CTI Trends

Cyber Threat Intelligence

Second Semester2024

Index

Index

Introduction

1.1. Report scope

This report aims to provide a detailed and comprehensive overview of the key trends, incidents, and developments in the field of Threat Intelligence during the second semester of 2024. It will analyze emerging threats that are reshaping the cybersecurity landscape, the Threat Actors that have exhibited significant activity, the most notable cyber campaigns, as well as the critical vulnerabilities identified during this period. Additionally, recurring patterns and future trends that could influence risk mitigation strategies will be examined.

1.2. Geographical and temporal scope of the report

The scope of this document focuses on Cyber Threat Intelligence (CTI) trends from a global perspective, allowing readers to understand how threats evolve in an interconnected manner across different geographical and temporal contexts.

The analysis covers events and dynamics observed within the cyber threat ecosystem during the second semester of 2024, from July to December. This period has been marked as a critical interval where significant events and shifts in threat behavior have been identified.

Global Threat Landscape

2. Global threat landscape

2.1 Geopolitics and Cybersecurity

The **Cyber Threat Intelligence** department at **NTT DATA** analyzed the increasing intersection between geopolitics and cybersecurity during the second semester of 2024, highlighting a world that is increasingly interconnected and vulnerable to global dynamics. Cyberspace has become a strategic domain where global tensions, regional conflicts, and power rivalries manifest through cyberattacks, digital espionage, and influence campaigns.

During this period, both state and non-state **Threat Actors** have intensified their operations, impacting critical infrastructure and key strategic sectors. This report provides an in-depth study of three key elements: global threats driven by geopolitical tensions, the main **Threat Actors** behind these operations, and the impact of these activities on specific sectors.

Technological advancements have also transformed this landscape. Tools such as **Artificial Intelligence (AI)** and the **Internet of Things (IoT)** have increased the complexity of cyberattacks, enabling the development of adaptable malware and tailored phishing campaigns.

Additionally, **Advanced Persistent Threats (APTs)** have become crucial instruments for espionage and sabotage, aiming to infiltrate critical systems while evading conventional security strategies. At the same time, **supply chain attacks** have proven to be particularly effective, compromising vendors and spreading malware through legitimate software updates, affecting entire sectors and emerging as a critical threat in 2024 (Xygeni, 2024).

Understanding this convergence between geopolitics and cybersecurity is essential for anticipating risks and strengthening defense strategies.

2.2 Geopolitics and key actors

The global situation in the second semester of 2024 and its projection for 2025 are closely tied to geopolitics. In the global cyber threat landscape, it is crucial to analyze how these geopolitical tensions manifest into specific conflicts. This section presents a classification of the most relevant geopolitical conflicts and their implications in cyberspace.

- **Russia and Ukraine: Cyber Warfare as an extension of the armed conflict**

The conflict between **Russia and Ukraine** continues to be the primary stage for hybrid warfare, where cyberspace amplifies conventional military operations. Russia is particularly notable for its use of cyberspace as a complement to its military strategies, leveraging **Threat Actor groups** such as **Sandworm** and **Fancy Bear**, which have conducted attacks on Ukraine's energy and transportation infrastructure using cutting-edge technologies. These operations have impacted not only Ukraine but also European companies and governments (ENISA, 2024; CrowdStrike, 2024, Google Threat Analysis Group, 2024) .

Additionally, Ukraine has enhanced its offensive cyber capabilities with support from international allies. Malicious groups such as **IT Army of Ukraine** have launched distributed attacks against Russian systems. This demonstrates how cyberspace has evolved into a force multiplier in modern conflicts.

- **Iran and Saudi Arabia: Cyberattacks in the Gulf**

In the **Persian Gulf**, Iran has deployed malware to infiltrate Saudi Arabia's energy infrastructure, disrupting critical operations in the oil and gas industry. These attacks are characterized by their destructive potential, targeting both operational systems and critical data, demonstrating the **strategic use of cyberspace** as an extension of the **political and military conflict** in the region (CrowdStrike, 2024).

Regarding Saudi Arabia, the country has strengthened its cybersecurity infrastructure through global alliances and the enhancement of domestic capabilities. This effort aims to protect critical sectors from sophisticated cyber threats that impact both energy stability and the country's global reputation as a reliable resource provider (International Telecommunication Union, 2024).

This conflict highlights how cyberspace amplifies regional tensions and has the potential to destabilize key markets, such as the energy sector.

- **North Korea and South Korea: Finance and espionage**

North Korea maintains strategic ties with China to sustain its regime through cyberattacks. These include operations by the Threat Actor group **Lazarus**, which has been linked to attacks on cryptocurrency exchanges and banks worldwide, stealing large sums through sophisticated methods such as backdoor implants in software and targeted attacks on global financial networks. (JPCERT, 2024).

South Korea, on the other hand, has increased its cybersecurity investments, focusing on Artificial Intelligence (AI) technologies for early threat detection and mitigation. These strategies include the implementation of advanced surveillance tools and global cooperation with allies to counter cross-border cyber threats (LISA Institute, 2024).

- **Israel and Gaza: Cybersecurity operations in an asymmetric conflict**

The conflict between these two entities has intensified the use of cyberattacks. Iran-backed organizations, such as the Threat Actor group **APT33**, have conducted disinformation and sabotage campaigns targeting Israeli financial and government entities (MITRE ATT&CK, 2024). These campaigns aim to undermine Israel's internal stability by disrupting critical services and spreading propaganda. However, Israel's defensive capabilities have enabled both the protection of its infrastructure and the execution of counteroffensive operations to mitigate threats posed by these Threat Actors. These operations highlight the evolution of cyberattacks, which have become essential instruments in modern conflicts, impacting both the global economy and public perception worldwide.

- **US and China: Digital empire and cyber espionage**

This conflict represents the struggle for technological dominance within the G20, led by the U.S., against the rise of China, a key BRICS member that has intensified its cyber espionage operations. Threat Actor groups such as **APT41** have been actively engaged in intellectual property theft and infiltration of US telecommunications networks (CISA, 2024; Mandiant, 2024). In response, the U.S. has established advanced cyber defense capabilities, imposing sanctions on Chinese companies and collaborating with allies to counter these threats. Additionally, agencies such as CISA and NSA have led initiatives to detect and mitigate risks, including phishing campaigns and other cyberattacks (CrowdStrike, 2024; ENISA, 2024).

2.3 Impact on specific sectors

NTT DATA's Cyber Threat Intelligence Department has identified an evolution in the most affected sectors in the second half of 2024.

During the second semester of 2024, the most targeted sectors included professional services, government, and finance. However, the latest global threat analysis reveals a significant shift in the distribution of cyberattacks. (ENISA, 2024; Verizon DBIR, 2024; CrowdStrike, 2024)

This new attack distribution reflects the strong influence of geopolitical tensions, primarily targeting strategic sectors and economically significant or conflict-affected countries. However, the impact was not uniformly distributed, as some sectors experienced greater disruption than others:

- **Public Administration and Government**

With 1,876 recorded attacks, government agencies and public sector entities face constant cyber threats, often originating from nation-state Threat Actors seeking strategic advantages, or hacktivists driven by ideological motives. The vast volume of citizen data and the critical infrastructure managed by these organizations make them high-priority targets.

- **Education**

With 1,440 recorded attacks, educational institutions, particularly universities, are increasingly targeted due to their intellectual property, personal data, and operational vulnerabilities. Threat Actors often aim to disrupt operations or monetize stolen data on the dark web.

- **Financial Services**

The financial services sector, with 658 recorded attacks, consistently ranks among the most targeted industries due to its access to funds and sensitive customer data. In 2024, cybercriminals have employed sophisticated tactics and exploited multiple internal vulnerabilities.

- **Information Technology (IT)**

With 795 recorded attacks, this sector is a prime target for Threat Actors looking to exploit technological resources. In 2024, 22% of global data breaches in this industry were linked to malware and phishing attacks.

- **Energy**

Attacks on this sector primarily targeted Advanced Persistent Threats (APTs) against power grids and oil systems, reflecting a strategic approach driven by global geopolitical tensions.

Most affected sectors from July to December 2024

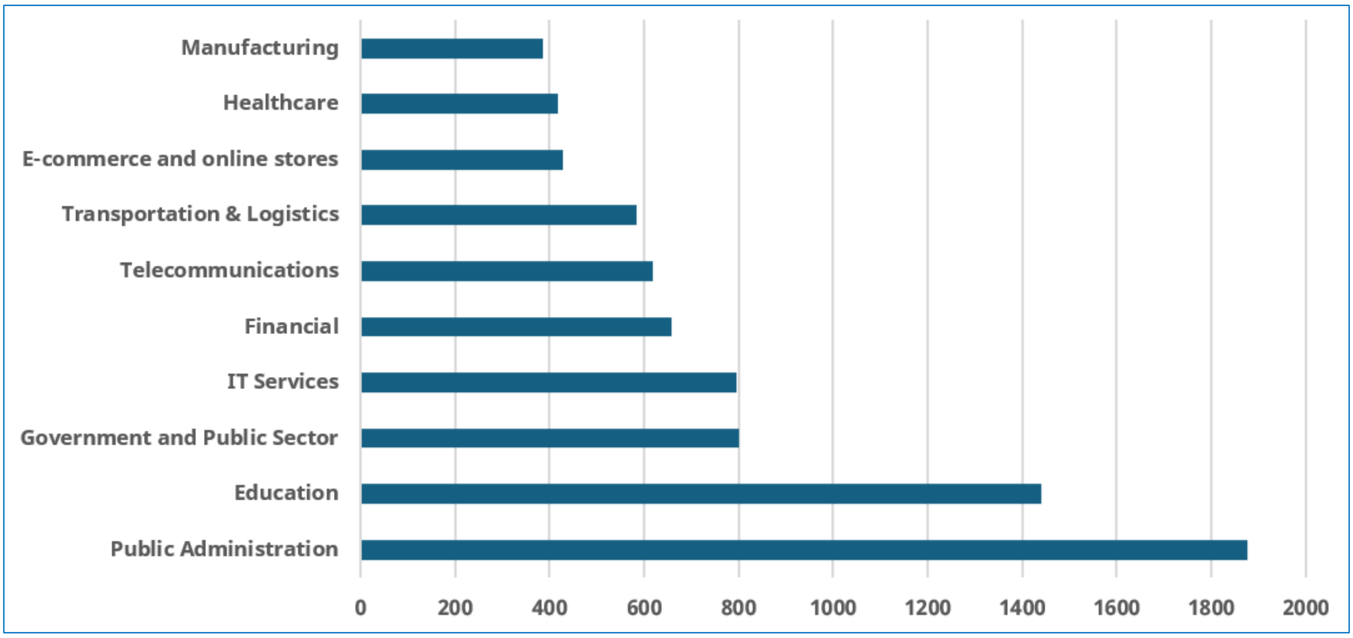


Table 1 | Most affected sectors by cyberattacks in the second semester of 2024.

Continuing with the impact distribution, not only is there a clear variation across sectors, but a marked trend can also be identified in specific countries that have experienced a higher volume of cyberattacks during this last semester of the year:

- **United States**

With 2,984 recorded attacks, the US tops the list of most affected countries, reflecting its strategic and economic significance.

- **India**

It recorded 2,069 attacks, driven by its rapid digitalization and technological expansion, with IoT and 5G being its critical vulnerability points.

- **Israel and Ukraine**

With 1,465 and 1,201 recorded attacks, respectively, both countries faced threats linked to regional conflicts, including cyber espionage and infrastructure sabotage.

- **Indonesia**

Among the 763 recorded attacks, the country experienced a significant cyberattack targeting its national data center, highlighting vulnerabilities in emerging economies.

Distribution of cyberattacks by country from July to December 2024

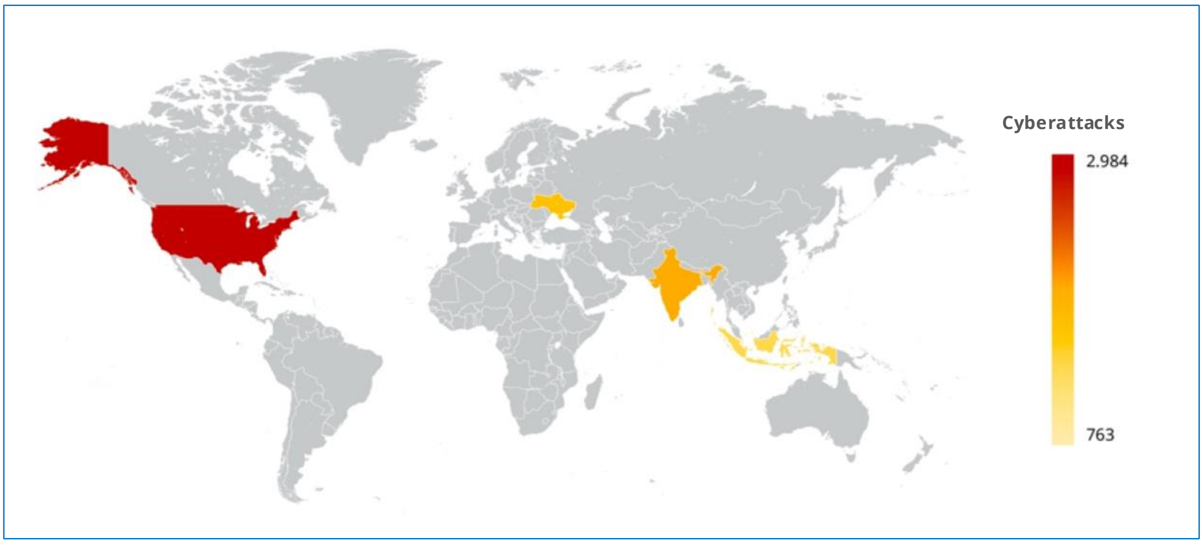


Figure 1 | Country-wise distribution of cyberattack impact in the second semester of 2024.

Major Global Threats

3. Major global threats

The cyber threats of the second semester of 2024 reflect a constantly evolving landscape, characterized by increasing sophistication and the interconnection of risks across multiple domains. Technological advancements, vulnerabilities in critical infrastructure, and challenges related to digital trust and identity have created a diverse and more complex threat environment, making it increasingly difficult to manage.

From the **Cyber Threat Intelligence department at NTT DATA**, we have analyzed these threats to identify key patterns, which have been classified into five thematic clusters: **Technology, Infrastructure, Identity & Trust, APTs, and Emerging Threats**. This categorization not only enhances a deeper understanding of current risks but also provides a strategic perspective to anticipate the trends shaping the cyber landscape in 2025.

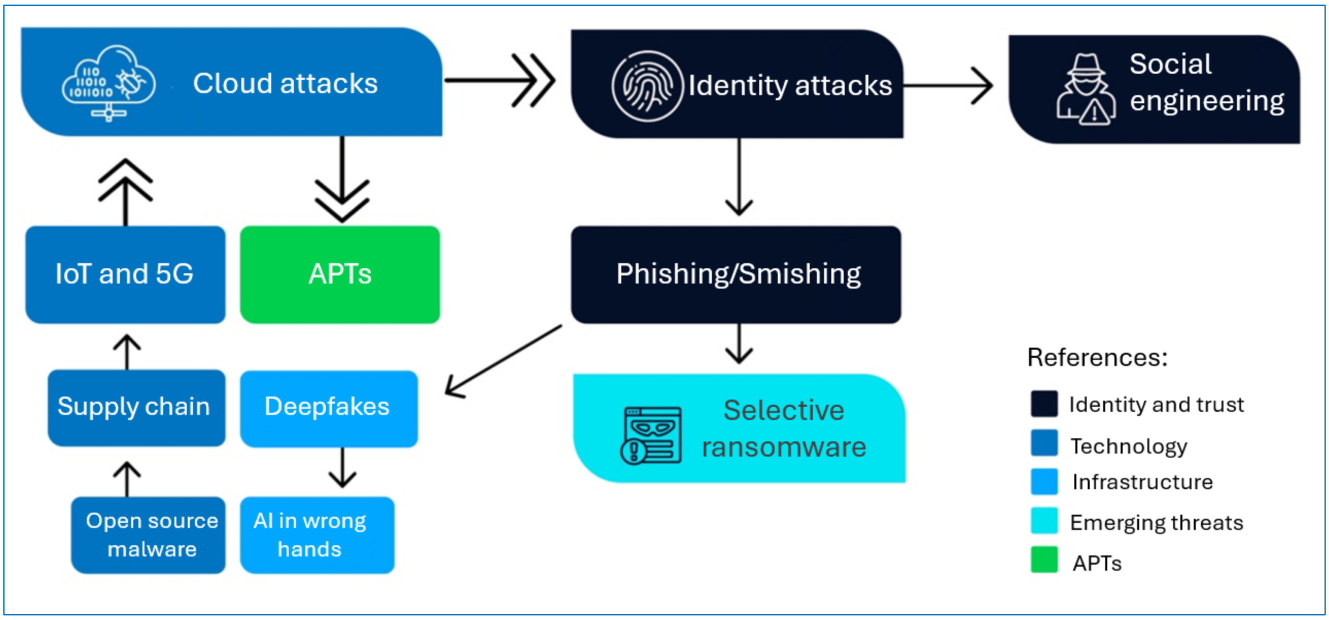


Figure 2| Diagram illustrating the connections between major cyber threats in 2024 and their organization into thematic clusters: Technology, Infrastructure, Identity & Trust, APTs, and Emerging Threats.

