CTI Trends

Cyber Threat Intelligence

January–June 2025

Index

Index

Introduction

1.1. Report Objective

This report provides a detailed overview of the latest trends, incidents, and developments shaping Cyber Threat Intelligence in the first half of 2025. It covers emerging threats that are redefining the cybersecurity landscape, the most active threat actors, major cyber campaigns, and critical vulnerabilities identified during this period. It also highlights recurring patterns and outlines potential future scenarios that may influence risk management and mitigation strategies.

1.2. Geographical and Chronological Scope

The analysis presented adopts a global perspective, allowing for an understanding of how threats evolve in interconnected ways across different geographical contexts. This broad view enables the identification of common dynamics and regional particularities that enrich the understanding of the current cyber environment.

This environment is characterized by significant changes in threat behavior and events that have had a substantial impact on the digital ecosystem. This reporting period is crucial for anticipating potential future developments and for strengthening response capabilities in an increasingly complex landscape.

Global Threat Landscape

2. Global Threat Landscape

In 2025, the world faces an increasingly interconnected and complex risk environment, where physical and cyberspace threats converge and amplify one another. Armed conflicts, extreme weather events, and cyberattacks targeting critical infrastructure rank among the top five global risks of the year (World Economic Forum, 2025), creating an increasingly uncertain outlook.

This convergence of threats underscores a critical trend: risks no longer appear in isolation but rather reinforce each other within a context of growing geopolitical fragmentation, social polarization, and accelerated technological change. In this scenario, international collaboration and organizational resilience have become essential pillars to face a rapidly evolving threat landscape that demands coordinated, adaptive, and threat intelligence–driven responses.

2.1 Geopolitics and Cybersecurity

In today's global landscape, geopolitical and technological risks represent the most pressing short-term concerns. On one hand, massive digitalization, along with the expansion of AI, has increased the attack surface and enabled new forms of cybercrime, espionage, and disinformation. On the other hand, rising geopolitical tensions and the resulting push toward deglobalization are driving governments and organizations to operate in increasingly hostile environments. These conditions are characterized by decentralized attacks and the difficulty of enforcing effective legal and regulatory frameworks, further complicating cybersecurity strategies.

During the first half of 2025, the following key trends have intensified the relationship between cybersecurity and the global geopolitical situation (Group-IB, 2025; CrowdStrike, 2025):

- **Rise of state-sponsored actors and geopolitical cyberespionage:**

There has been a noticeable increase in cyber activity attributed to state-sponsored actors. Notably, operations linked to entities from the People's Republic of China have multiplied in strategic sectors such as finance, manufacturing, and media. **North Korea** and **Iran** have also intensified their operations, combining espionage, illicit revenue generation, and politically motivated disinformation campaigns. In addition, Advanced Persistent Threats (APTs) have become more specialized and harder to track, operating with higher OPSEC (Operational Security) and sharing tools among groups.

- **Use of generative AI in disinformation and espionage campaigns:**

As highlighted in the previous semester's report, generative AI has become a key tool for adversaries. It enables more sophisticated social engineering campaigns, fake profiles, deepfakes, and large-scale electoral disinformation, prompting governments to establish specialized detection units (Federal Ministry of the Interior, 2025). This technology has lowered the entry barriers for malicious actors by facilitating the automation of attacks and the development of malicious scripts for faster and more effective exploitation of vulnerabilities and phishing campaigns.

- **Ransomware as a geopolitical pressure tool:**

The Ransomware-as-a-Service (RaaS) model, along with the volume of ransomware attacks disclosed on leak sites, continues to grow at a steady pace. Some attacks have had direct geopolitical impact, particularly on critical infrastructure such as government networks and manufacturing industries, highlighting their destabilizing potential. Additionally, the emergence of new ransomware groups during the first half of the year points to an ongoing trend toward cybercrime professionalization, with some groups implementing branding strategies and public messaging approaches that resemble those used by legitimate businesses.

- **Digital fragmentation and regulatory barriers:**

Digital deglobalization and rising political tensions are hampering international cybersecurity cooperation. Jurisdictional barriers and the lack of common legal frameworks complicate the prosecution of transnational actors, a situation exploited by criminal and state-sponsored groups operating from regions with low legal cooperation.

As a result, cybersecurity has become a strategic instrument in the global geopolitical context—key to anticipating technological threats that extend beyond the digital realm and into the physical world.

2.2 Geopolitics and Key Threat Actors

The evolution of the cybersecurity landscape during the first half of 2025 has been significantly shaped by armed conflicts, diplomatic tensions, and strategic rivalries between global powers. In this context, nation-state-linked threat actors have intensified their operations, leveraging digital tools to conduct espionage, sabotage, and disinformation campaigns.

This section analyzes the main geopolitical hotspots and the most active cyber groups, highlighting how their actions have affected regional and global stability through persistent, targeted campaigns.

- **Shadow Cyberwar: Russia and Ukraine on the Digital Frontline**

In the Russia–Ukraine conflict, digital operations have played a central role in **attrition strategies and information control**, extending to third-party countries with geopolitical interests, especially within the European Union.

Campaigns attributed to Russian threat actors have revealed a dual dimension: on one hand, cyber espionage and disinformation are being used as tools for diplomatic pressure and narrative manipulation; on the other, disruptive and sabotage-oriented digital operations have been directed at critical infrastructure, particularly targeting Ukraine.

This hybrid tactic blends technical persistence with political objectives, amplifying the reach of the conflict beyond its physical borders. A detailed technical analysis of these operations, along with the threat actors involved, is presented in section "6.4, APTs." This section delves into the evolution of specific campaigns, the tools deployed, and their impact across different regions.

- **Middle East: Regional Escalation and Transnational Threats**

In the first half of 2025, the Middle East has seen rising geopolitical tensions with direct consequences in cyberspace. On June 13, Israel launched a major air offensive against Iran, followed by a 700% surge in cyberattacks targeting Israeli systems over the next two days. The number of Iranian or pro-Iranian groups appears to be considerably higher. While activist culture remains strong in Western countries, the hacktivist scene is largely dominated by actors from the Eastern hemisphere, where Iran receives broader support.

Multiple sources have identified 65 pro-Iranian, 11 anti-Iranian, and 6 pro-Israeli groups—totaling 82. This figure is expected to increase as the conflict evolves.

Threat actors aligned with Iran remained highly active, led by MuddyWater, which frequently deployed RMM tools in phishing campaigns. BladedFeline also resumed targeting a previously attacked telecommunications company in Uzbekistan, coinciding with Iran's diplomatic engagement in the region. Other actors, such as CyberToufan, carried out destructive operations, including a data-wiping attack on multiple Israeli organizations.

- **U.S.–China: Digital Power Struggle Between Superpowers**

By 2025, the geopolitical rivalry between the United States and China has transcended diplomatic and economic dimensions, evolving into a high-intensity cyberwar over technological dominance, information sovereignty, and control of trade and critical infrastructure—amid growing global supply chain fragmentation.

Volt Typhoon, an APT group linked to the Chinese government, has been at the forefront of infiltration campaigns targeting U.S. and Taiwanese networks, particularly in the telecommunications, energy, and defense sectors. Their approach prioritizes stealth and persistence, using Living off the Land (LotL) techniques to evade detection. These infiltration efforts have been accompanied by a surge in military maneuvers and cyberattacks around Taiwan, reflecting the heightened strategic tensions in the region.

