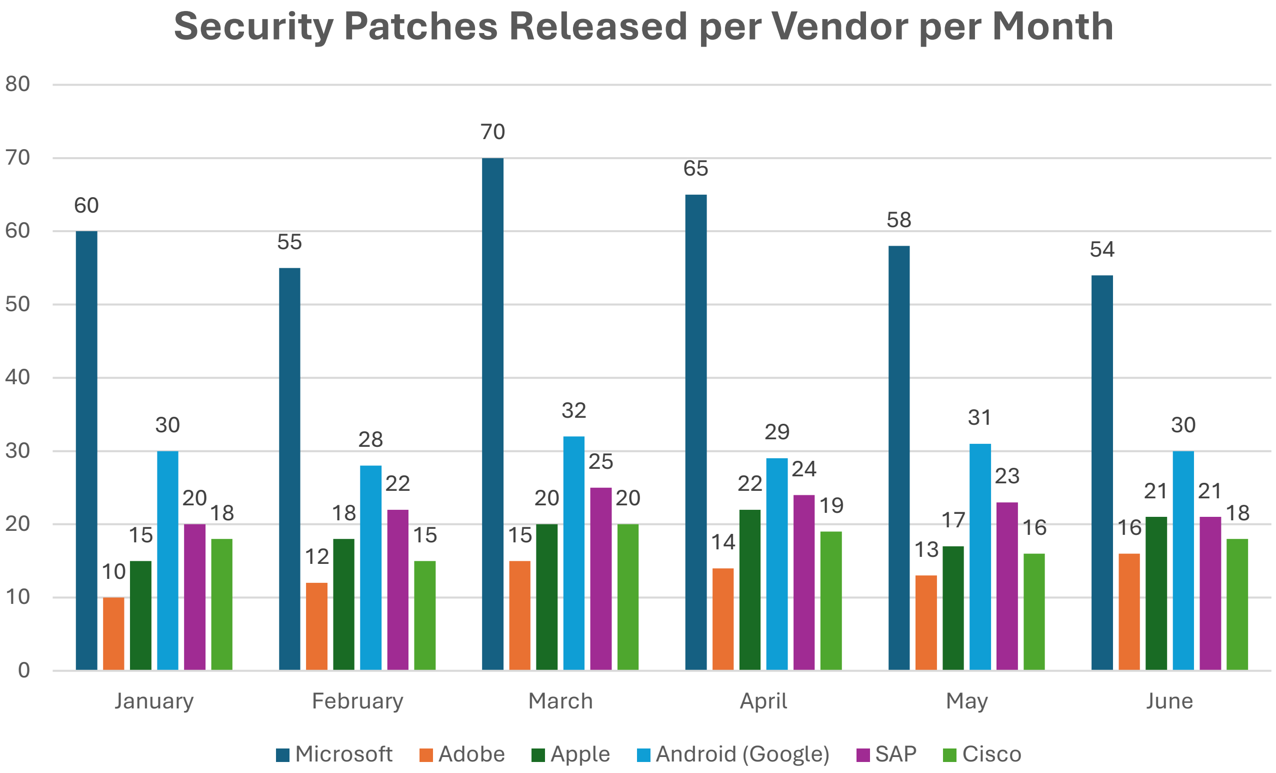


TABLE 19 - TREND OF SECURITY PATCHES RELEASED BY VENDOR BY MONTH