The second semester of 2024 reinforced the convergence of threats around advanced technologies, such as AI and IoT, alongside an increase in the use of social engineering tactics and supply chain vulnerabilities. This analysis underscores that, by 2025, focusing on the interconnection of these threats will be essential for managing an increasingly complex cyberspace.

3.1 Major cyber incidents and/or campaigns

The second semester of 2024 saw a significant increase in the number and scale of cyber incidents worldwide, surpassing the records from the first half of the year. This period was characterized by a rise in attack sophistication, the emergence of new malicious tactics and tools, and a widespread impact across key sectors, ranging from critical infrastructure to private enterprises and individual users.

The following events are chronologically organized to highlight their evolution and impact throughout the period:

Company, Technology, and/or Government Affected	Attacker	Affected Country	Attacker's Country	Incident Date	URL
Prudential Financial	Alphy Ransomware	USA	Unknown	07/01/2024	Source
CrowdStrike	Unknown	Global	Unknown	07/19/2024	Source
Critical Infrastructure, Government, Universities, IT Companies, and Hospitals	Earth Baku	Global	China	08/13/2024	Source
Internet Archive attack	Pro-Palestinian Hacktivists	Global	Unknown	09/04/2024	Source
American Water	Unknown	USA	Unknown	10/07/2024	Source
Schneider Electric	Hellcat	Global	Unknown	11/03/2024	Source
Nokia	IntelBroker	Global	Unknown	11/04/2024	Source
US Telecommunications Companies (Verizon & AT&T)	Salt Typhoon	USA	China	11/10/2024	Source
Equinox	LockBit	USA	Russia	11/20/2024	Source
Costa Rican Petroleum Refinery (RECOPE)	Unknown	Costa Rica	Presumably Russia	12/02/2024	Source
Public Administration and Critical Infrastructure	Storm-2077	USA	Presumably China	12/06/2024	Source

Table 2 | Major cybersecurity incidents in the second semester of 2024.

3.2 Emerging attack trends

As we approach 2025, the cybersecurity landscape is becoming increasingly complex and dynamic, driven by rapid technological advancements. Threat Actors are expanding their capabilities at an unprecedented pace, broadening the threat landscape and challenging organizations to anticipate and adapt to this constantly evolving environment.

3.2.1 AI-Generated attacks

In the coming year, cybercriminals are expected to continue rapidly adopting AI-based tools to enhance and streamline their operations across various attack lifecycle phases. The use of AI and Large Language Models (LLMs) is anticipated to persist in developing and scaling phishing, vishing, SMS-based scams, and other more sophisticated and persuasive social engineering attacks. Additionally, Threat Actors are expected to leverage deepfakes for identity theft, fraud, and bypassing Know Your Customer (KYC) security requirements. Furthermore, an increase in demand for LLMs without security restrictions is projected in underground forums, allowing malicious actors to explore illicit topics without ethical constraints. As AI capabilities continue to expand and become more accessible throughout 2025, organizations will face greater challenges in defending against these more frequent and effective attacks.

3.2.2 Ransomware attacks: Automation and strategic targets

Ransomware and data theft extortion are, and will continue to be in 2025, the most disruptive forms of cybercrime worldwide.

Their impact is not only measured by the volume of attacks, but also by the potential damage each incident can trigger. These operations are characterized by their ability to amplify damage far beyond the initial victim, creating cascading effects across communities and entire sectors.

In 2024, major ransomware attacks targeted the healthcare sector, negatively impacting patient care in hospitals, preventing access to medical prescriptions, and hindering doctors from conducting vital laboratory tests or billing insurance companies.

Ransomware and extortion operations in 2024 affected over 100 countries and all industries. The number of Dedicated Leak Sites (DLS) doubled in 2024 compared to 2023, and the emergence of multiple Ransomware-as-a-Service (RaaS) offerings highlights the thriving and prolific nature of the ransomware and extortion threat landscape.

3.2.3 Infostealer attacks: A Gateway to high-impact data breaches

Infostealers, while not a new threat, have evolved into an increasingly sophisticated and effective tool within the arsenal of Threat Actors. Throughout 2024, these tools were used to mass-harvest stolen credentials, enabling deep infiltrations into organizations and leading to high-impact intrusions.

The most alarming aspect is the ease with which these credentials are available on underground markets, allowing even low-skilled actors to execute effective cyberattacks, significantly amplifying their disruptive potential.

This trend is expected to continue in 2025, with infostealers remaining the primary vector for stolen credential acquisition.

Their impact will be particularly pronounced in environments lacking multi-factor authentication (MFA), leaving many organizations vulnerable to severe data breaches.

Additionally, infostealer malware has become more sophisticated in recent years, incorporating anti-evasion techniques and capabilities to bypass Endpoint Detection and Response (EDR) solutions, making them an even more formidable challenge in the evolving cyber threat landscape.

3.2.4 Commoditization of cyberattack tools

In 2025, organizations will continue to face a threat landscape where the barriers to entry for state-sponsored actors and less sophisticated cybercriminals will continue to decrease. The proliferation of attack tools, phishing kits, and "as-a-service" resources with advanced capabilities will enable low-skilled Threat Actors and new entrants to execute operations more efficiently and with greater proficiency.

This professionalization of cybercriminal services will broaden the threat landscape and complicate mitigation efforts. Additionally, the use of Generative Artificial Intelligence (AI) in various attack phases will increase the efficiency and adaptability of Threat Actors against current cybersecurity defenses.

3.3 Global statistics on security incidents, attack types, and involved Threat Actors

From the **Cyber Threat Intelligence Department at NTT DATA**, it was determined that during the first half of 2024, cyberattacks increased both in volume and scope, with a significant surge in ransomware activity. Although **defensive measures have improved in mitigating ransom payments**, **the number of confirmed ransom payments continues to rise**, driven by the growing frequency and scale of cyberattacks. This trend has exerted additional pressure on global cybersecurity costs, maintaining the economic and operational impact at critical levels **(CTI Trends Report, First Half of 2024 - NTT DATA, 2024).**

During the second half of the year, the **proliferation of Ransomware-as-a-Service** (RaaS) **offerings and supply chain attacks led to a 39% increase** in reported incidents. **Sectors such as healthcare, education, government, SMEs, and finance** were among the most impacted (Acronis, 2024; IOCTA - Europol; 2024; ENISA, 2024).

Among the key statistics and trends observed during the second half of 2024, we can identify:

- **Dark Web activity**

During the second half of 2024, approximately 2,126 Threat Actors were active on the Dark Web, collectively generating around 18,537 posts. These activities were primarily focused on the sale of compromised data and unauthorized access credentials, highlighting the expanding threat landscape within underground forums.

- **Ransomware**

The United States remained the primary target for ransomware attacks, accounting for 54.12% of all recorded incidents worldwide. During the second half of 2024, ransomware attacks surged by 15% in July and an additional 18% in September, solidifying ransomware as the dominant cyber threat. Additionally, the manufacturing sector was particularly affected, concentrating 18.26% of all ransomware activity.

- **Top ransomware groups**

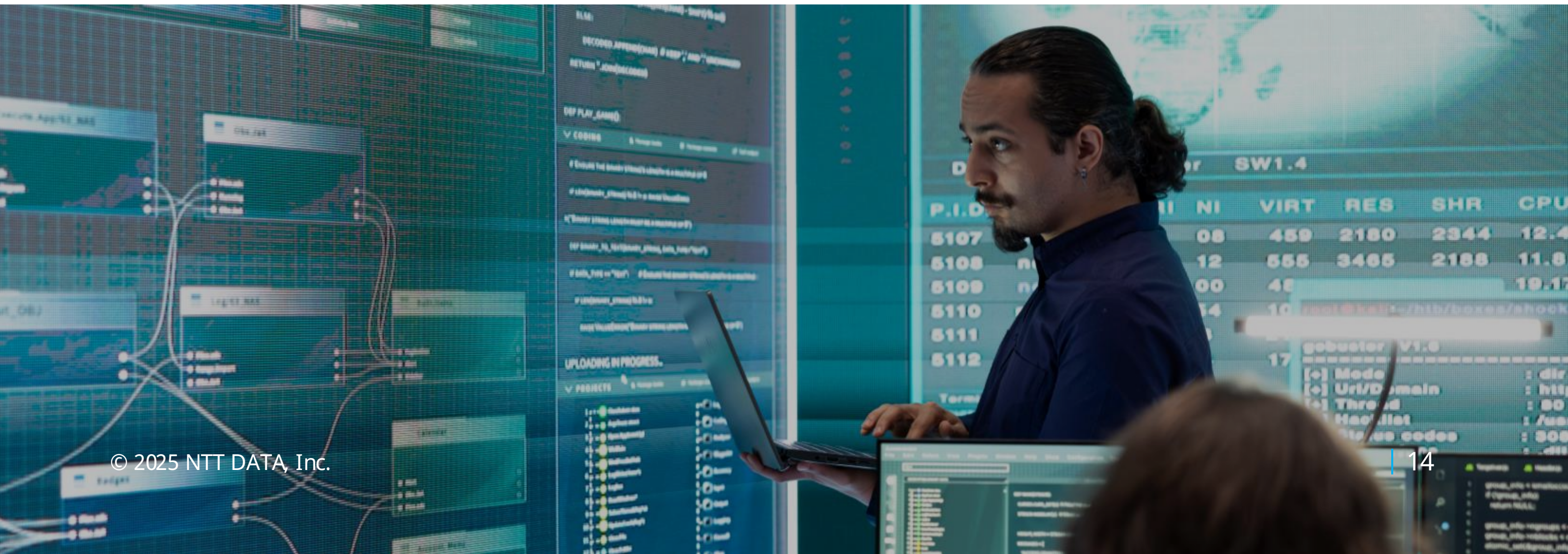
The key ransomware threat groups that dominated the 2024 landscape were **RansomHub (9.45%)**, **Play Ransomware Group (6.91%)**, and **Lockbit (6.96%)**. These threat groups exploited vulnerabilities in critical sectors, causing widespread damage.

- **Phishing attacks**

The United States experienced the highest proportion of phishing attacks worldwide, accounting for 34.89%, followed by Singapore (15.89%) and the United Kingdom (3.06%). These statistics highlight the regional concentration of phishing campaigns. Phishing attacks increased by 12% in August but stabilized in October, particularly targeting the banking and healthcare sectors.

- **Denial of Service (DoS)**

Increased by 20% between September and October, particularly impacting public administrations.



Estimated percentage increase in attacks by category for the second half of 2024.

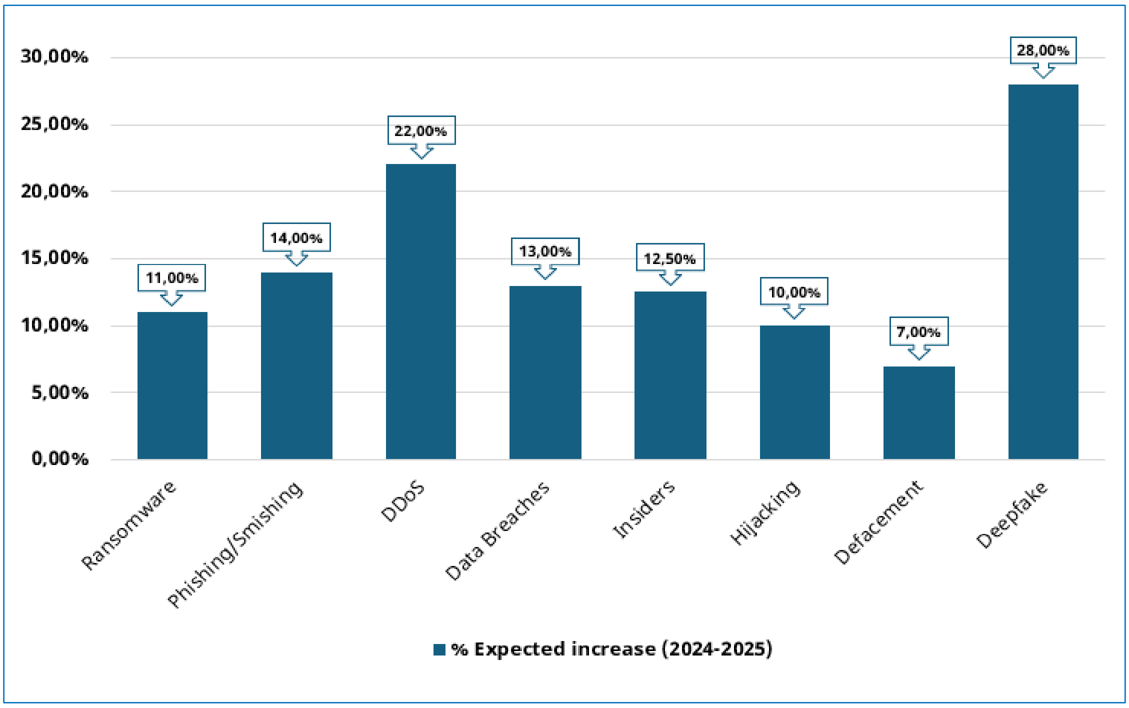


Figure 3 | Percentage increase in the number of attacks by category compared to the first half of 2024.

- The percentage increase during the second half of 2024 highlights the operational intensification of Threat Actors and the diversification of their objectives.

- The increase in ransomware, phishing, and deepfakes indicates a stronger focus on methods that combine mass reach with direct economic impact.

- On the other hand, the increase in DoS attacks and data breaches demonstrates a systematic focus on disrupting critical services and compromising sensitive information.

- The most impacted sectors are healthcare, manufacturing, and financial services, where structural weaknesses and the need for interconnected devices amplify the impact of these incidents.

- The increase in the frequency and complexity of cyberattacks presents significant challenges in mitigation costs. This scenario pressures organizations to invest in more robust cybersecurity solutions, which is expected to **increase annual cybersecurity budgets by 20% to 30% by 2025.**

(Cybersecurity Magazine, 2024; Kaspersky, 2024; Silicon Week, 2024; T21, 2024).

3.4 Costs of cyberattacks for businesses

Since the beginning of 2024, cybersecurity-related costs have seen an estimated **35% increase**, with projections reaching up to **40%** during critical campaigns such as the **holiday season**. This increase reflects not only **the higher volume of cyberattacks** but also the **financial impact** of maintaining **resilience** against emerging attack vectors. For example, the adoption of **emerging technologies** in business environments, such as the **Metaverse** and the integration of **OT and IoT systems**, has led to a **40% rise in containment costs** for companies implementing these tools, compared to those that do not (Gartner, 2024; IT User Cybersecurity, 2024; WEForum, 2024).

In this context, the economic impact of cyberattacks follows a pattern of sustained growth, also accumulating the effects of global events such as the digital acceleration during the pandemic, the rise of new technologies, and the evolution of cyber threats.

Therefore, by analyzing the growth from **2020** to the **last semester of 2024**, we can understand how certain events and technologies have led to a **gradual increase in sanctions**, **ransom payments**, **business disruptions**, and **cybersecurity reinforcement efforts.**

This historical perspective not only allows us to visualize clear trends but also provides a solid foundation for assessing the challenges of 2024, a year marked by the consolidation of emerging attack vectors and the increasing financial impact associated with them.

Annual evolution of estimated cybersecurity costs from 2020 to 2024.