On the U.S. side, Equation Group and TAO—both affiliated with the NSA—represent the country's cyber response capabilities, known for their sophisticated offensive operations. These groups have been accused of conducting digital sabotage and espionage campaigns targeting foreign infrastructure, including Chinese assets.

- **Korean Peninsula: A War Without Bullets**

Threat actors aligned with North Korea were particularly active in financially motivated campaigns.

The group **DeceptiveDevelopment** significantly broadened its targets, using fake job offers mainly in the cryptocurrency, blockchain, and finance sectors. These campaigns employed social engineering techniques such as **ClickFix** attacks and fake posts used to distribute the cross-platform malware **WeaselStore**.

Meanwhile, the cryptocurrency theft targeting **Bybit**—attributed by the FBI to the **TraderTraitor** group—compromised Safe's supply chain and resulted in losses estimated at $1.5 billion.

Meanwhile, other North Korea–aligned groups showed fluctuating operational tempos: early 2025 saw **Kimsuky and Konni** return to usual levels of activity after a decline at the end of 2024, focusing their attacks on South Korean diplomatic entities and personnel.
The threat group **Andariel** also reemerged after a year-long dormancy with a sophisticated attack on a South Korean industrial software company.

- **Flashpoints in the Indo-Pacific**

The current situation in Myanmar has fostered an environment where internal **cyberespionage and digital** repression by the military regime intersect with **large-scale transnational cybercrime operations.** Fraud schemes such as pig butchering, illegal gambling, and crypto scams have evolved through the use of deepfakes, generative AI, and blockchain technologies—providing criminal groups with enhanced anonymity, operational efficiency, and technical sophistication.

Meanwhile, tensions escalated between India and Pakistan following a terrorist attack on Indian territory in the Jammu and Kashmir region. This incident sharply escalated political friction between the two nations, triggering a series of military clashes that continued until a U.S.-mediated ceasefire was achieved on May 10. These episodes triggered an intense disinformation campaign across social networks and digital media, characterized by **manipulated videos, falsified storylines, and the amplification of polarizing content** via fake account networks. Indian government services were also targeted by numerous cyberattacks attributed to actors such as **AnonSec, Sylhet Gang (SG), and DieNet**—part of an information warfare campaign involving both state and non-state actors in an increasingly volatile cyber conflict.

Overall, 2025 has solidified cyber espionage as a central instrument in global geopolitical competition. Spear phishing remains the preferred technique among APT groups across multiple regions, while disruptive operations—particularly originating from the Middle East—and disinformation campaigns are gaining prominence, shaping the trajectory of the modern digital conflict.

2.3 Impact of Cyberattacks on Specific Sectors

To conclude the global threat assessment, **NTT DATA's Cyber Threat Intelligence Department** highlights the evolution of cyberattacks during the first half of 2025. The analysis focuses on the most affected sectors and countries, showing only slight structural variations compared to the pattern observed in the second half of 2024.

The distribution of attacks once again reflects the strong influence of geopolitical tensions, with threats directed primarily at strategic sectors and countries of high economic relevance or those involved in conflict. The impact of these attacks has not been uniform, although the gap between sectors has narrowed considerably. Compared to H2 2024, sectoral impact variability has decreased by nearly 8%.

- **Public Administration and Government:**

Building on this trend, this sector remains the most targeted, with **3,005 cyberattacks** directed at public administrations and **779 targeting government and public sector institutions**, totaling 3,784 incidents. This represents a **41.30% increase** compared to the previous report and underscores the sustained interest of threat actors in exploiting governmental vulnerabilities. Continued geopolitical tensions are once again motivating targeted threats against these entities, often aimed at extracting sensitive information that may provide strategic advantage or support hacktivist campaigns.

- **Education:**

Cyberattacks on educational institutions **dropped by nearly 23% compared to last year**, **totaling 1,110 incidents**. While the number of attacks on this sector has declined, educational institutions—particularly universities—continue to represent high-value targets due to their intellectual property assets, the volume of sensitive personal data they hold, and their often-undersecured operational environments.

- **Financial Services:**

The financial sector recorded a **26.9% increase in incidents compared to 2024, with 835 cyberattacks reported**. It remains among the top three most targeted sectors. This trend reflects a shift in threat actor priorities, with a growing preference for governmental and financial targets due to ongoing geopolitical dynamics.

- **IT and Telcos:**

With 739 and 652 incidents respectively, technology and telecom infrastructure continue to be lucrative targets. The most common attack vectors include data theft and system compromise, executed with objectives ranging from financial gain and operational disruption to, in some cases, causing physical damage on critical infrastructure.

Ransomware continues to dominate as the primary attack vector. Although its trend declined between April and June 2025, the highest peaks of activity were recorded between January and February. In the last three months, the most affected industries have been construction and manufacturing, accounting for 12% of all attacks. From a geographic perspective, the United States (664), Canada (77), and Germany (69) were the most frequently targeted countries.

Further detail on this attack type can be found in section "6.2 Ransomware Groups."

Sectors most affected by cyberattacks (H1 2025 vs. H2 2024)

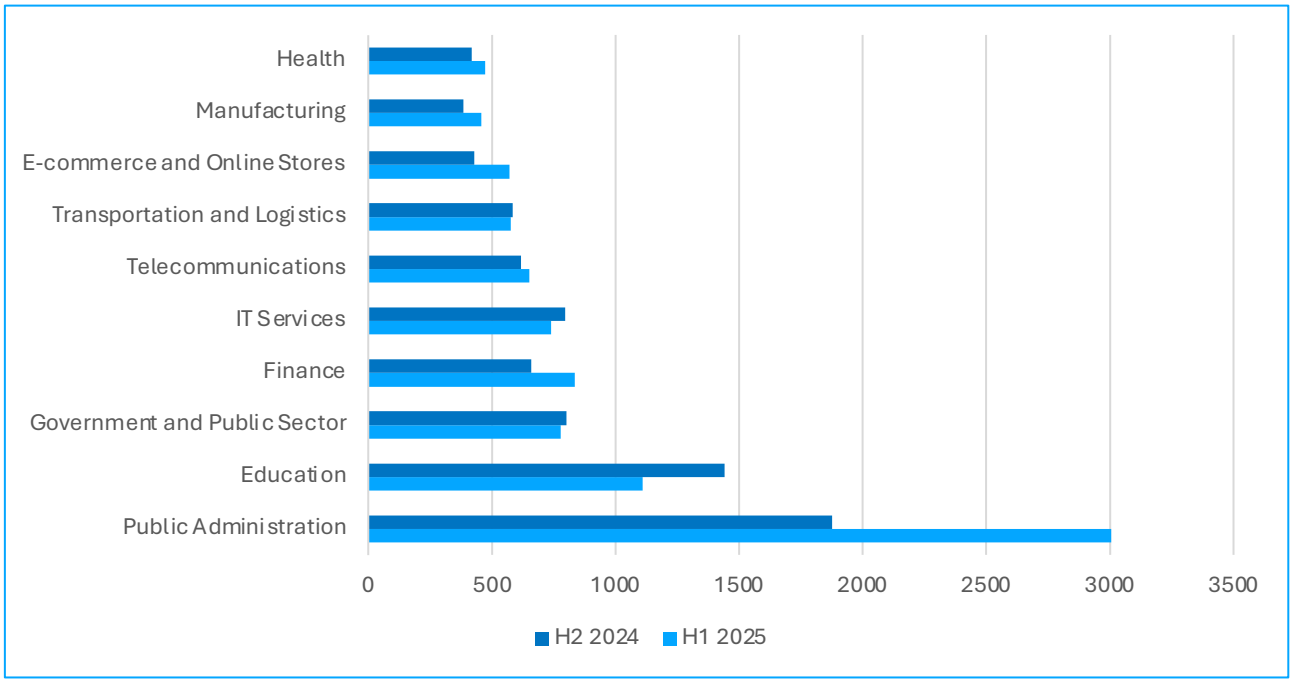


Figure 1 | Sectors most affected by cyberattacks in the first half of 2025

Meanwhile, the overall temporal distribution of recorded cyberattacks showed a steady rise during the last quarter of 2024, remained mostly stable in Q1 2025, and declined sharply in April. The trend has stabilized since May, although attack volumes are expected to rise again throughout the year.

Chronological evolution of cyberattacks

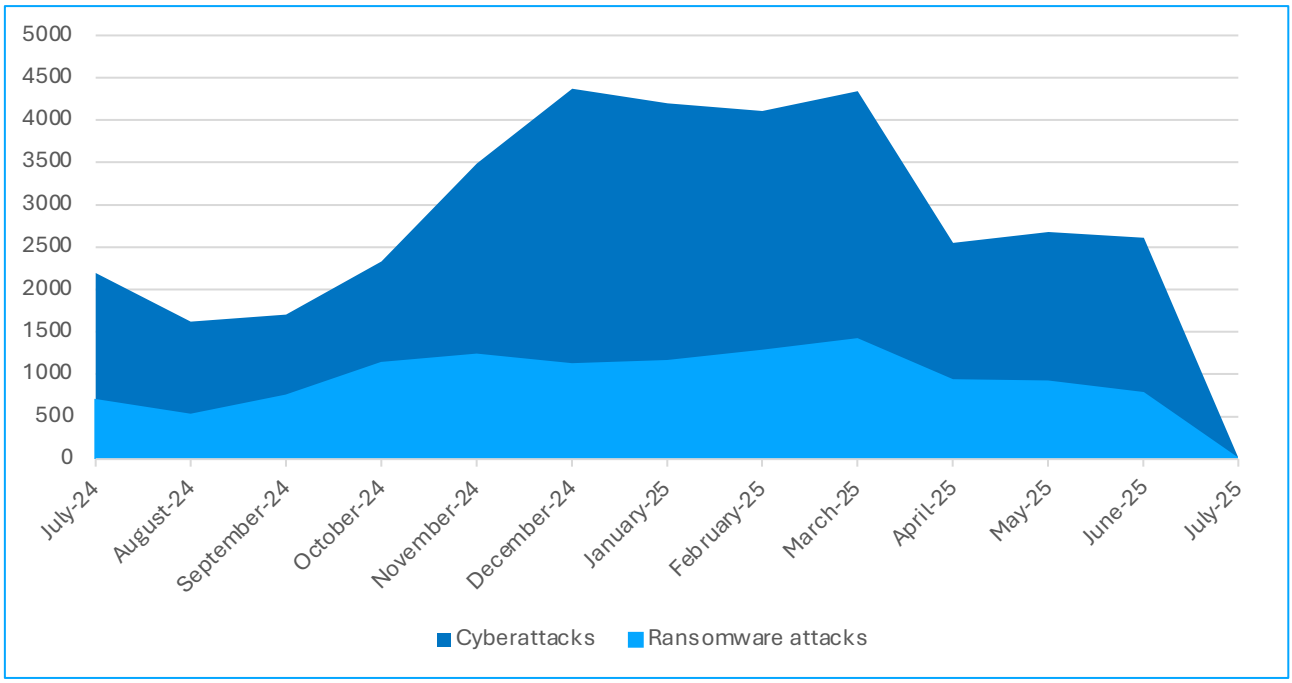


Figure 2 | Chronological distribution of cyberattacks registered from Q2 2024 to 2025

Continuing with the analysis of impact distribution, not only is there a clear variation across sectors, but a distinct trend can also be observed in certain countries that have recorded significantly higher volumes of cyberattacks during the first half of 2025:

- **United States:** With **4,046 attacks**, the U.S. tops the ranking of most affected countries, highlighting its strategic and economic importance. This figure marks a **35.6% increase compared to 202**4.
- **India:** Despite being recently targeted by multiple threat actors and involved in armed conflicts, India recorded **1,644 attacks**—down nearly 21% from the previous semester.
- **Israel:** In 2025, Israel registered **1,637 cyberattacks**, placing it as the third most frequently targeted country worldwide.

This surge is largely attributed to the ongoing conflict with Palestine, which continues to drive threat actor activity against Israeli assets.

- **France:** Representing **4% of total global attacks with 921 incidents**, France has increased its cyber defense readiness through simulated drills inspired by the Russia–Ukraine conflict.
- **Ukraine:** With **768 recorded attacks**, Ukraine continues to face cyber threats linked to regional conflict—including cyberespionage and sabotage of critical infrastructure. However, its current volume of attacks is down **36% compared to the previous semester**, indicating that defensive and counterattack strategies may be proving effective.

Distribution of cyberattacks by country (H1 2025)