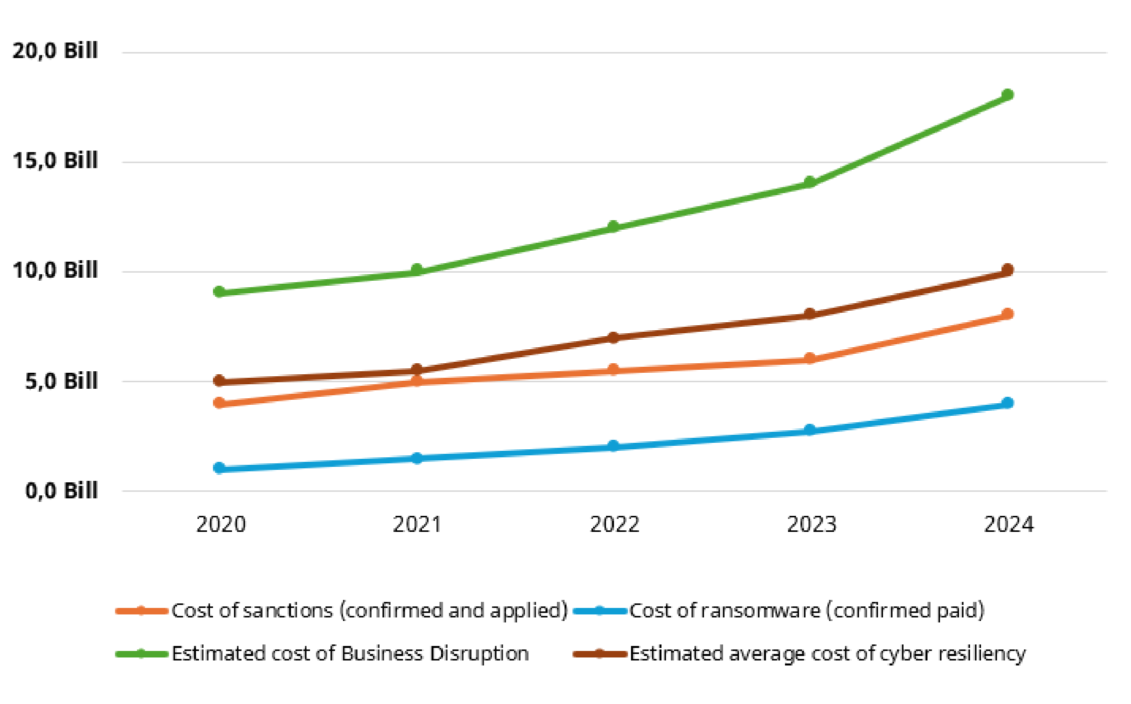


Figure 4 | Comparative annual evolution of estimated cybersecurity costs (2024-2024) breakdown by sanctions, ransoms, business disruptions, and cybersecurity reinforcement.

Legal Framework and Cybersecurity Arrests

4. Legal framework and cybersecurity arrests

From the **Cyber Threat Intelligence Department at NTT DATA,** it is considered essential to analyze the security measures implemented, the laws passed within the realm of cybersecurity, and the arrests made by law enforcement agencies worldwide in the second half of 2024.

This analysis evaluates the commitment of countries to regulating and controlling current and emerging technologies, as well as their responsible application. Furthermore, it reflects the joint efforts of legislative, judicial, and defense bodies to address corporate security breaches and combat illegal activities in cyberspace.

4.1 Key cybersecurity laws

Regarding **Applicable Cybersecurity Legislation**, there has been a global escalation in the creation of **laws, regulations, directives**, and **applicable legislation**, primarily focused on the regulation of current technologies, with some interest in regulating the use of other emerging technologies that are gaining significant presence in the market.

In this context, the **growing need for cybersecurity legislation** and regulation of emerging technologies is evident. This is reflected in the steady increase in the number of legal documents that have been passed globally since 2020, with an upward trend (ITU, 2024; WE Forum, 2024; Enisa, 2024):

Annual evolution of total cybersecurity laws passed (2020 – 2024)

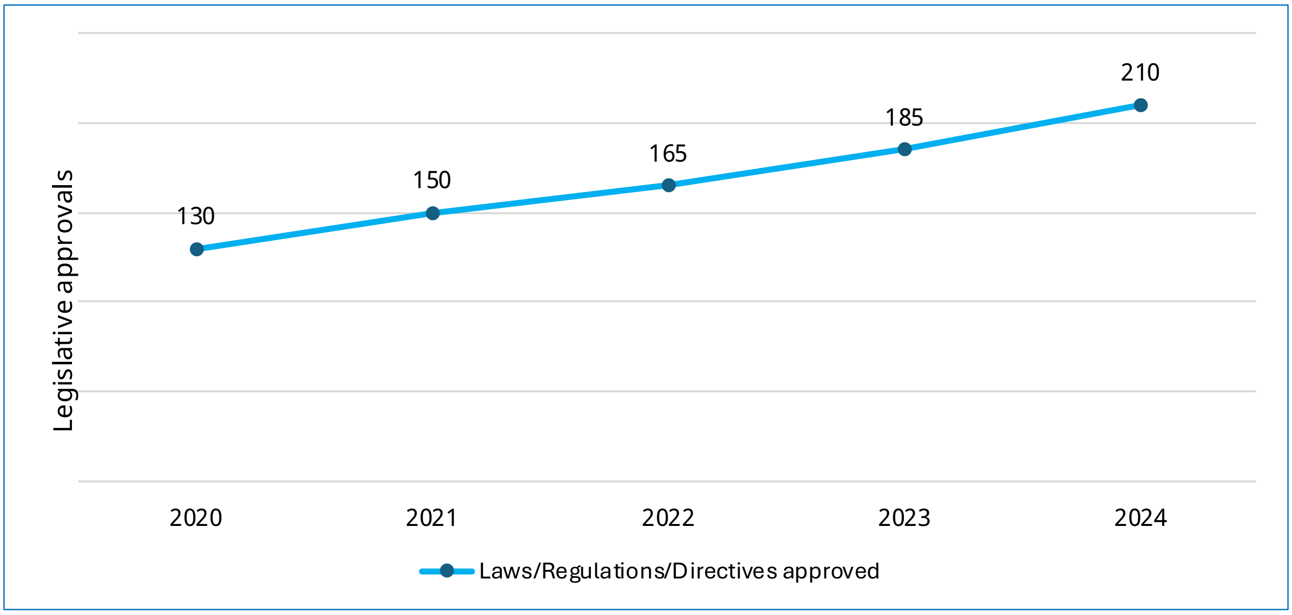


Figure 5 | Trend of law approvals since 2020 and estimation for 2025.

Regarding the approval of legislation in the second half of 2024, the following legal documents were approved, including:

Continent	Law	Institution	Reference
Asia	Cybersecurity Master Plan for Operational Technology	Singapore Government	CSA
Europe*	Network and Information Security Directive 2 (NIS2)	European Union	European Parliament
	Digital Operational Resilience Regulation (DORA)	European Union	EIOPA
Oceania	Cyber Security Bill	Australian Government	Australian Parliament

** In the context of European legislation, two key aspects stand out: On one hand, the **NIS2 Directive** has begun to be directly implemented after the transposition deadline was surpassed, even in countries like Spain that have not completed this process. On the other hand, while the **DORA Regulation** was not applicable during the second half of 2024, it came into effect on January 17, 2025, with a significant impact not only on financial entities but also on IT service providers that support them.*

Table 3 | Laws approved in the second semester of 2024.

4.2 Key arrests in the field of cybersecurity

The second half of 2024 has been a period of activity for both cybercriminal organizations and law enforcement agencies worldwide. This period has been marked by several arrests and dismantling of some of the most active and dangerous cybercriminal groups responsible for a high incidence of attacks in previous months. According to gathered data, international law enforcement interventions have shown a significant increase in both frequency and scope (Europol, 2024; Interpol, 2024).

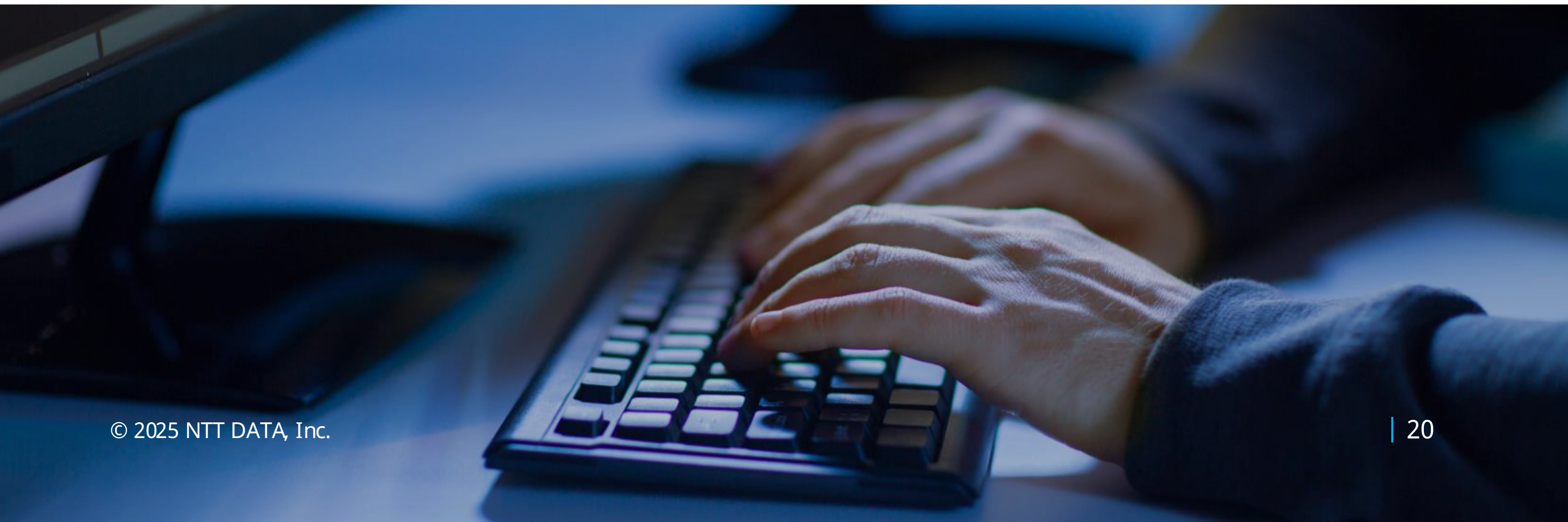
In the case of **LockBit, Operation Cronos**, led by the UK's National Crime Agency (NCA) in collaboration with the FBI, Europol, and the Spanish Civil Guard, dismantled a significant portion of the group's infrastructure through key arrests, including the capture of a primary operator in Spain. This operation, with its final phase carried out in October 2024, significantly weakened global ransomware attacks (Ministerio del Interior, 2024).

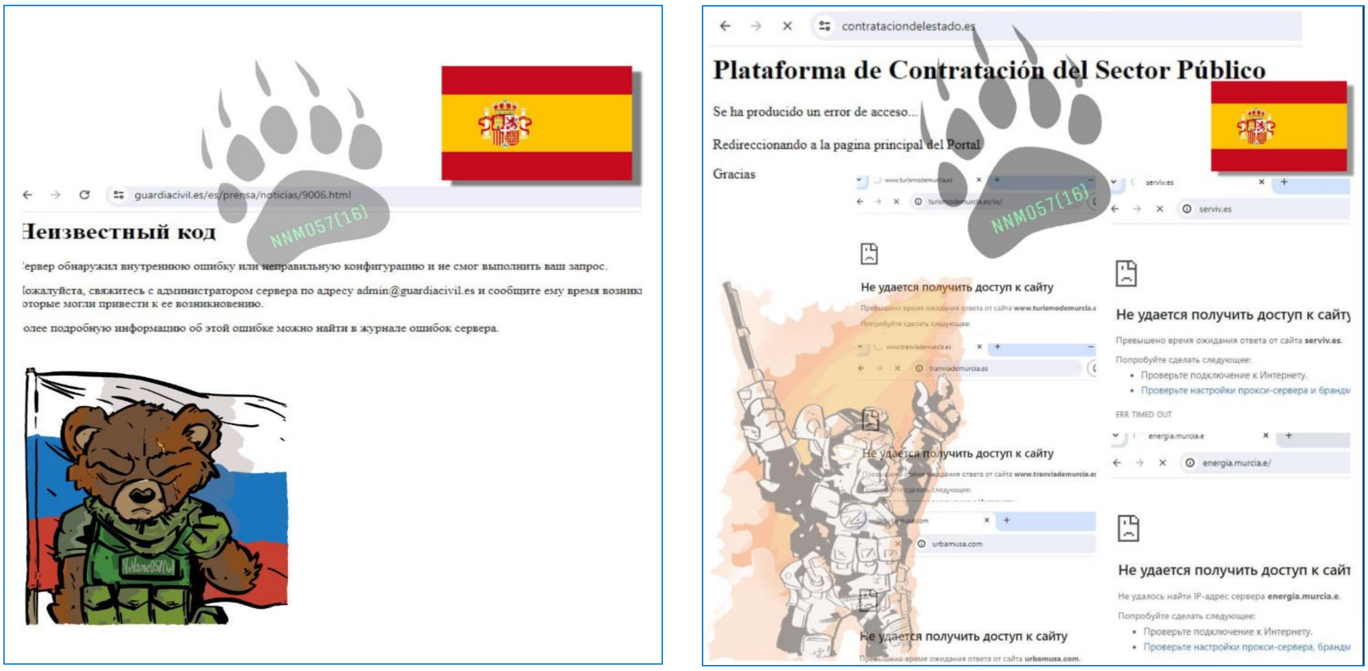
Operation	Threat Actor group	Law Enforcement and Security Forces	References
CRONOS	LockBit	NCA (United Kingdom) FBI (USA) Europol Civil Guard (Spain) Eurojust Local Agencies of Poland and Ukraine	Europol Cybercrime Operations Interpol Europol Europol Europol
Operation Synergy II	Various (Europe, South Sudan, Zimbabwe)	Europol Interpol Local Agencies of several countries	Interpol
Unnamed	NoName057(16)	Civil Guard (Spain) Interpol Europol	INCIBE

Table 4 | Main cybercrime gang takedown operations carried out in 2024.

Despite these successes, there is a "dark side" to these interventions. A clear example is the reaction following the arrest of three members of the Russian hacktivist group **Noname057(16)** in Spain, as part of a joint operation between the Civil Guard, Interpol, and Europol. Although this action weakened their activities to some extent, the group issued public threats via their **Telegram** channel and soon after launched DDoS attacks aimed at government websites and critical services in Spain, causing significant disruptions.

These reprisals highlight how arrests can, in some cases, trigger an escalation in cybercriminal activities. This underscores the importance of not only successfully carrying out these operations but also preparing robust cyber defenses to mitigate the potential consequences.





guardiacivil.es/es/prensa/noticias/9006.html

Неизвестный код

Сервер обнаружил внутреннюю ошибку или неправильную конфигурацию и не смог выполнить ваш запрос.

Пожалуйста, свяжитесь с администратором сервера по адресу admin@guardiacivil.es и сообщите ему время возник которые могли привести к ее возникновению.

Более подробную информацию об этой ошибке можно найти в журнале ошибок сервера.

contrataciondelestado.es

Plataforma de Contratación del Sector Público

Se ha producido un error de acceso...

Redireccionando a la pagina principal del Portal

Gracias

www.turismodemurcia.es

turismodemurcia.es/es/

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта www.turismodemurcia.

Попробуйте сделать следующее:

www.tranviademurcia.es

tranviademurcia.es

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта www.tranviademurcia.es

Попробуйте сделать следующее:

urbamusa.com

urbamusa.com

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта urbamusa.com.

serviv.es

serviv.es

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта serviv.es.