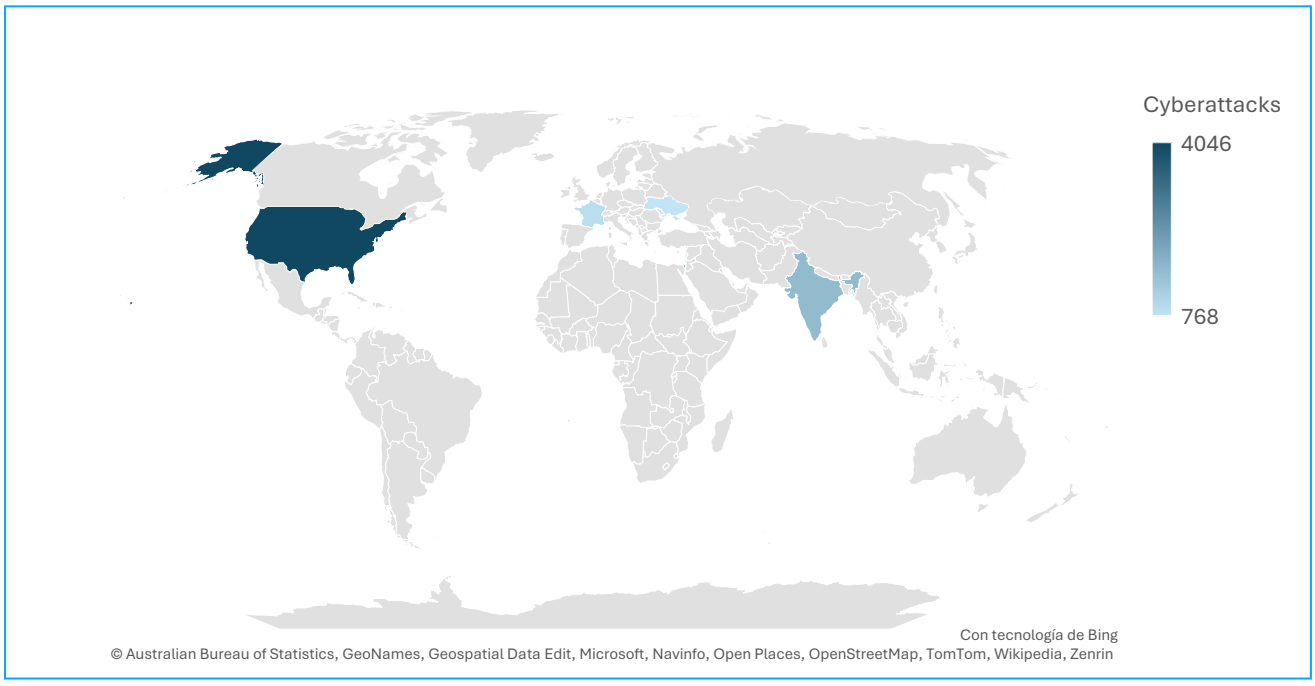


Figure 3 | Geographical distribution of cyberattack impact in the first half of 2025

The geographical distribution of cyberattacks places the United States at the epicenter, driven by its ongoing conflict with China over trade, technology, and territorial influence, along with its enduring rivalry with Russia—home to some of the world's most advanced APT groups. Meanwhile, other major powers remain in the crosshairs of cyber threats, as long as current conflicts persist. The regional spread of these attacks continues to reflect the broader geopolitical landscape as it increasingly plays out in cyberspace.


Global Threat
Landscape

3. Global Threat Landscape

The first half of 2025 has been defined by an evolving cyberthreat landscape, marked by increased sophistication and a growing focus on exploiting critical vulnerabilities. Although many tactics observed in 2024 remain in use, threat actors have become increasingly specialized, demonstrating a deeper focus on refining their techniques and targeting strategies.

High-impact cyber incidents, the rise of new access and persistence techniques, and the professionalization of models such as Ransomware-as-a-Service (RaaS) all underscore a threat environment that is not only persistent but rapidly adapting. Meanwhile, underground markets remain active, though with less public visibility due to their migration to more private channels.

3.1 Major Cyber Incidents and Campaigns

During the first six months of 2025, the world witnessed a series of large-scale cyber incidents that compromised critical infrastructure, disrupted essential services, and affected the privacy of millions. These events highlighted not only technical vulnerabilities but also deficiencies in risk management, incident response, and preparedness for complex threats.

NTT DATA's Cyber Threat Intelligence Department has documented some of the most significant cyber incidents of H1 2025, selected for their representative value in illustrating the main threats observed during this period. The ranking includes confirmed cases of ransomware, data breaches, phishing campaigns, DDoS attacks, malware, and destructive cyberattacks. It aims to demonstrate the range of affected sectors and the evolution of malicious tactics.

Target	Technology/ Sector	Attacker	Targeted Country	Attacker's Country	Incident Date	URL
United Health	Health/ Personal data	Unknown	US	Unknown	01/01/2025	Source
E-commerce Platform	Web Infrastructure	Unknown	Japan	Unknown	01/01/2025	Source
Cloudflare	Network/ Infrastructure	Unknown	Global	Unknown	02/02/2025	Source
Insight Partners	Financial Services	Unknown	US	Unknown	02/19/2025	Source
Marks & Spencer	Retail	Scattered Spider	United Kingdom	Unknown	04/27/2025	Source
Synnovis	Public Health	Qilin	United Kingdom	Unknown	05/20/2025	Source
Cobb County	Local government	Qilin	US	Unknown	05/20/2025	Source
Several platforms	Online services/ passwords	Malware/ Infostealer	Global	Unknown	05/28/2025	Source
GLS (Phishing)	Logistics	Unknown	Spain	Unknown	05/31/2025	Source
Victoria's Secret	Retail/ E-commerce	Unknown	US	Unknown	06/02/2025	Source
Coinbase	Technology/BPO	Insider/ Internal Threat	India	Unknown	06/02/2025	Source
Telefónica	Telecommunications	Dedale	Peru	Unknown	06/03/2025	Source
SVT/ Bank ID	Television/ Identification systems	Unknown	Sweden	Unknown	06/11/2025	Source

Table 1 | Major security incidents in the first half of 2025

3.2 Emerging Attack Trends

In the first half of 2025, the threat landscape experienced a marked acceleration. The operational maturity of ransomware groups, the adoption of offensive AI, the industrialization of initial access, and the systematic exploitation of vulnerabilities have given rise to a more agile, opaque, and unpredictable cybercriminal ecosystem.

In this context, the following technical and operational trends have defined cyber activity in the first half of the year:

3.2.1 Widespread Use of Access Brokers and Offensive AI

Initial Access Brokers (IABs) have cemented their role as key enablers of ransomware and exfiltration operations. Their listings have grown by 15%, featuring access to technologies such as Ivanti Connect Secure, Fortinet FortiOS, and Palo Alto appliances (Group-IB, 2025).

These access credentials are sold at prices ranging from $300 to $5,000. Simultaneously, AI-powered tools are being leveraged to automate the reconnaissance of exposed attack surfaces, providing both access brokers and APT groups with real-time intelligence on vulnerable assets.

3.2.2 Ransomware Professionalization: Alliances, Reorganization, and Specialization

The Ransomware-as-a-Service (RaaS) model has reached an unprecedented level of operational maturity. Groups such as Cl0p, Akira, Qilin, and RansomHub led most campaigns, accounting for more than 1,200 attacks during the semester. One notable trend is the widespread use of legitimate tools before encryption—a tactic known as "Living off the Land"—which enables attackers to maintain persistence and avoid detection by traditional antivirus solutions.

Additionally, an unprecedented development has emerged within the ransomware ecosystem: the absorption of affiliates and the reuse of infrastructure by emerging groups, who are capitalizing on the operational and technical remnants of dismantled groups like LockBit and Alphv.

This recycling effort is supported by intelligence gathered from leaked Telegram channels and underground forums.

At the same time, alliances are forming between actors with specialized skills, even among groups from geopolitically opposed regions. These partnerships facilitate profit sharing, outsourcing of specific attack phases, and optimized resource allocation, resembling corporate business structures.

Opposing dynamics have also emerged, including infighting between groups—such as the shutdown of Black Basta's operations in April 2025 following internal leaks. Meanwhile, public disputes among malicious actors have surfaced on platforms like X over the control of leaked data targets, highlighting an increasingly competitive and fragmented threat ecosystem (Group-IB, 2025).

3.2.3 AI-Driven Fraud Automation: Impersonation and Targeted Attacks

In the first half of 2025, the use of AI in fraud, impersonation, and social engineering campaigns became firmly established, enabling more personalized, credible, and automated attacks. AI is being used to generate fake identities, synthetic voices, and spear phishing emails based on leaked data or public profile information. It is also automating entire stages of attacks targeting the financial and government sectors (Hitachi Cyber, 2025; KrakenLabs, 2025).