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера и бранд

ERR TIMED OUT

energia.murcia.e

energia.murcia.e/

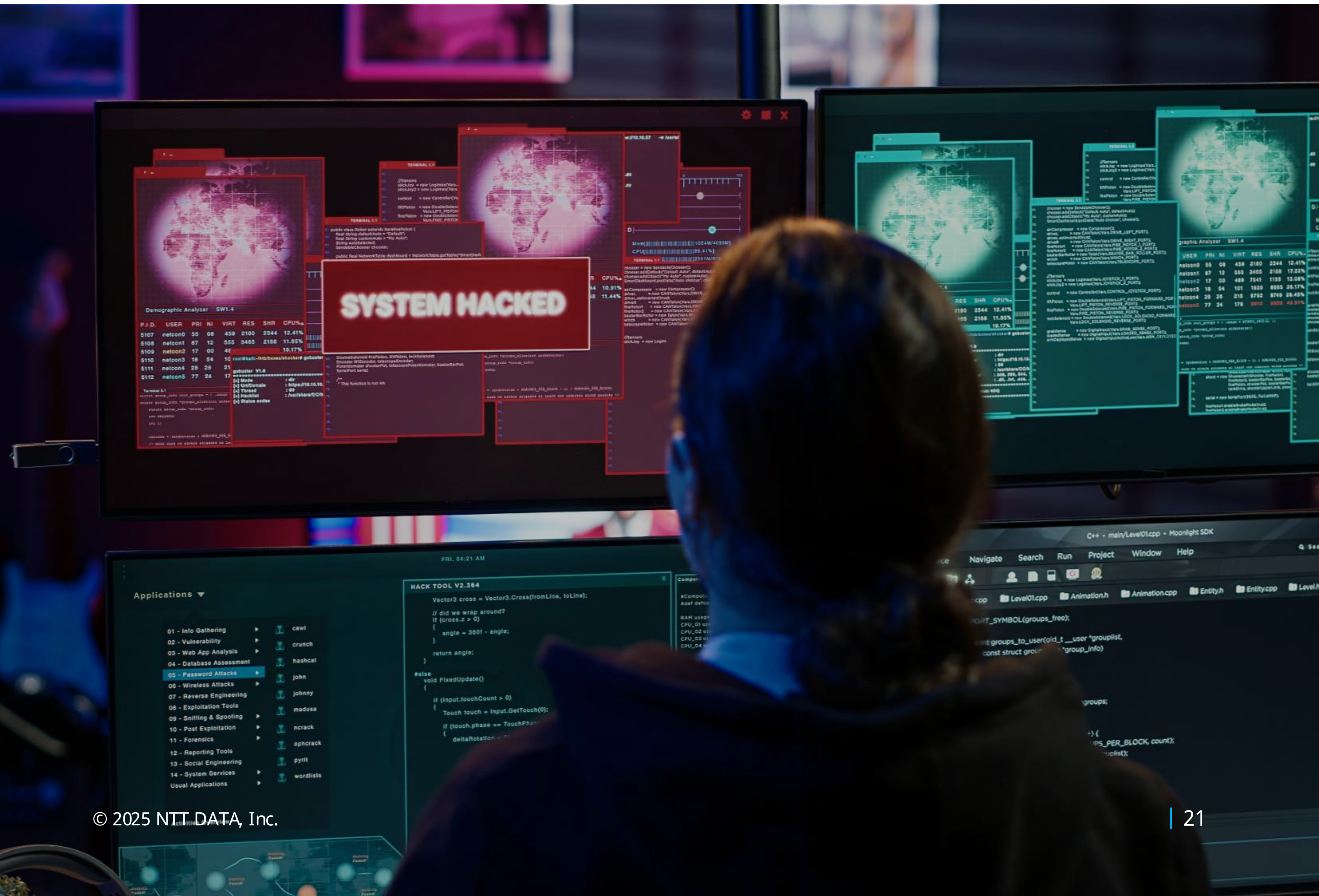
Не удается получить доступ к сайт

Не удалось найти IP-адрес сервера energia.murcia.e.

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера, бранд

Illustrations 1 and 2 | Messages from the Telegram channel of the NoName057(16) group about their successful attacks on Spanish websites.



Dark Web Insights

5. Dark Web Insights

In the second half of 2024, numerous activities took place on the Dark Web, highlighting its role as a hub for cybercriminal activity. In total, **NTT DATA's Cyber Threat Intelligence Department detected more tan 10,352 incidents** on the Dark Web, ranging from large-scale data breaches to the sale of information.

During the second half of 2024, following revelations related to data breaches (44.59%), it was identified that the second most common category of posts on the Dark Web, according to the analysis conducted by **NTT DATA**, consisted of advertisements related to the sale (41.15%), promotion, and distribution of malware. This environment shows a constant emergence of new strains of malware, which can be sold at fixed prices or auctioned to the highest bidder, or distributed for free as open-source tools, available to any malicious actor.

The third most prominent category of posts on the Dark Web, according to **NTT DATA**, is related to access to services (12.62%). This type of content includes the sale or direct exchange of access to compromised systems, networks, or databases, enabling their exploitation by other malicious actors. The presence of such posts is particularly alarming given their potential to amplify cyber threats and further facilitate malicious activities.

At the bottom of the list are posts regarding new partnerships or cooperation between malicious actors (1.17%), the purchase of information (0.41%), and those that disclose the target of the attack (0.06%).

Main publications on the Dark Web

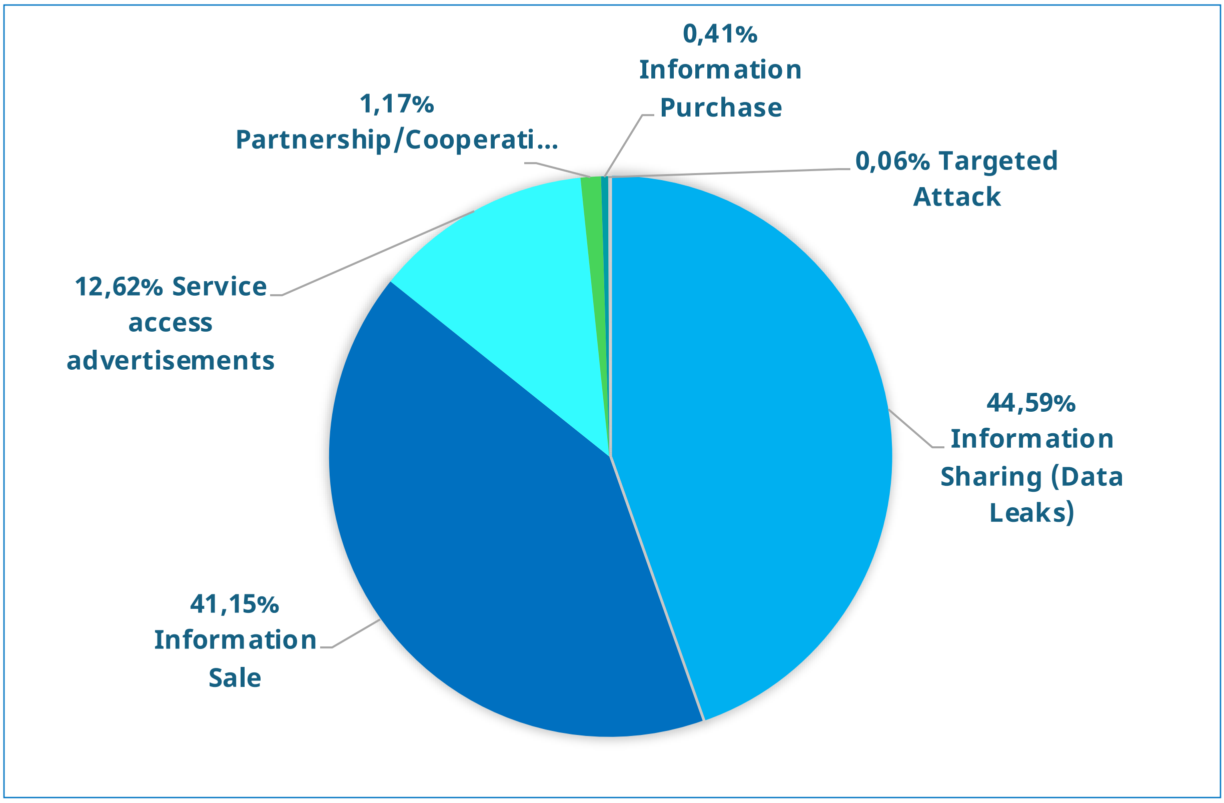


Figure 6 | Main categories of publications on the Dark Web in the second half of 2024.

During the evaluated semester, underground forums have continued to play a critical role as operation centers for cybercriminals, facilitating the purchase, sale, and coordination of resources for cyberattacks. In this context, **Breach Forums** stood out significantly, recording over 2,000 associated incidents. It was followed by **Exploit Forum**, with 500 incidents, and **Xss Forum**, with 300 incidents.

These platforms not only provide access credentials but also offer a variety of tools and services necessary for carrying out effective cyberattacks. This environment has given rise to a flourishing market that facilitates cybercrime in a coordinated manner, presenting a significant challenge for cybersecurity.

Underground sales platforms

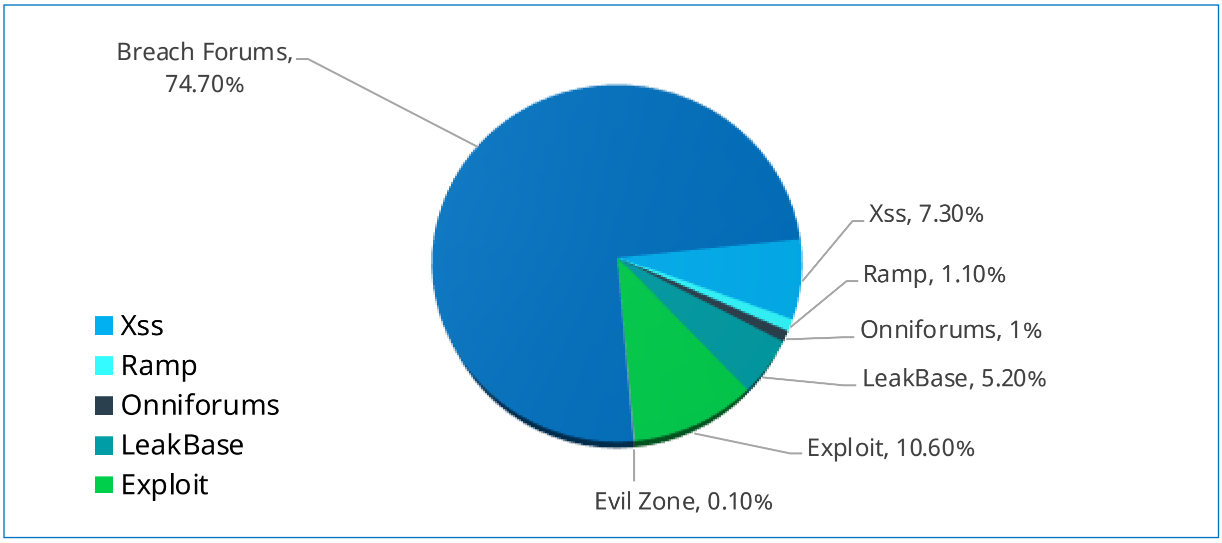


Figure 7 | Main underground selling platforms identified in the second half of 2024.

Malicious actors often begin their operations by infiltrating the systems of external providers, thereby gaining access to the target organization’s infrastructure and sensitive data. Notable examples of this tactic include significant data breaches that occurred in 2024, such as the case where attackers accessed **Ticketmaster's Snowflake** cloud account through external contractors.

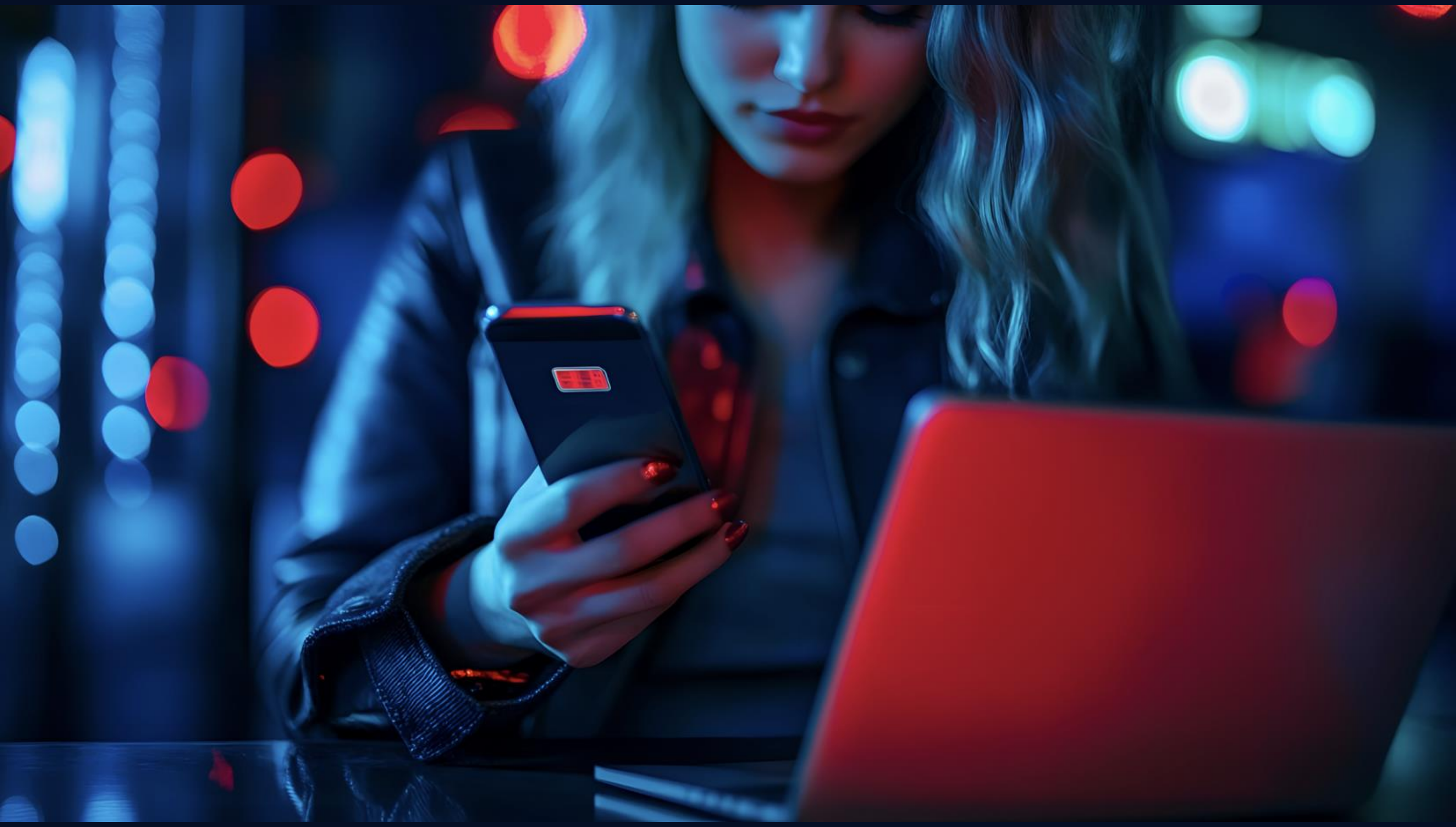
Another prominent malicious actor during this period was **IntelBroker**, which employed similar methodologies to infiltrate major corporate entities, including Nokia, Ford, and multiple Cisco clients, among which is **Microsoft**.

On the other hand, in 2024, there has been a notable increase in cybercriminal activities on the **Telegram** platform. However, it is projected that the underground community could migrate back to **the Dark Web forums**, partly due to the strict bans imposed on **Telegram** by its administrators. This migration will likely intensify competition among **Dark Web forums**. To attract new users and differentiate themselves, forum operators may implement innovations .such as **automated escrow services, more efficient dispute resolution processes, and improvements in security and anonymity**, setting a new standard in the underground market.

Continuous monitoring of these forums is essential for organizations to maintain a proactive stance against emerging threats. This active surveillance is crucial for preventing incidents before they occur, thereby strengthening defense strategies and risk mitigation in the cybersecurity landscape.

Threat Actors

Threat Actors



In 2024, the cyber landscape has been marked by a complex network of malicious actors who have stood out not only for the volume of their attacks but also for their innovative tactics and global impact. This report identifies the key actors of the year, providing a strategic overview of their methods, motivations, and recent attacks to help organizations strengthen their defenses against these threats.

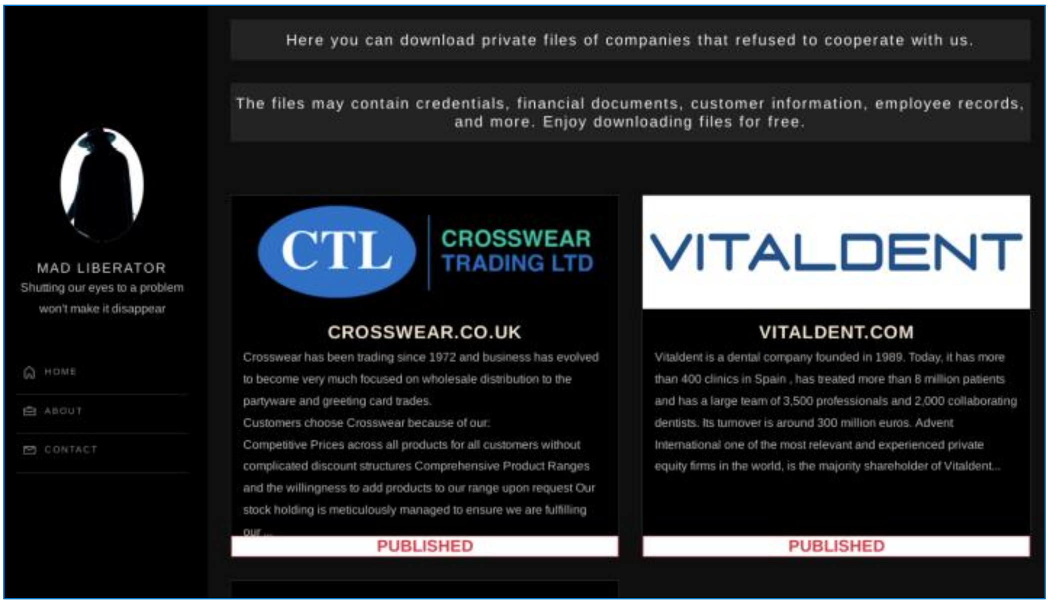
The Cyber Threat Intelligence team at NTT DATA analyzed incidents, industry reports, and activities on the Dark Web to identify new and most critical malicious groups.

6.1 Emerging Threat Actors

• Mad Liberator Blog

Mad Liberator Blog is a **Dark Web extortion blog**, classified as a "name-and-shame" site, allegedly operated by the **Mad Liberator Ransomware Group**. First reported on July 12, 2024, in open sources, the blog has already listed **nine victims** from various industries globally. The site, written entirely in English, is only accessible through the Tor browser.

According to information published by the malicious actors, the group is composed of hackers from various parts of the world and does not identify as an APT or a hacktivist group with political motivations. Their extortion strategy is straightforward: they threaten companies with listing their name on the blog if they do not respond within a day. They then provide a seven-day deadline before publishing the stolen files, and if the ransom is not paid within five days, they promise to release all the company's information.



Here you can download private files of companies that refused to cooperate with us.

The files may contain credentials, financial documents, customer information, employee records, and more. Enjoy downloading files for free.

MAD LIBERATOR
Shutting our eyes to a problem won't make it disappear

CROSSWEAR.CO.UK

Crosswear has been trading since 1972 and business has evolved to become very much focused on wholesale distribution to the partyware and greeting card trades.
Customers choose Crosswear because of our:
Competitive Prices across all products for all customers without complicated discount structures Comprehensive Product Ranges and the willingness to add products to our range upon request Our stock holding is meticulously managed to ensure we are fulfilling our ...

VITALDENT.COM

Vitaldent is a dental company founded in 1989. Today, it has more than 400 clinics in Spain , has treated more than 8 million patients and has a large team of 3,500 professionals and 2,000 collaborating dentists. Its turnover is around 300 million euros. Advent International one of the most relevant and experienced private equity firms in the world, is the majority shareholder of Vitaldent...

Illustration 3 | Mad Liberator blog post.

• Helldown Blog

In August 2024, the **Helldown Blog** was launched, an extortion website accessible via Tor, allegedly operated by the **Helldown Ransomware** Group. This blog became a key tool for their ransomware activities, focusing on extortion and the publication of stolen data.

Between August 5 and August 22, the malicious group posted information on 22 victims, spread across countries such as United States, United Kingdom, Poland, Italy, Austria, Switzerland, and Lebanon. The affected companies were from sectors including Information Technology (IT), construction, manufacturing, real estate, and logistics.

The Helldown Ransomware operators used **Tox**, an encrypted communication platform, to coordinate negotiations and manage their illicit activities, highlighting their sophisticated approach to anonymization and evading digital traces.

• Valencia Blog

In September 2024, **Insikt Group** observed a new extortion website allegedly operated by the **Valencia Ransomware Group**. The extortion website was active for a brief period at the end of September 2024 and no longer exists. The malicious actors listed their Tox ID on the extortion blog as the primary method of communication.

Before disconnecting, the extortion blog listed four victims:

- **Grupo Cortefiel:** A Spanish company operating in the retail and textile sectors.
- **Duopharma Biotech:** A Malaysian company operating in the manufacturing and pharmaceutical industries.
- **Satia Industries Ltd:** An Indian company operating in the manufacturing industry.
- **Globe Pharmaceuticals Ltd:** A Bangladeshi company operating in the healthcare sector.

The ransomware group used a now-deleted social media account on the X platform (@valenciaLeaks72).

• HellCat Blog (HellCat Ransomware)

HellCat Blog is an extortion blog on the Dark Web, written in English and operated by **the Hellcat Ransomware Group,** which has been active since October 2024. As of the time of writing this article, the extortion blog had three victims:

- **College of Business Education:** A higher education institution dedicated to providing education in business, accounting, procurement, and related fields in Tanzania.
- **Ministry of Education of Jordan:** The government authority responsible for overseeing and managing the education system in Jordan.
- **Schneider Electric:** A multinational company headquartered in France, specializing in energy management and automation solutions.

6.2 Ransomware groups

From the **Cyber Threat Intelligence Department at NTT DATA**, a comprehensive analysis was conducted on ransomware activities during the second half of 2024, highlighting a significant increase in these attacks led by groups such as **LockBit** and **RansomHub**. This analysis also examines the sectoral impacts, such as in education, government, and energy, showing notable increases in attacks.

In addition, the evolution of key ransomware malicious groups such as **Black Basta**, **Play**, and emerging threats like **Valencia Ransomware** and **MAD LIBERATOR** is analyzed, highlighting the increasing complexity and global reach of ransomware operations.

Below is a chart displaying the 6 most active ransomware groups during this period, illustrating their distribution and emphasizing the prominence of **RansomHub** in the threat landscape.

Main ransomware groups

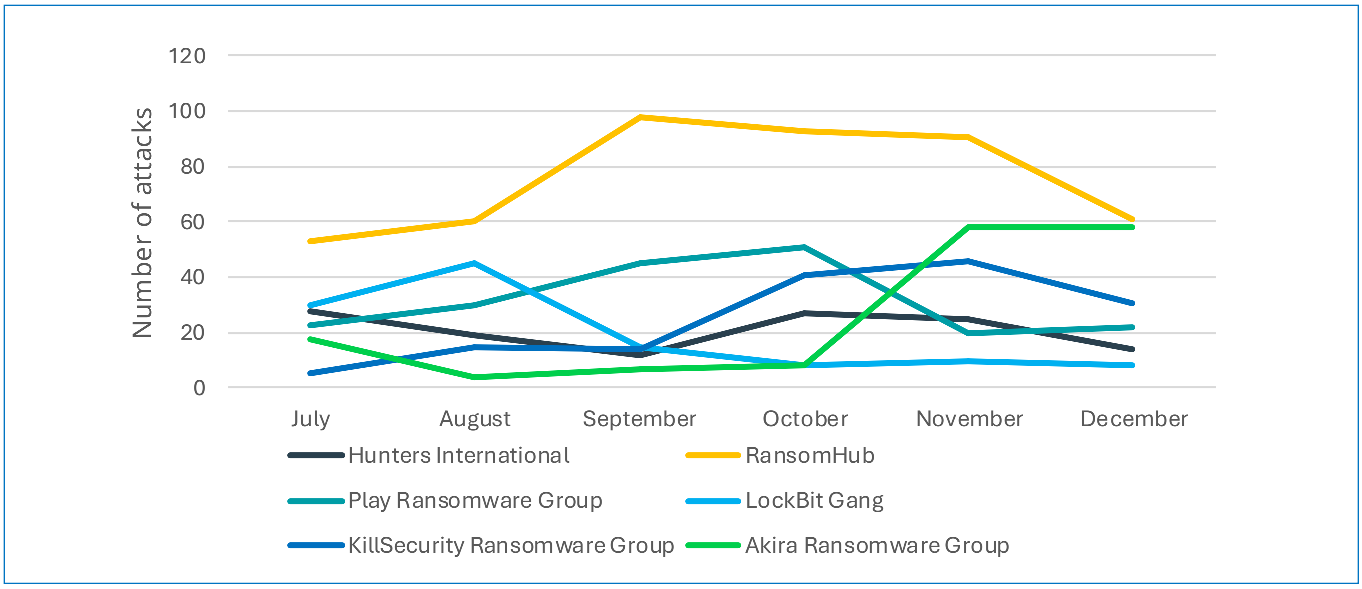


Figure 8 | Activity in the second half of 2024 by the 6 most active ransomware groups.

- **RansomHub**

First detected in February 2024, **RansomHub** has quickly gained prominence in the ransomware landscape, capitalizing on the disruption of major players like ALPHV and LockBit. Likely rooted in Russia and with connections to former ALPHV affiliates, the group has established itself as a formidable force by leveraging its Ransomware-as-a-Service (RaaS) model, offering attractive profit-sharing terms to affiliates.

This approach has led to an increase in attacks, particularly in August and September 2024, when more than half of their attacks occurred. An interesting fact is that **the attack count for these two months represents more than 10% of all ransomware attacks we have analyzed during this semester.**

- **PLAY *Ransomware***

PLAY ransomware has been responsible for numerous destructive attacks against major U.S. municipalities and is believed to have successfully carried out over 560 attacks since June 2022. Multiple researchers have discovered a Linux variant of Play ransomware that only encrypts files when executed in a VMWare ESXi environment, which helps expand their operations. Finally, **Play has set a new record for annual victims in 2024, with a total of 364 victims.**

• Akira

Active since March 2023, Akira has gained notoriety for its technical adaptability, becoming the third largest contributor, **claiming responsibility for 153 victims during the last half of 2024.** In the months of November and December, this group reached a significant operational peak, recording a total number of victims that exceeds more than three times the usual monthly average. This increase not only underscores the growth of their activity but also solidifies Akira's position as one of the most active ransomware actors today.

Over the past six months, ransomware attacks have affected organizations in every part of the world, but some countries have suffered a disproportionate impact. The **United States tops the list of the most affected countries** by a wide margin, solidifying its position as the primary target of ransomware actors.

This trend can be attributed to the high concentration of technologically advanced companies, critical infrastructures, and systems with highly valuable data, which attract cybercriminals. The following chart illustrates the distribution of the most affected countries by this type of attack during the second half of 2024:

Countries most affected by ransomware from July to December 2024

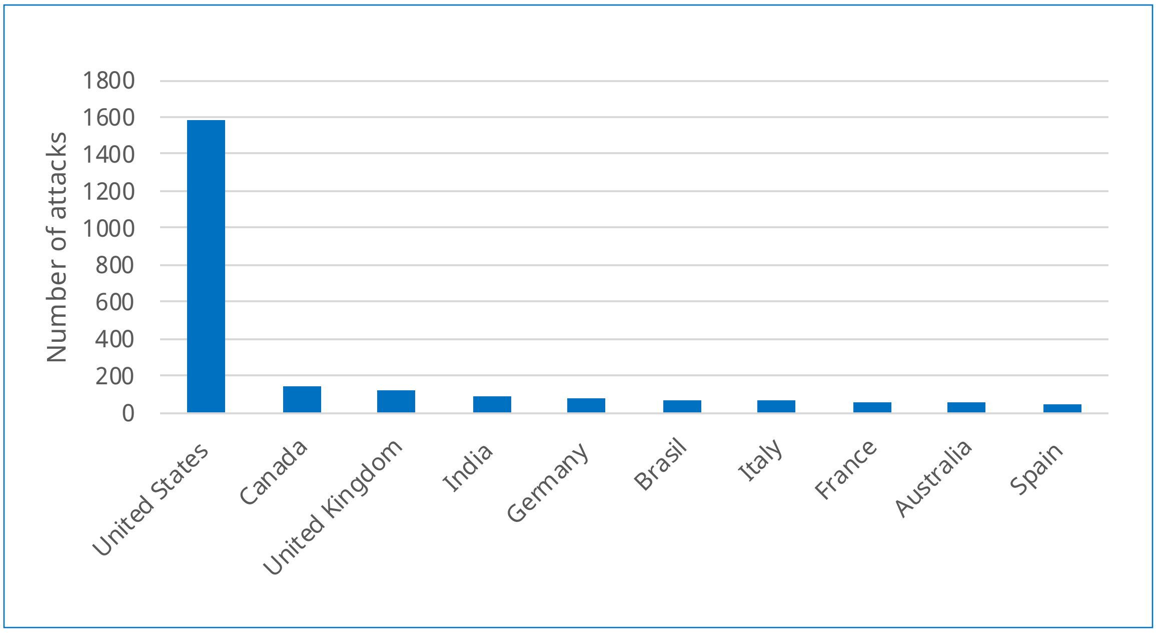


Figure 9 | Countries most affected by ransomware in the second half of 2024.

In the analysis of the sectors most affected by ransomware attacks over the past six months, **the manufacturing sector stands out as the primary target of cybercriminals**. This sector has experienced a significantly higher volume of attacks compared to others, reflecting its vulnerability due to heavy reliance on critical operating systems and the potential disruption of global supply chains.

Ransomware actors appear to prioritize this sector due to the financial and operational impact their attacks can generate, increasing the pressure on organizations to comply with their demands. The following chart illustrates the most affected sectors, highlighting the prominence of the manufacturing sector during this period:

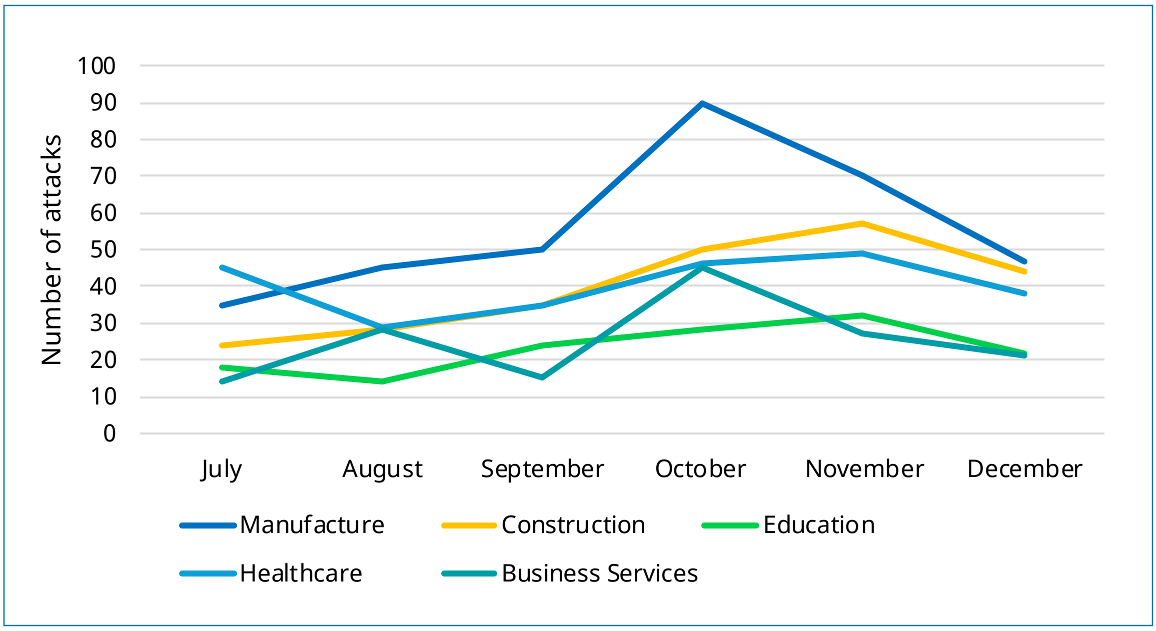


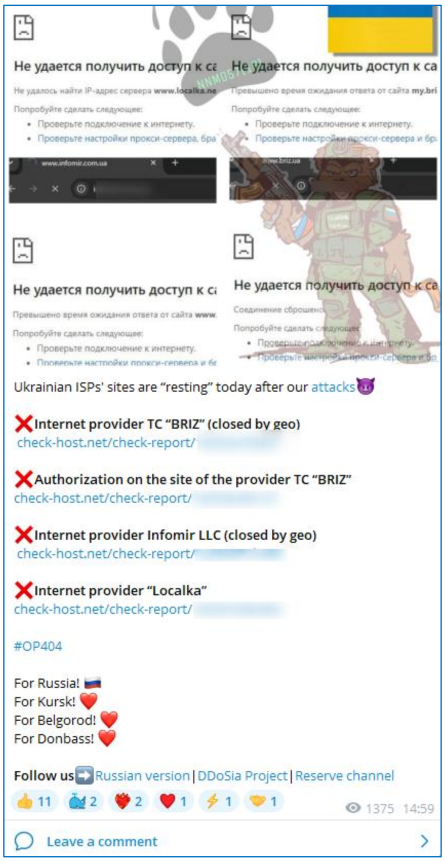
Figure 10 | Sectors most affected by ransomware in the second half of 2024.