At the same time, a growing ecosystem of AI-powered offensive tools is driving down the cost and complexity of cybercrime. These include text generators such as FraudGPT and WormGPT for composing fraudulent communications; voice cloning tools (e.g., ElevenLabs, Voicemy.ai) and video deepfake software (e.g., DeepFaceLab, Faceswap) used to bypass identity verification; and phishing kits such as EvilProxy and Robin Banks, which offer Adversary-in-the-Middle (AITM) capabilities for stealing credentials protected by multi-factor authentication (MFA). AI-driven social bots have also been observed on Telegram and other platforms, simulating technical support conversations to extract sensitive data.

These capabilities are reducing the technical threshold required to engage in cybercrime, actors with no prior experience to launch complex and targeted campaigns—intensifying the threat landscape for both enterprises and governments.

3.2.4 Malware-as-a-Service: The Rise of Infostealers Like Lumma and RedLine

The MaaS (Malware-as-a-Service) market has been led by Lumma Stealer and RedLine, with over 3 million stolen credentials recorded per day (MTI, MDC & MSE, 2025). Lumma has been implicated in several high-volume data exfiltration campaigns, with a focus on session cookies, crypto wallets, browser-stored credentials, and VPN configuration files.

Although Europol and Microsoft disrupted its infrastructure in May, it quickly resurfaced through forks and rebranding of its command-and-control (C2) servers. In addition, attackers have shifted distribution to private channels such as Discord and Telegram, further complicating detection and attribution.

3.2.5 Target Selection and Industry-Specific Exploitation

Threat actors are refining their campaigns based on the targeted industry. Sectors such as finance, education, and public administration have faced the majority of attacks due to their low security thresholds, high digital dependence, and potential reputational damage (CERT-EU, 2025). This segmentation not only improves success rates but also enables threat actors to maximize extortion pressure by tailoring language, stolen documentation, and communication techniques.

3.3 Global Statistics on Security Incidents, Attack Types, and Threat Actors Involved

According to NTT DATA's Cyber Threat Intelligence Department, cyberattacks maintained a consistent pace during the first half of 2025 and exhibited a clear evolution in targeting strategies, technical sophistication, and sector-specific segmentation.

Below is a summary of key statistics and observed trends during this period:

- **Ransomware:** Remains the top global threat. The number of attacks **increased by approximately 32% compared to the previous half-year.** Over 1,200 incidents were attributed to groups such as Akira, Cl0p, and RansomHub, noted for their industry-specific targeting and systematic use of double extortion techniques and legitimate tools prior to encryption (CrowdStrike, 2025; KrakenLabs, 2025).
- **Phishing and Vishing:** There has been a significant rise in AI-assisted vishing attacks, especially since late 2024. Campaigns have become more realistic, using voice cloning technologies and synthetic profiles to conduct targeted fraud, particularly in financial and human resources environments (Group-IB, 2025; Hitachi Cyber, 2025).
- **Data breaches:** In the first half of the year, more than 1,000 significant breaches have been reported, many of which have affected organizations in the financial, retail, and public administration sectors. The upward trend observed in 2024 has continued, with threat actors leveraging increasingly sophisticated tools for data exfiltration and monetization (World Economic Forum, 2025; CyberArk, 2025).
- **DDoS Attacks:** While the global volume of attacks has declined slightly, their sophistication has increased, often in combination with extortion tactics. Selective campaigns targeting critical infrastructure and payment platforms have become a recurring method of pressure (CERT-EU, 2025).
- **AI-Driven Attacks:** The offensive use of artificial intelligence has become a cross-cutting tactic throughout the cyberattack lifecycle. Threat actors are now applying AI at multiple stages — from automating reconnaissance to generating malicious emails and synthetic identities. This approach has significantly enhanced the credibility, scale, and effectiveness of phishing, impersonation, and multivector campaigns (KrakenLabs, 2025; CrowdStrike, 2025).

Estimated percentage increase in attacks by category (H1 2025)

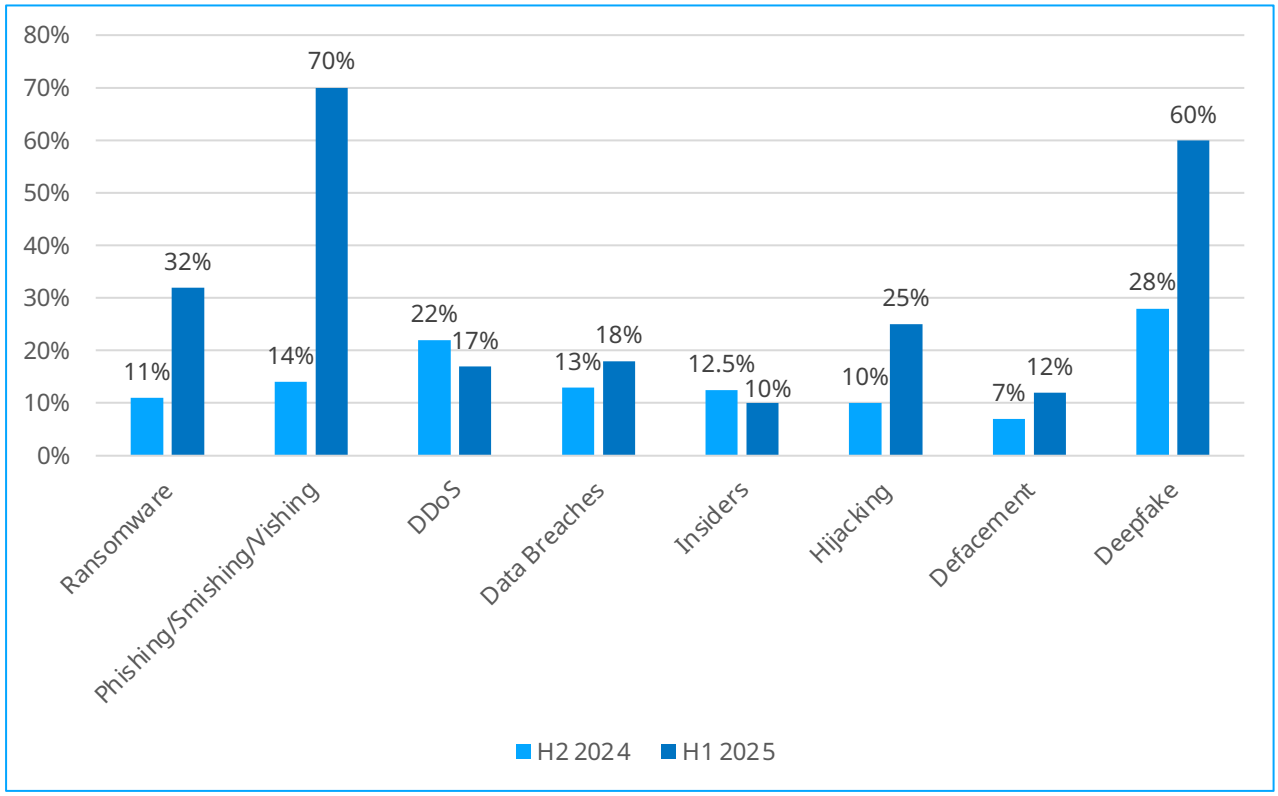


Figure 4 | Percentage increase in attack volume by category compared to H2 2024

Although categories such as phishing, smishing, and deepfakes recorded higher percentage increases compared to the second half of 2024, this does not indicate that they have surpassed well-established threats like ransomware in absolute volume.