6.3 Hacktivists

In the second half of 2024, hacktivist groups continued to influence global events, driven by political, social, and ideological agendas. These groups deployed various tactics, such as distributed denial of service (DDoS) attacks, website defacement, and data breaches to promote their causes. As we closely monitor this phenomenon, it is clear that hacktivism is on the rise, fueled by increasing political polarization. Among the most prominent groups are:

- **NoName057(16);**

This group is a threat actor, allegedly based in Russia, specialized in **DDoS attacks**, defacement, and data leaks. In August 2024, NoName057(16) launched **Operation #OP404**, a campaign that began in August with the goal of disrupting access to government and media websites in Ukraine and allied countries, including **NATO members**. The attacks, focused on generating the "404 Page Not Found" error, reflect the symbolic intent to disconnect and destabilize these websites.


Не удается получить доступ к са
Не удалось найти IP-адрес сервера www.localka.ne
Попробуйте сделать следующее:
- Проверьте подключение к интернету.
- Проверьте настройки прокси-сервера, бра

Не удается получить доступ к са
Превышено время ожидания ответа от сайта my.bri
Попробуйте сделать следующее:
- Проверьте подключение к интернету.
- Проверьте настройки прокси-сервера и бр

www.infomir.com.ua

www.briz.ua

Не удается получить доступ к са
Превышено время ожидания ответа от сайта www.
Попробуйте сделать следующее:
- Проверьте подключение к интернету.
- Проверьте настройки прокси-сервера и бе

Не удается получить доступ к са
Соединение сброшено.
Попробуйте сделать следующее:
- Проверьте подключение к интернету.
- Проверьте настройки прокси-сервера и бр

Ukrainian ISPs' sites are “resting” today after our attacks😈

❌**Internet provider TC “BRIZ” (closed by geo)**
check-host.net/check-report/[redacted]

❌**Authorization on the site of the provider TC “BRIZ”**
check-host.net/check-report/[redacted]

❌**Internet provider Infomir LLC (closed by geo)**
check-host.net/check-report/[redacted]

❌**Internet provider “Localka”**
check-host.net/check-report/[redacted]

#OP404

For Russia! 🇷🇺
For Kursk! ❤️
For Belgorod! ❤️
For Donbass! ❤️

Follow us➡️Russian version | DDoSia Project | Reserve channel

👍 11 🐳 2 ❤️‍🔥 2 ❤️ 1 ⚡ 1 💛 1 👁 1375 14:59

Leave a comment

Illustration 4 | Telegram post by the NoName057(16) group.

- **Cyber Army of Russia Reborn**

It resurfaced in 2024 as a key actor in the realm of cyberhacktivism, driven by strong nationalist motives. In July 2024, the group actively participated in **#OpSpain**, a cybercampaign launched by pro-Russian hacktivist groups against the websites and media of the Spanish Government. The operation includes DDoS attacks and defacements, aiming to disrupt services and spread pro-Russian propaganda. The campaign is a retaliation against Spain's support for Ukraine and its strategic alignment with NATO.

- **Indian Cyber Force**

This Indian hacktivist group collaborates with other pro-India teams such as **TeamUCC**, **Team-Network-Nine**, and **BlackDragonSec**. It is a pro-Israel group, known for claiming responsibility for cyberattacks on critical infrastructures in multiple countries, including Bangladesh, China, Pakistan, and Indonesia. In August 2024, the group recently launched cyberattacks in Bangladesh, posting videos in which they claim to have hacked the **Grameenphone Telecom** network control panel and other Internet service providers, as well as the Bangladesh government's national email system.

- **UserSec**

It is a pro-Russian group known for carrying out distributed denial of service (DDoS) attacks and posting data leaks, primarily targeting entities that support Ukraine. Following the arrest of Telegram CEO Pavel Durov, several pro-Russian groups, including UserSec, launched attacks against French entities under the campaign hashtag #FreeDurov. In a recent joint operation, UserSec and the **Cyberarmy of Russia reborn** successfully disabled the websites of the National Court of France and the Paris Court.

6.4 APT

- **Iranian APT**

Iranian APTs expanded their regional reach during this semester, with groups such as **MuddyWater** and **APT34** deploying custom malware, such as **BugSleep**, and employing advanced social engineering tactics. These campaigns primarily targeted governments and critical infrastructures across the Middle East, with **Israel** as the primary target, highlighting a significant intensification in their espionage activities.

- **Russian APT**

Meanwhile, Russian APTs exploited zero-day vulnerabilities to carry out strategic attacks. Groups such as **APT29** and **APT28** focused on vulnerabilities in iOS and Chrome, **using watering hole techniques** and modular malware to infiltrate diplomatic and government networks, thus enhancing their espionage capabilities. In Ukraine, Russia-aligned groups maintained high activity, attacking government entities, the defense sector, and essential services such as energy, water, and heating.

- **Chinese APT**

Chinese APTs adopted a renewed focus on critical network infrastructures. Groups such as **APT41** and **Earth Baku** used advanced malware, such as ShadowPad and VELVETSHELL, to compromise network devices, including Cisco Nexus switches, significantly impacting the security of these infrastructures.

- **North Korean APT**

Finally, North Korean APTs intensified their cyber espionage efforts, with groups such as **Kimsuky** and **Lazarus Group** targeting the education sector. Their campaigns focused on researchers and academics related to the Korean Peninsula and Southeast Asia, using **spear-phishing** techniques and advanced malware such as **MoonPeak** and **FPSpy** to achieve their objectives.

Tactics, Techniques and Procedures (TTPs)

7. Tactics, Techniques and Procedures (TTPs)

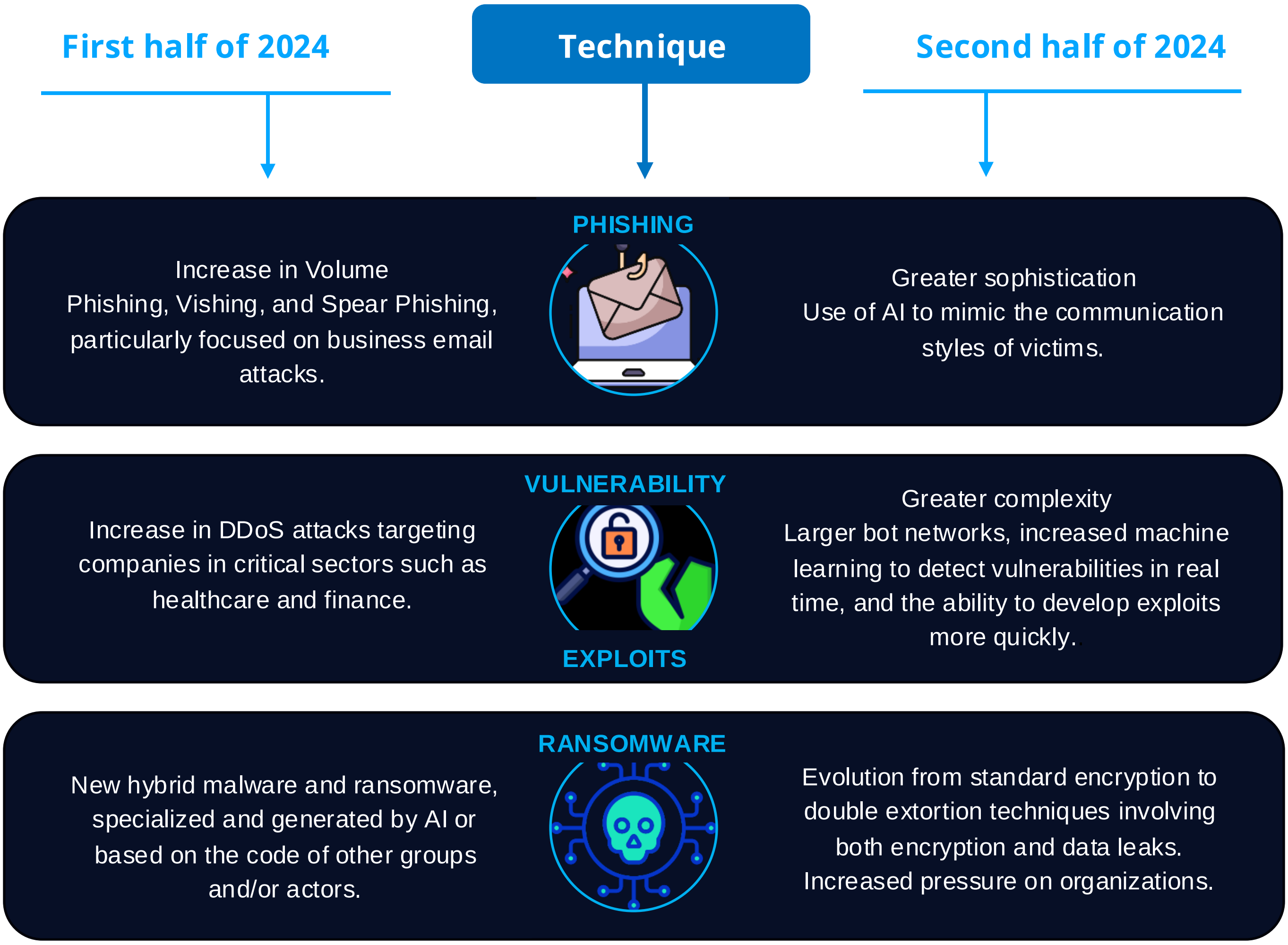
Tactics, Techniques, and Procedures (TTPs) are a fundamental approach to understanding the strategies employed by malicious actors in the cyber landscape. Identifying these patterns not only allows organizations to strengthen their defensive posture but also to proactively anticipate and mitigate potential risks.

The following will address the key TTPs of the second half of 2024, based on the identified trends.

7.1 Description of the most common TTPs used by cybercriminals

In the second half of 2024, cybercriminals have shown a notable evolution in their TTPs, continuously adapting to new technological environments and the defensive measures that have been implemented.

This section provides a summary of the most commonly used TTPs during this period, analyzing their relation to the MITRE ATT&CK framework, and offering both an overview of their impact and key recommendations for mitigation.



First half of 2024

Technique

Second half of 2024

PHISHING

Increase in Volume
Phishing, Vishing, and Spear Phishing, particularly focused on business email attacks.

Greater sophistication
Use of AI to mimic the communication styles of victims.

VULNERABILITY
EXPLOITS

Increase in DDoS attacks targeting companies in critical sectors such as healthcare and finance.

Greater complexity
Larger bot networks, increased machine learning to detect vulnerabilities in real time, and the ability to develop exploits more quickly.

RANSOMWARE

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

Evolution from standard encryption to double extortion techniques involving both encryption and data leaks.
Increased pressure on organizations.

Figure 11 | Evolution of the most common techniques used during 2024.

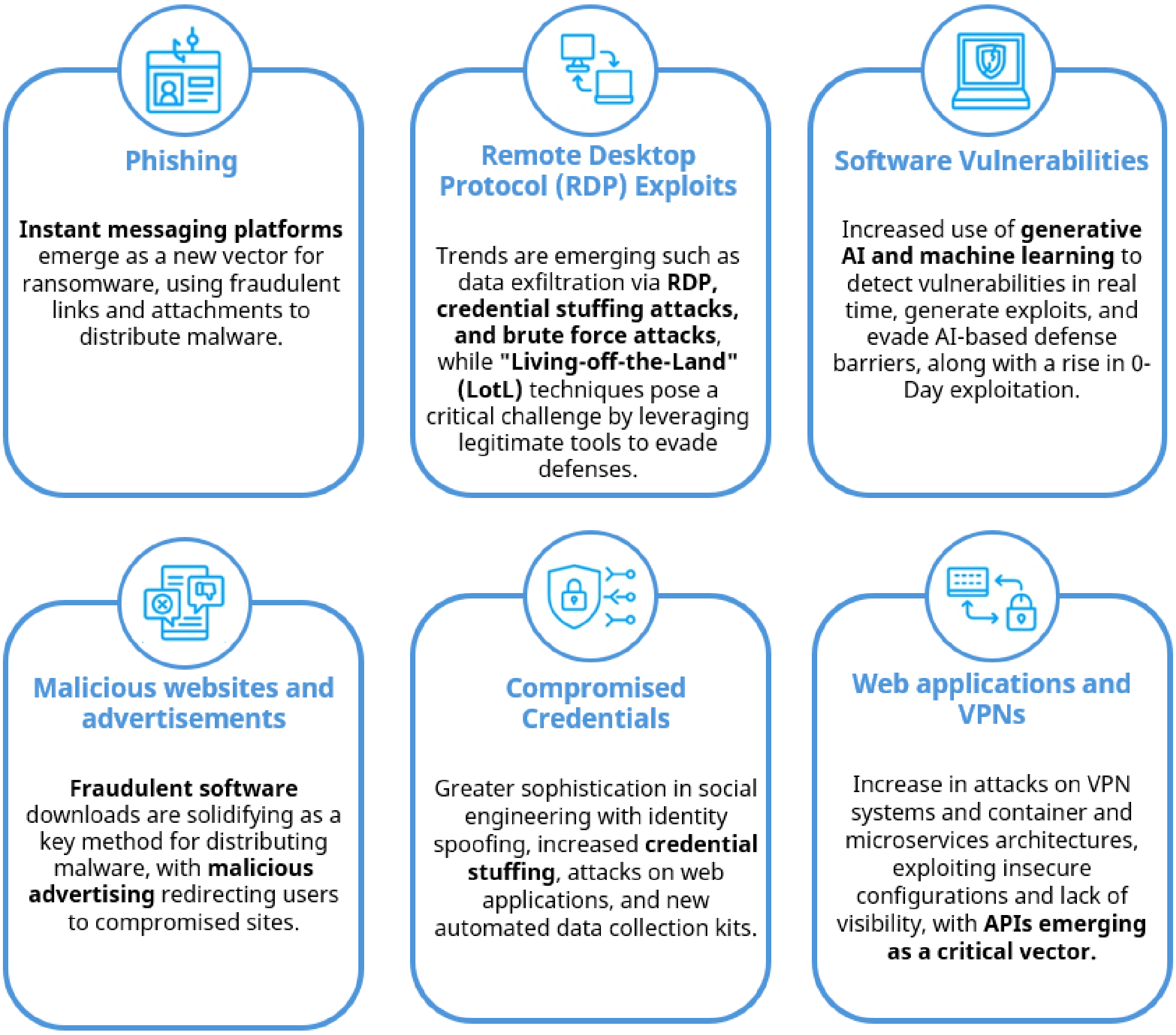
Technique	MITRE ATT&CK ID	Description	Mitigation	References
Phishing	T1078 – Valid Accounts	Credential dumping via phishing, used for initial access or persistence.	- Implement MFA on all accounts. - Educate employees to identify malicious emails..	T1078
	T1059 – Command and scripting interpreter	Use of malicious commands after compromising accounts to execute payloads or scripts.	- Enable attack surface reduction rules. - Limit the execution of unsigned scripts.	T1059
Vulnerability Exploits	T1583 – Infrastructure	Preparation of bot servers and networks to launch DDoS attacks or exploit vulnerabilities in critical systems.	- Monitor unusual network activities. - Implement DDoS solutions for critical services.	T1583
	T1547 – Boot or logon autostart execution	Persistence in compromised systems through configurations that automatically execute upon system startup.	- Monitor changes in startup programs. - Limit administrative privileges.	T1547
Ransomware	T1547 – Boot or logon autostart execution	Use of auto-configuration for persistence after infecting the system.	- Limit administrative permissions. - Audit programs configured to run during startup..	T1547
	T1078 – Valid Accounts	Use of compromised credentials to move ransomware within the network.	- Change default passwords. - Regularly audit accounts to detect anomalous activities.	T1078

Table 5 | Most common TTPs during the second half of 2024.