These figures illustrate the evolving threat landscape, where emerging techniques are expanding rapidly. Nevertheless, **ransomware remains the dominant threat in terms of operational impact, global frequency, and profitability for malicious actors.**

3.4 Cost of Cyberattacks for Businesses

In the first half of 2025, the costs associated with cyberattacks have continued on an upward trajectory, driven by both the increasing frequency and sophistication of incidents, as well as the operational impact they cause. The latest estimates place the global **cost of cybercrime at a record high of $10.5 trillion annually**, with **sustained growth potentially reaching $12 to $15 trillion by the end of the year** if current levels of malicious activity persist (Cybersecurity Ventures, 2025).

Specifically, the most significant expenses for organizations during this semester have been:

- **Business disruptions**, topping the economic impact with an **estimated average of $13.2 trillion**, due to interruptions in supply chains, payment platforms, and critical services.
- **"Cyber hardening" costs**, including investments in detection, response, and training, have risen to **$10.8 trillion**, pressured by the rapid adoption of AI-based technologies and multicloud environments.
- **Ransom payments** to ransomware groups have reached **$6.3 trillion**, with a notable increase in demands exceeding $5 million per incident, especially in the healthcare, manufacturing, and transportation sectors.

- **Economic and legal penalties stemming from incidents and data breaches** have **surpassed $7.14 trillion**, partly due to stricter regulations in regions such as the EU, the UK, and Asia-Pacific (Gov.UK, 2025; Stamford, 2024).

Compared to the end of 2024, there has been an **estimated 15% increase in global cybersecurity costs,** particularly concentrated in sectors such as critical infrastructure and highly interconnected processes.

Targeted campaigns during key calendar periods have also contributed to this cost escalation, with peaks of up to 40% additional containment expenses in affected companies during December and January (Stamford, 2024; Tamzid, 2025).

Yearly evolution of estimated cybersecurity costs from 2020 to 2025

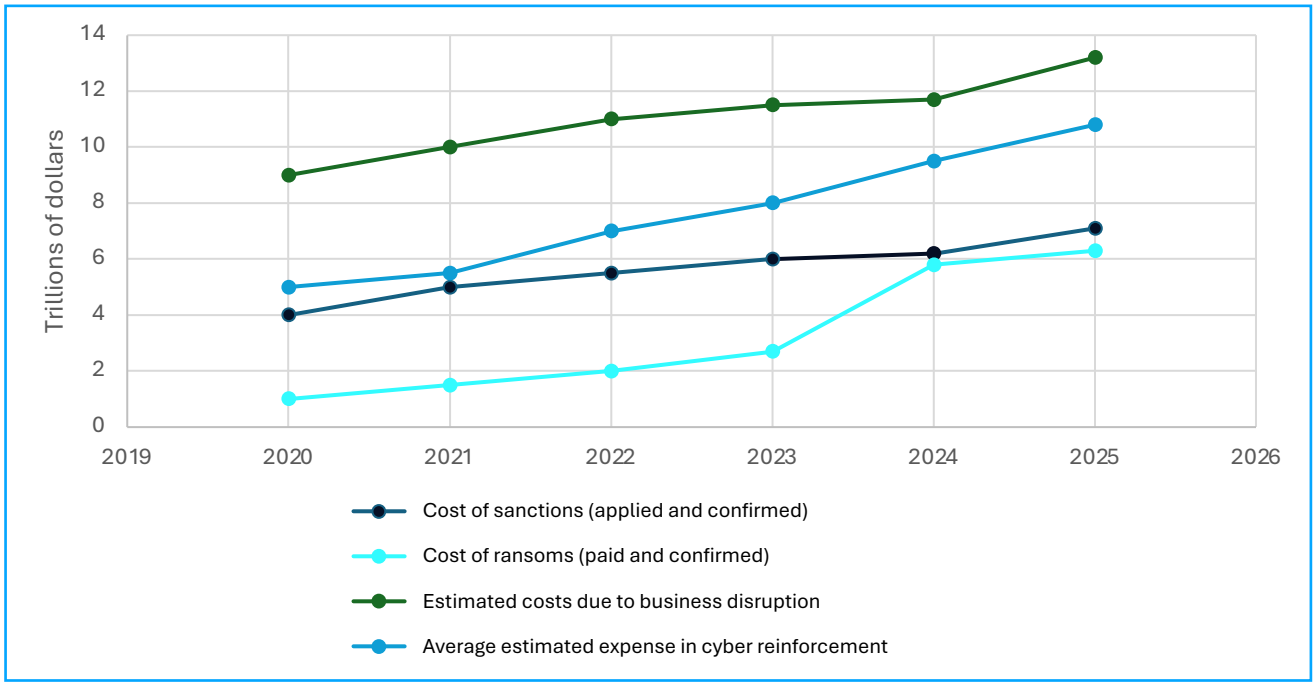


Figure 5 | Yearly comparative evolution of estimated cybersecurity costs (2020–2025), broken down by penalties, ransoms, business disruptions, and cyber hardening

The chart in this section has been updated to reflect consolidated data from the second half of 2024 and the first half of 2025, based on official sources and publications from international vendors. During the drafting of the previous report, the 2024 figures were estimated within a partial-year context and still subject to revision. With the publication in 2025 of standardized and reliable metrics on the economic cost of cybercrime, the initial discrepancies have been corrected, providing a more accurate picture of the actual impact.

Legal Framework and Cybersecurity-Related Arrests

4. Legal Framework and Cybersecurity-Related Arrests

At **NTT DATA's Cyber Threat Intelligence Department**, it is considered essential to analyze the security measures implemented, the cybersecurity laws enacted, and the arrests made by law enforcement agencies worldwide during the first half of 2025.

This analysis evaluates the level of commitment by different countries to regulating and controlling current and emerging technologies, as well as their responsible application. It also highlights the joint effort of legislative, judicial, and defense bodies to address corporate security gaps and combat illicit activities in cyberspace.

4.1. Key Cybersecurity Laws

In the first half of 2025, the legal and regulatory framework for cybersecurity continued to evolve globally and nationally. Although some documents are still in the implementation or review phase, significant progress is already visible in terms of legislative harmonization across cyberspace. Key developments include:

Region	Regulation	Institution	References
Africa	The Cyber Security Act, 2025 The Cyber Crime Act, 2025	Parliament of Zambia	National Assembly of Zambia
North America	Insure Cybersecurity Act of 2025	US National Telecommunications and Information Administration	USA Government
	HIPAA Privacy Rule (2025 Updates)	US Department of Health & Human Services	Access Partnership
South America	Cybersecurity Framework Law No. 21,663	Ministry of the Interior and Public Security of Chile	National Congress Library of Chile
	Federal Plan for Cybercrime Prevention and Strategic Cybersecurity Management (2025 - 2027)	Ministry of National Security of Argentina	Official Gazette of the Argentine Republic
Asia	Regulation on Network Data Security Management (New Draft Amendments)	State Council of the People's Republic of China	China Briefing
	Digital Technology Law (DTI Law – Approved in June)	Ministry of Science and Technology of Vietnam	Vietnam Briefing
	Critical Infrastructure Protection Bill (Computer Systems)	Legislative Council of Hong Kong	Legislative Council of Hong Kong
	Anti-Fraud Protection Bill	Parliament of Singapore	Singapore Government
	Active Cyber Defense Law (ACD – Approved in May)	National Diet of Japan	The House of Representatives, Japan
Europe	Cyber Resilience Regulation Cyber Resilience Act (CRA)	European Commission	European Commission
	Artificial Intelligence Regulations	European Union	European Council
	Regulation (EU) 2025/37	European Union	European Union
	Cybersolidarity Regulations (Cyber Solidarity Act)	European Union	European Union
	Directive NIS2	European Union	Directive NIS2
	Digital Operational Resilience Act (DORA)	European Commission/ European Union Financial Authorities	Field Fisher
	EU Cybersecurity Act (in review with new certification)	EU Agency for Cybersecurity (ENISA)	Field Fisher
	Spanish Law on Coordination and Governance of Cybersecurity	Government of Spain/ INCIBE Spain	Ministry of the Interior
Oceania	Cyber Security (Ransomware Payment Reporting) Rules 2025	Government of Australia	Federal Register of Legislation

Table 2 | Laws approved or enforced in the first half of 2025

These legal provisions—both national and European—seek to improve resilience against digital risks, strengthen the protection of data and critical infrastructure, and establish a more robust risk assessment framework. In particular, the NIS2 Directive and the DORA Regulation represent a step toward harmonizing digital security standards among EU member states.

4.2 Major Cybersecurity-Related Arrests

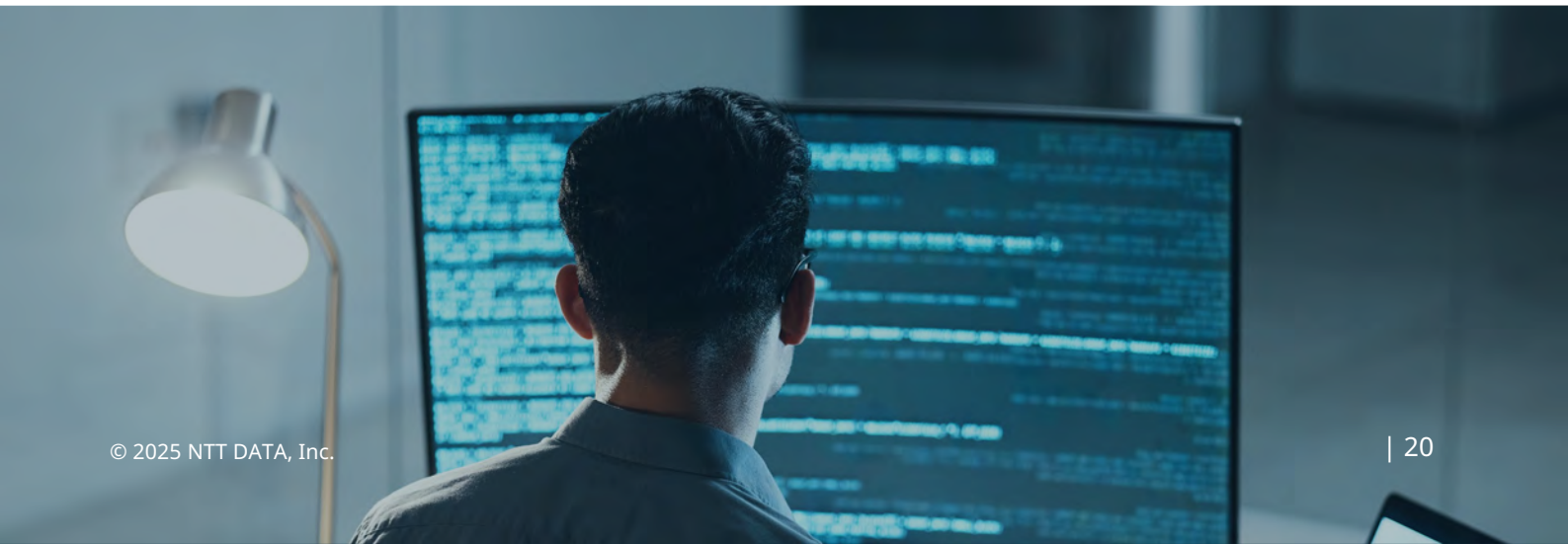
During the first half of 2025, several international operations were launched to dismantle cybercriminal networks and disrupt the activities of ransomware groups, disinformation campaigns, and advanced persistent threats (APTs).

These efforts, often driven by collaborations between law enforcement agencies, government bodies, and private organizations, have succeeded in disrupting the activities of highly organized actors with transnational presence.

The table below provides a summary of the main operations carried out during this period:

Operation	Threat Sector Group	Law Enforcement Bodies	References
Operation against Lumma Stealer	Multiple threat vectors	U.S. Department of Justice Europol Microsoft's Digital Crimes Unit (DCU)	Justice Government
Phobos	Phobos Ransomware	Europol Interpol Local agencies in various countries	United States Attorney's Office
Phobos Aetor	8Base Ransomware	Europol Police Lieutenant General Trairong Phiwphan Local law enforcement agencies	Dark Web Informer
Sindoor	AnonSec and actors linked to disinformation and terrorism	Government of India Military intelligence	Clarion India
RapTor	Dark web vendors	Europol Police authorities in Austria, Brazil, Germany, and others	Europol
Operation secure	Malicious infrastructure hosting infostealers	Interpol Local agencies in various countries	Interpol
Operation Deep sentinel	Archetyp Market	German police authorities Europol Eurojust	Europol
Operation against BreachForums	BreachForums leadership	Cybercrime Brigade (BL2C) (Paris) FBI	USA Attorney's Office Le Parisien

Table 3 | Major cybercriminal takedown operations carried out in 2025



In addition to these globally coordinated police operations, there has been a notable rise in **internal leaks and the exposure of known ransomware groups** by other disreputable actors. One of the most prominent examples is the Telegram channel "**GangExposed**," managed by the group **CactusPulse**. This channel has gained notoriety for collecting, verifying, and publishing operational intelligence about members of highly destructive groups such as **Conti, Trickbot, and Black Basta**.

In April and May, GangExposed released images and profiles of 15 Conti members, including the group's alleged chief negotiator, Arkady Valentinovich Bondarenko. It also revealed the identity of an actor known as "8G," reportedly one of Black Basta's main coordinators responsible for deployment operations, antivirus evasion, target selection, and cryptocurrency payments.