The second half of 2024 was characterized by the sophistication and scalability of the TTPs used by cybercriminals, who prioritized initial access and persistence techniques to maximize their impact. The connection with the MITRE ATT&CK framework not only helps understand these threats but also provides a practical approach for mitigating them.

7.2 Most common entry vectors:

Now, to access systems and carry out attacks, malicious actors use a wide variety of entry vectors or initial access points. Following the thread of the most used techniques this semester, and considering that ransomware has positioned itself as the main threat, the trends of the most common entry vectors are summarized as follows:



Phishing

Instant messaging platforms emerge as a new vector for ransomware, using fraudulent links and attachments to distribute malware.

Remote Desktop Protocol (RDP) Exploits

Trends are emerging such as data exfiltration via **RDP, credential stuffing attacks, and brute force attacks**, while **"Living-off-the-Land" (LotL)** techniques pose a critical challenge by leveraging legitimate tools to evade defenses.

Software Vulnerabilities

Increased use of **generative AI and machine learning** to detect vulnerabilities in real time, generate exploits, and evade AI-based defense barriers, along with a rise in 0-Day exploitation.

Malicious websites and advertisements

Fraudulent software downloads are solidifying as a key method for distributing malware, with **malicious advertising** redirecting users to compromised sites.

Compromised Credentials

Greater sophistication in social engineering with identity spoofing, increased **credential stuffing**, attacks on web applications, and new automated data collection kits.

Web applications and VPNs

Increase in attacks on VPN systems and container and microservices architectures, exploiting insecure configurations and lack of visibility, with **APIs emerging as a critical vector.**

Table 6 | Most common entry vectors used in the second half of 2024

7.3 Innovation in attacks: New unknown techniques and tactics

• Blast Radius

Description: Vulnerability that exploits the **RADIUS protocol (Remote Authentication Dial In User Service)** with **MITM (Man in the middle)** and a collision attack, to compromise an initial device by spoofing a valid response after a failed authentication, without needing to know the user's credentials. The lack of authentication and encryption in the protocol facilitates unauthorized access and exposure of sensitive data. (Ars Technica, 2024; Blast-RADIUS, 2024).

Impact: Affects all RADIUS implementations that use non-EAP authentication methods over UDP.

Mitigations/Recommendations:

- Conduct network audits to identify devices in use.
- Update obsolete and insecure protocols.
- Implement network segmentation to limit lateral movement.
- Establish continuous monitoring to detect suspicious activity.
- Train employees in cybersecurity.

This attack underscores the importance of modernizing network infrastructures and adopting proactive measures to minimize risks.

• RustyAttr

Description: The Lazarus group (North Korea) has developed **RustyAttr**, a trojan for macOS that uses extended attributes to hide malicious code and evade antivirus. Using the **Tauri framework**, it hides malicious scripts in files that simulate being legitimate documents, such as PDFs. This technique is unprecedented in the MITRE ATT&CK framework, marking a breakthrough in security evasion. (The Hacker News, 2024).

Impact: RustyAttr represents a high risk for organizations that rely on traditional security measures in macOS, such as Gatekeeper, compromising systems with innovative camouflage techniques.

Mitigations/Recommendations:

- Maintain strict Gatekeeper policies to block unauthorized applications.
- Conduct regular security status audits of macOS.
- Establish continuous monitoring to detect suspicious activity.
- Train staff to identify social engineering tactics.

• *QRishing - Identity theft through QR code*

Description: It uses **QR codes as an attack vector**, redirecting users to malicious sites after scanning. These sites can install malware, steal credentials, or offer fraudulent content. The technique exploits the trust and familiarity that users have with QR codes, evading conventional cyber defenses (ITWeb, 2024).

Impact: This method can compromise any device that reads the QR code, infecting it with malware, stealing personal information, or spreading attacks within organizational networks. The social impact falls on user trust regarding QR technology.

Mitigations/Recommendations:

- Implement secure browsing and malware detection tools to verify URLs before access.
- Configure network controls to block unauthorized or suspicious sites.
- Train users and employees about the risks of QR codes and how to identify fraudulent links.
- Promote secure verification practices when scanning QR codes.

• RDPWrap y Tailscale

Description: The combination of **RDPWrap**, which enables multiple RDP sessions on Windows, and **Tailscale**, a private network tool, allows attackers to establish covert remote access to infected systems. These accesses have been used to manipulate and steal cryptocurrencies or other digital assets, as well as exfiltrate sensitive information, without visibly modifying the system (The Cyber Express, 2024).

Impact: This attack primarily affects users in the cryptocurrency market, compromising the confidentiality, integrity, and availability of their digital accounts. Attackers can unauthorizedly access Windows 10 and Windows Server systems that support **RDPWrap**, as well as routers, firewalls, and IoT devices present during communication.

Mitigations/Recommendations:

- Restrict the use of RDP and disable it on systems where it is not necessary.
- Implement multi-factor authentication (MFA) to protect remote access.
- Use monitoring tools to log and alert unusual access.
- Conduct regular reviews of access logs to detect intrusions.
- Keep systems updated with patches and access control policies that limit unnecessary incoming connections.
- Train employees on the risks of tools like RDPWrap and the use of unauthorized software.

OtterCookie

Description: OtterCookie is an attack based on **credential stuffing** (the use of leaked credentials from other platforms) on web applications with weak security that automates the **mass sending** of username and password combinations to access vulnerable accounts. It is designed in **JavaScript** to execute additional payloads, including data exfiltration, access to credentials, and the implementation of spam via SMTP services or phishing kits (Bleeping Computer, 2024; The Hacker News, 2024) .

Impact: This attack primarily affects systems in Japan and North Korea, compromising the confidentiality, integrity, and availability of accounts and data. Additionally, the obtained accesses can be used to deploy ransomware, carry out identity theft, or compromise the internal network of organizations.

Mitigations/Recommendations:

- Implement multi-factor authentication (MFA) on all critical accounts.
- Enforce the use of strong and unique passwords, encouraging practices such as using password managers.
- Monitor failed access attempts and set alerts for multiple consecutive failures.
- Conduct regular audits on web applications and strengthen their security.
- Train users to avoid password reuse and detect phishing attempts.

New RaaS platform by KillSecurity

Description: The hacktivist group **KillSecurity** has launched a new Ransomware-as-a-Service (RaaS) platform available through Telegram and accessible via Tor. Developed in C++, it allows attackers to **customize ransomware**, **track campaign statistics**, and **communicate with victims via chat**. Upcoming features will include **DDoS attacks**, automated calls to pressure ransom payments, and data exfiltration tools (RedHotCyber, , 2024).

Impact: It affects both individual users and organizations. It compromises personal and business accounts, exposes sensitive data, and leads to significant financial losses due to asset theft and operational disruption.

Mitigations/Recommendations:

- Conduct ongoing training programs for employees, including phishing attack simulations and social engineering tactics.
- Implement multi-factor authentication (MFA) to protect access to critical systems.
- Review and strengthen cybersecurity policies.
- Deploy real-time monitoring solutions that detect access attempts from unknown locations or unusual download patterns.

Vulnerability trends

8. Vulnerabilities

The second half of 2024 has highlighted the persistent and changing threat of **critical vulnerabilities** in software and hardware systems. These vulnerabilities, often exploited by malicious actors, pose significant risks to organizations across various sectors. They can lead to critical data leaks, loss of confidential data, and disruption of essential services.

To prioritize and effectively address these vulnerabilities, it is crucial to evaluate not only their technical severity but also their potential real-world impact; therefore, the following analyzes how critical vulnerabilities evolved month by month during the second half of 2024.

• July

In July 2024, **104 vulnerabilities** were identified, of which **28 are of critical severity** and **10 were actively exploited**. These vulnerabilities stood out for their impact on critical platforms used in business environments and for their ability to compromise confidential data and essential workflows.

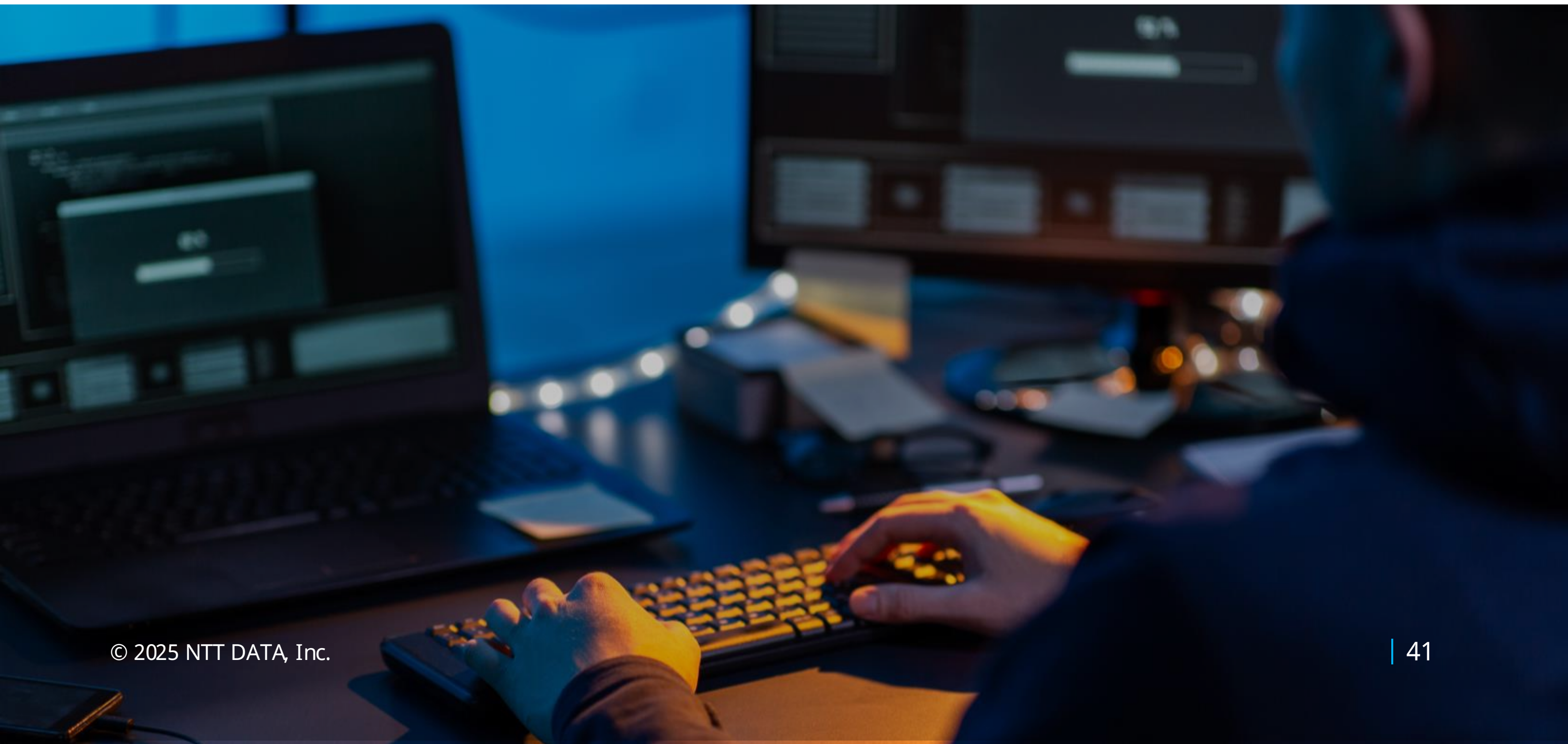
Key vulnerabilities highlighted:

- **ServiceNow (CVE-2024-4879 y CVE-2024-5217):** The vulnerabilities allowed unauthorized access to critical data and the exfiltration of sensitive information by exploiting workflows on this cloud-based platform.
- **OpenSSH (CVE-2024-6387 - "regreSSHion"):** A serious vulnerability in the Secure Shell (SSH) protocol that allowed arbitrary code execution as root, affecting more than 200 products.
- **GeoServer (CVE-2024-36401):** Vulnerability in the evaluation of property names as XPath expressions, which allowed attackers to execute arbitrary commands on outdated systems.

Main impacts:

- Unauthorized access to critical infrastructures and confidential data.
- Compromise of secure networks through arbitrary code execution.
- Significant risks in geospatial data management platforms.

This month's activity reinforces the need for proactive patch management, especially on critical platforms like **ServiceNow** and **OpenSSH**. It also highlights the importance of regular security audits to mitigate risks associated with known vulnerabilities.



• August

In August 2024, **118 vulnerabilities** were identified, of which **20 are of critical severity** and **19 were actively exploited**, marking a significant increase compared to the previous month. These vulnerabilities were primarily targeted at broad and widely used platforms.

Key vulnerabilities highlighted:

- **Windows SmartScreen (CVE-2024-38213 - "Copy2Pwn"):** Allows attackers to bypass protections through malicious WebDAV shared resources. It was linked to malware operators such as DarkGate.
- **Microsoft Project and Windows Kernel (CVE-2024-38107, CVE-2024-38189):** These critical vulnerabilities facilitated privilege escalation and remote code execution.
- **Google Chrome (CVE-2024-7965):** A flaw in the V8 engine that allowed heap corruption, actively exploited in browsers.
- **SolarWinds Web Help Desk (CVE-2024-28986):** A Java deserialization vulnerability, quickly exploited after its disclosure.

Main impacts:

- Privilege escalation in operating systems and web browsers.
- Increased risks in widely used browsers and collaboration tools.
- Exploitation directed at the cryptocurrency sector by groups like **Citrine Sleet**.

• September

In September 2024, **96 vulnerabilities** were identified, of which **24 are of critical severity** and **9 were actively exploited.** This month was marked by the predominance of vulnerabilities in Microsoft products, reflecting their ubiquity in business and personal environments.

Highlighted key vulnerabilities:

- **CVE-2024-38226 (Microsoft Publisher):** Used to bypass security controls and facilitate social engineering attacks.
- **CVE-2024-38217 (Windows Mark-of-the-Web):** Allowed the execution of malicious files by bypassing security functions.
- **Ivanti (CVE-2024-819) and Veeam (CVE-2024-40711):** Escalated privileges and circumvented security functions to distribute malware.

Main impacts:

- Social engineering attacks that relied on user interaction.
- Distribution of malware through key business management products.
- Elevated risk due to actively exploited zero-day vulnerabilities.

• October

October marked a peak in the number of vulnerabilities, with **153 identified**, of which **13 are of critical severity** and **7 were actively exploited**. The great diversity of affected products this month underscores the need for broader defense strategies and effective collaboration among security teams.

Key vulnerabilities highlighted:

- Diversity of affected products: Microsoft Windows, Zimbra, Mozilla Firefox, Qualcomm, Samsung Exynos, Cisco, Ivanti, ScienceLogic, and Grafana.
- **Microsoft Windows Kernel (CVE-2024-43640):** Actively exploited for privilege escalation.
- **Zimbra and Mozilla Firefox:** Critical vulnerabilities that compromised data and access in widely used tools.

Main impacts:

- Diversification of targets to maximize the impact of attacks.
- Elevated risks on mobile devices, collaboration tools, and browsers.
- Increased exposure due to the release of proof of concept (PoC) exploits.

• November

In November 2024, **98 vulnerabilities** were identified, of which **16 are of critical severity** and **12 were actively exploited**. The activity in November reinforces the need to protect mobile systems and critical enterprise platforms through timely patches and constant monitoring.

Key highlighted vulnerabilities:

- **Oracle Agile Product Lifecycle Management (CVE-2024-21287):** Exploited to compromise enterprise productivity platforms..
- **Apple iOS and GeoVision GVLX Mobile Video Recorder (CVE-2024-11120):** Attacks targeting mobile systems and physical security devices.
- **Needrestart (Linux):** A utility for managing processes, compromised for privilege escalation.

Main impacts:

- Arbitrary code execution and remote access.
- Impact on critical infrastructures and mobile devices.
- Elevated risk in enterprise management software and SCADA.

• December

December closed the year with a significant increase, reaching **65 high-risk vulnerabilities**, of which **6 are of critical severity** and **7 were actively exploited**. Among these critical vulnerabilities, activity was notable on file transfer platforms and operating systems. The rise in critical vulnerabilities during December underscores the importance of robust cybersecurity strategies to mitigate risks during periods of high malicious activity.

Key highlighted vulnerabilities:

- **CVE-2024-50623 and CVE-2024-55956 (Cleo MFT):** Exploited by the CL0P group, affecting file transfer products.
- **CVE-2024-49138 (Microsoft Windows Common Log File System Driver):** Zero-day vulnerability that allowed buffer overflow.

Main impacts:

- Exploitation of zero days in key systems..
- Elevated risks in widely used products for data transfer.
- Increase in unexploited critical vulnerabilities, but with published PoCs.

Trends

After analyzing the vulnerabilities of the second half of 2024, a monthly evolution is observed that highlights both the **volume of critical failures and their active exploitation**. Attackers have demonstrated a **growing ability to exploit high-impact vulnerabilities**, especially **zero days**, before the corresponding patches are applied.

After analyzing the vulnerabilities of the second half of 2024, a monthly evolution is observed that highlights both the volume of critical failures and their active exploitation. Attackers have demonstrated a growing ability to exploit high-impact vulnerabilities, especially zero days, before the corresponding patches are applied.

In **November and December**, an increase in zero-day exploitation was observed, highlighting a tactical shift towards newly discovered vulnerabilities.

Comparison of vulnerabilities and their exploitation (July / December 2024)

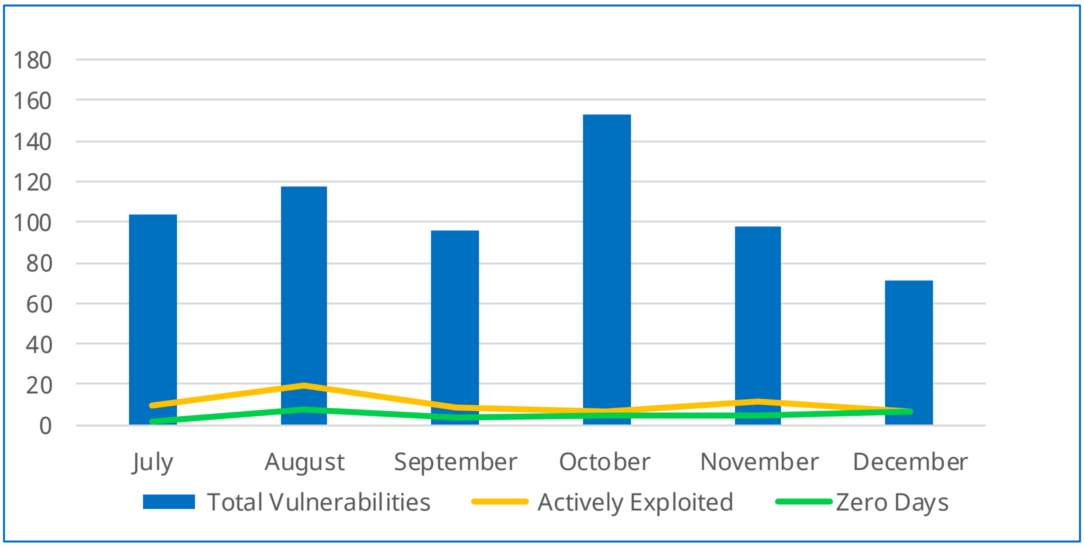


Figure 12 |. Monthly comparative of identified critical vulnerabilities, actively exploited vulnerabilities and zero days during the second half of 2024.

The monthly evolution of vulnerabilities during the six-month period reflects the need to strengthen patch management, improve collaboration between security teams and prioritize education in social engineering to mitigate the risks derived from these constantly evolving threats.

Future outlook

9. What awaits us in 2025?

The threat groups analyzed in this report will not disappear in the short term and, with high probability, will continue to pose significant risks in the medium term (6-12 months). The ransomware group **RansomHub** solidified its position as the most active group during 2024, especially following the low activity of **Lockbit** and **ALPHV**, and its activity is expected to remain prominent due to its spread through the ransomware-as-a-service (RaaS) model, its advanced technical capabilities for achieving remote control of devices and evading detection by monitoring systems.

Activity on the Dark Web, theft, and exfiltration of confidential data has been, and will continue to be, one of the main dangers in the digital realm. The threat actor **IntelBroker** has stolen and published several high-profile leaks from more than 400 of the largest and most important companies in the technology industry worldwide in recent months, although the total impact of these leaks is still unfolding. Consequently, it is expected that supply chain attacks will increase in frequency and complexity.

By focusing on less secure partners, these attacks exploit the interconnectedness of companies to gain access to more secure networks. Cyber damage worldwide is expected to reach $10 trillion by 2025, with most of it resulting from identity theft used to demand ransoms from companies and individuals. On the other hand, during 2025, the activity of "the four big players" (Russia, China, Iran, and North Korea) will be monitored, as they pursue their respective geopolitical objectives through cyber-espionage, disruption, and influence operations.

Rapid technological advances, especially in Artificial Intelligence, are reconfiguring the tactics of defenders and adversaries. While its use is rapidly providing new tools for threat detection and response, it also gives malicious actors powerful capabilities for social engineering, misinformation, and other attacks. A significant increase in patching times and vulnerability mitigation is expected in 2025, driven by the growing complexity of IT and OT systems and the prevalence of unsupported IoT devices. Multiple findings from 2024 reveal that organizations take an average of 97 days to address critical vulnerabilities and 146 days for low-impact ones, far exceeding best practice recommendations of 7 to 30 days. These delays expose organizations to prolonged periods of risk, allowing attackers to exploit known vulnerabilities.

Staying proactive and flexible is crucial. By continuously monitoring changes in tactics, techniques, and procedures (TTPs), security teams can anticipate attacks and adjust their defenses accordingly. Implementing automated incident responses can improve remediation by automatically containing threats upon detection, isolating hosts, blocking suspicious IoCs, terminating sessions, and rotating user credentials.

Aligning threat intelligence with a specific threat model ensures that the most relevant threats are prioritized and effectively mitigated. This vigilant and adaptive approach helps protect against emerging risks and maintains the integrity of critical systems and data.

References

- Infosecurity Magazine. (s.f.). *Operation Cronos: LockBit Takedown*. Retrieved from: https://www.infosecurity-magazine.com/news/operation-cronos-lockbit-takedown/

- CiberPrisma. (2024). *Operación Synergia II: Un golpe global contra el cibercrimen*. Retrieved from: https://ciberprisma.org/2024/11/09/operacion-synergia-ii-un-golpe-global-contra-el-cibercrimen/

- INTERPOL. (2024). *Descubrimiento de una red delictiva: 5,100 detenciones en una vasta operación contra las apuestas futbolísticas ilegales*. Retrieved from: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/Descubrimiento-de-una-red-delictiva-5-100-de

- T21. (2024). *Sectores más atacados por cibercriminales en 2024*. Retrieved from: https://t21.pe/sector-atacado-cibercriminales-2024

- Líder Empresarial. (2024). *Ciberataques en aumento: nuevos grupos de ransomware emergen en 2024*. Retrieved from: https://www.liderempresarial.com/ciberataques-en-aumento-nuevos-grupos-de-ransomware-emergen-en-2024/

- Statista. (2024). *Estadísticas de ciberseguridad global. Statista Cybersecurity*. Retrieved from: https://www.statista.com/outlook/tmo/cybersecurity/worldwide

- World Economic Forum. (2024). *Annual Report*. Retrieved from: https://es.weforum.org/publications/series/annual-report/

- Ingecom. (s.f.). *Predicciones de ciberseguridad en privacidad de datos. Ingecom Cybersecurity Trends*. Retrieved from: https://www.ingecom.net/es/blog/295/tendencias-en-ciberseguridad-para-2024-lo-que-necesitas-saber/

- IBM. (2023). *Costos de violaciones de seguridad en 2023. IBM Cost of a Data Breach Report*. Retrieved from: https://www.ibm.com/reports/data-breach/

References

- Kaspersky. (2024). *Kaspersky pronostica ransomware más resistente y nuevas amenazas a finanzas móviles para 2025*. Retrieved from: https://latam.kaspersky.com/about/press-releases/kaspersky-pronostica-ransomware-mas-resistente-y-nuevas-amenazas-a-finanzas-moviles-para-2025?srsltid=AfmBOooatD2O-cSpZ4Xfy33s9w_9tRdA5nzsIMn78tnkJVk-JbhEwzzG

- Ciberseguridad.com. (s.f.). *Principales tendencias y predicciones para 2024*. Retrieved from: https://ciberseguridad.com/blog/predicciones-ciberseguridad-2024/

- McKinsey. (s.f.). *Impacto de la digitalización y ciberseguridad en la economía global*. McKinsey Digital Insights. Retrieved from: https://www.mckinsey.com/business-functions/mckinsey-digital/

- Kroll. (2024). *Q2 2024 Threat Landscape Report: Threat Actors, Ransomware, Cloud Risks Accelerate*. Retrieved from: https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q2-2024-threat-landscape-report-threat-actors-ransomware-cloud-risks-accelerate

- CRN. (2024). *10 Major Ransomware Attacks and Data Breaches in 2024*. Retrieved from: https://www.crn.com/news/security/2024/10-major-ransomware-attacks-and-data-breaches-in-2024

- Semperis. (2024). *España: Riesgo de ransomware en 2024*. Retrieved from: https://www.semperis.com/es/resources/espana-ransomware-risk/

- ESET. (2024). *Reporte de amenazas: Segundo semestre de 2024*. Retrieved from: https://www.welivesecurity.com/es/informes/eset-reporte-amenazas-segundo-semestre-2024/

- Europol. (2024). *Nuevo informe: La inteligencia artificial como refuerzo de las organizaciones policiales*. Retrieved from: https://notesdeseguretat.blog.gencat.cat/2024/10/07/nuevo-informe-de-europol-la-inteligencia-artificial-como-refuerzo-de-las-organizaciones-policiales/

References

- Ciberseguridad Blog. (2024). *El impacto del 5G en la ciberseguridad*. Retrieved from: https://www.ciber-seguridad.blog/el-impacto-del-5g-en-la-ciberseguridad

- Gartner. (2024). *Tendencias en ciberseguridad 2024*. Retrieved from: https://www.gartner.es/es/tecnologia-de-la-informacion/tendencias/tendencias-ciberseguridad

- Acronis. (2024). *Cyberthreats Report H1 2024: Breaking Down Key Findings*. Retrieved from: https://www.acronis.com/es-es/blog/posts/acronis-cyberthreats-report-h1-2024-breaking-down-key-findings-from-the-report/

- VPN Ranks. (2024). *Tendencias y amenazas de deepfake*. Retrieved from: https://www.vpnranks.com/es-es/recursos/tendencias-y-amenazas-deepfake/

- Ramos-Zaga, F. (2024*). Deepfake: Análisis de sus implicancias tecnológicas y jurídicas en la era de la Inteligencia Artificial. Derecho Global. Estudios sobre Derecho y Justicia, 9(27)*. Retrieved from: https://doi.org/10.32870/dgedj.v9i27.754

- DeuSens. (2024). *Innovaciones y desafíos en el metaverso para 2024*. Retrieved from: https://deusens.com/es/blog/innovaciones-desafios-metaverso-2024#:~:text=En%20el%20a%C3%B1o%202024%2C%20el,Interfaz%20de%20Usuario%20e%20Interacci%C3%B3n

- Alcoyinnova. (2024). *Las 5 tecnologías que están revolucionando el mundo en 2024*. Retrieved from: https://alcoyinnova.com/las-5-tecnologias-que-estan-revolucionando-el-mundo-en-2024/

- VPN Ranks. (2024). *Tendencias tecnológicas*. Retrieved from: https://www.vpnranks.com/es-es/recursos/tendencias-tecnologicas/

References

- Recorded Future. (s.f.). *Threat Intelligence 101: Ransomware Attack Vectors*. Retrieved from: https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-attack-vectors

- Balbix. (s.f.). *Attack Vectors and Breach Methods*. Retrieved from: https://www.balbix.com/insights/attack-vectors-and-breach-methods/

- AIMultiple. (s.f.). *Most Common Cyber Attack Vectors*. Retrieved from: https://research.aimultiple.com/most-common-cyber-attack-vectors/

- Arctic Wolf. (s.f.). *Top Five Cyberattack Vectors*. Retrieved from: https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/

- Bleeping Computer. (2024). *Russian Hackers Use RDP Proxies to Steal Data in MiTM Attacks*. Retrieved from: https://www.bleepingcomputer.com/news/security/russian-hackers-use-rdp-proxies-to-steal-data-in-mitm-attacks/

- Hackers4U. (s.f.). *Top Cyber Attack Vectors and How to Mitigate Them*. Retrieved from: https://www.hackers4u.com/top-cyber-attack-vectors-and-how-to-mitigate-them

- Hispasec. (2024). *La Botnet Matrix desata ataques DDoS masivos explotando dispositivos IoT vulnerables*. Retrieved from: https://unaaldia.hispasec.com/2024/11/la-botnet-matrix-desata-ataques-ddos-masivos-explotando-dispositivos-iot-vulnerables.html

- Weber, M. (2024). *Hybrid Warfare and Cybersecurity. Journal of Global Threats, 14(3), 25–47*. Retrieved from: https://www.sia-partners.com/en/insights/publications/hybrid-warfare-how-cyber-warfare-transforming-international-relations

References

- European Union Agency for Cybersecurity (ENISA) (2024). *ENISA Threat Landscape 2024: July 2023 to June 2024*. European Union Agency for Cybersecurity. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

- Gartner. (2024). *Cybersecurity Predictions for 2024.* Retrieved from: https://www.gartner.com/en/webinar/619414/1383687

- Sonatype. (2023). *The Evolution of Supply Chain Attacks*. Retrieved from: https://www.sonatype.com/hubfs/WP-Evolution-of-SSC-Attacks_03152023.pdf

- Ámbito. (2024). *BRICS vs G20: El ascenso del bloque señala un cambio en el poder global*. Retrieved from: https://www.ambito.com/finanzas/brics-vs-g20-el-ascenso-del-bloque-senala-un-cambio-el-poder-global-n6073582

- TV BRICS. (2024). *Países del G20 apoyan la cooperación en la regulación de la IA en la declaración final de la cumbre*. Retrieved from: https://tvbrics.com/es/news/pa-ses-del-g20-apoyan-la-cooperaci-n-en-la-regulaci-n-final-de-la-cumbre

- Carnegie Endowment for International Peace. (2024). *Emerging Middle Powers: BRICS Summit and Its Global Implications*. Retrieved from: https://carnegieendowment.org/research/2024/10/brics-summit-emerging-middle-powers-g7-g20?lang=en

- Foro Económico Mundial. (2024). *Foco en la ciberseguridad: 10 cosas que necesitas saber en 2024*. Retrieved from: https://es.weforum.org/stories/2024/10/foco-en-la-ciberseguridad-10-cosas-que-necesitas-saber-en-2024

- CrowdStrike. (2024). *Global Threat Report 2024*. Retrieved from: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

References

- Google Threat Analysis Group. (2024). *APT44 and Sandworm Activities*. Retrieved from: https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm/

- CISA. (2024). *People's Republic of China-Linked Cyber Actors Hide in Router Firmware*. Retrieved from: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a

- Mandiant. (2024). *Chinese Espionage Group UNC3886 Found Exploiting VMware Vulnerabilities Since 2021*. Retrieved from: https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021

- JPCERT. (2024). *New Malicious PyPI Packages Used by Lazarus*. Retrieved from: https://blogs.jpcert.or.jp/en/2024/02/lazarus_pypi.html

- Lisa Institute. (2024*). Tendencias Globales en Seguridad*. Retrieved from: https://www.lisainstitute.com/blogs/blog/lista-10-riesgos-geopoliticos-tendencias-seguridad-2019-2025

NTT DATA