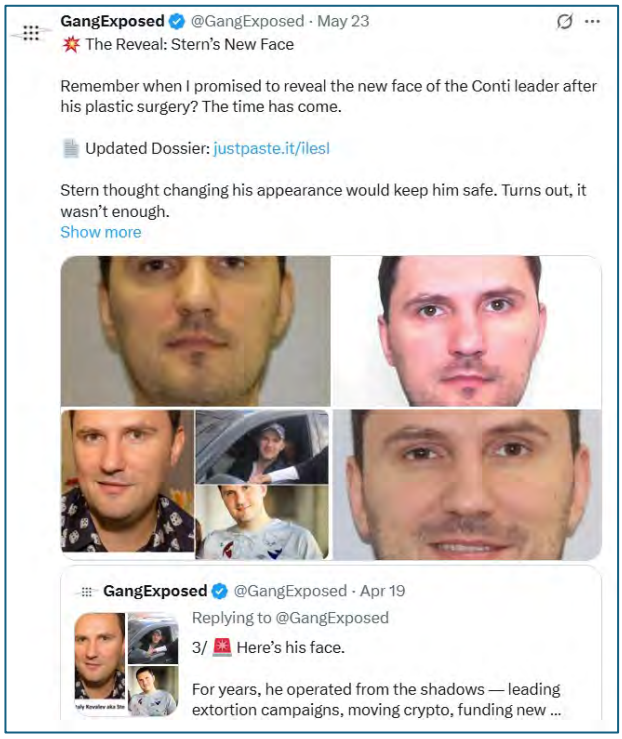
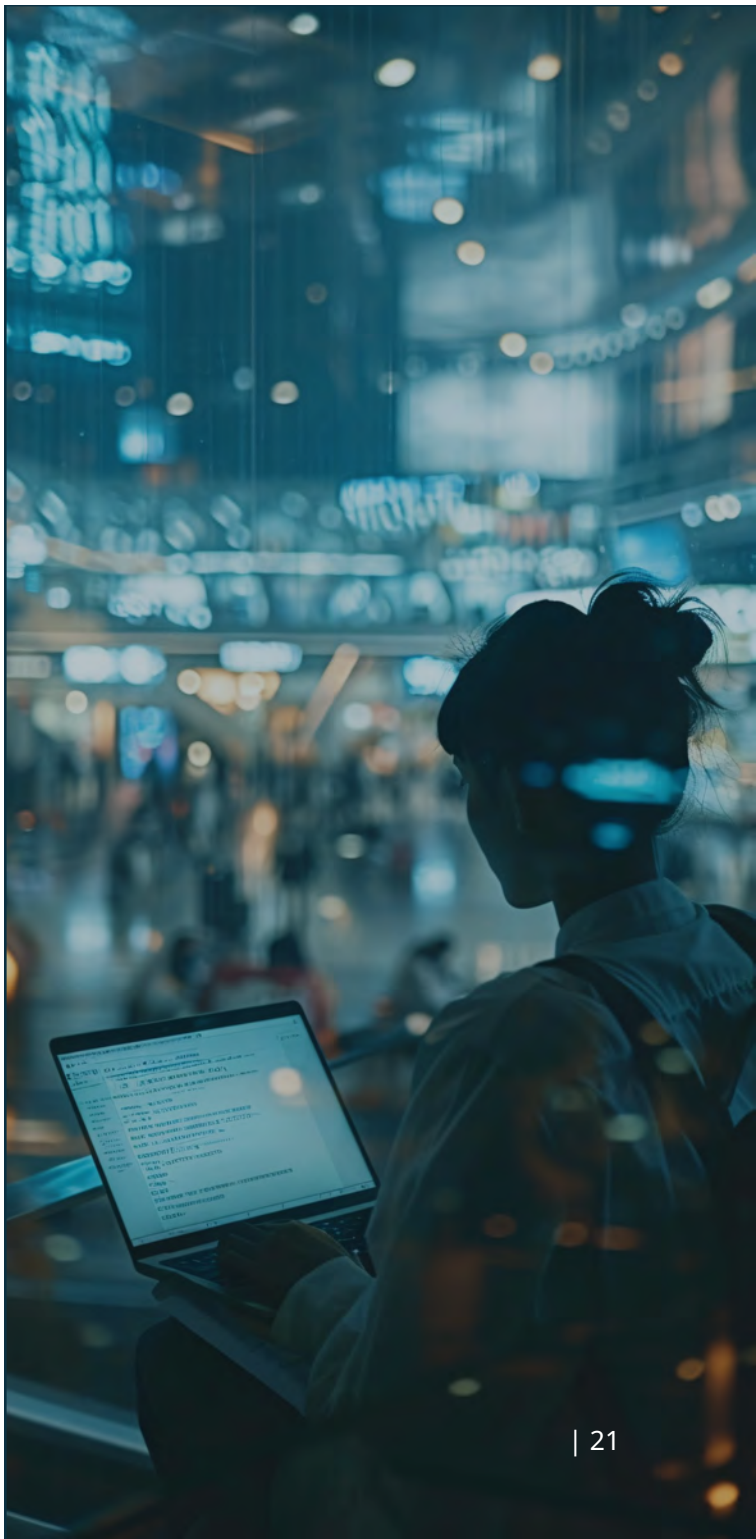


Illustration 1 | Exhibition on the X platform by the GangExposed group

The publications on this channel have included leaked internal chats, evidence of payments, social engineering strategies used to contact targets, and procedure manuals for malicious operations. This activity marks an unprecedented form of intelligence warfare within the cybercriminal landscape.

Motivated by retaliation, government rewards, or internal schisms, some groups, or individuals are disclosing confidential information and hierarchical structures of their former allies.

This trend is not only assisting law enforcement agencies in identifying and prosecuting high-ranking cybercrime leaders but also destabilizing criminal organizations once believed to be shielded by anonymity and decentralization.



Dark Web Insights

5. Dark Web Insights

In the first half of 2025, the dark web remained one of the primary ecosystems for cybercriminal activity. This includes the buying and selling of stolen data, unauthorized system access, credentials, malware tools, and hacking services under the Crime-as-a-Service (CaaS) model. This period was marked by a deep reconfiguration of both markets and underground forums, largely driven by the downfall of BreachForums.

5.1 The Shutdown of BreachForums: Impact and Implications

The shutdown of BreachForums in April 2025, its attempted sale by one of the administrators in June, and the arrest of its most prominent figures, such as IntelBroker, marked a turning point.

This forum had been one of the leading platforms for the exchange of stolen databases, compromised accesses, infostealer logs, and offensive tools. Its disappearance created both a logistical and symbolic void in the cybercriminal ecosystem. The collapse triggered **user migration** to private forums, encrypted channels, and established marketplaces. This shift has led to greater decentralization of malicious activity and the growth of specialized platforms.

5.2 Underground Forums Active in 2025

- Following the shutdown of BreachForums, various alternative forums have emerged as key hubs for cybercriminal activity:
- **Dread:** A Reddit-like forum on the dark web, used for doxing, leaks, and technical discussions.
- **XSS.is:** Considered the "elite forum" for Russian-speaking actors; some members have been linked to attacks on critical infrastructure in Eastern Europe.
- **Dark Forums:** With **over 12,767 registered users as of April 2025**, it has grown rapidly following BreachForums' disappearance. It hosts a highly active community around malware, infostealers, and account cracking. It is also one of the few forums with an educational section featuring detailed malicious scripting guides.
- **Exploit.in:** Established over 15 years ago, it is the longest-standing forum. Zero-day vulnerabilities are often published here before receiving CVE identifiers. **In February 2025, a zero-day affecting Palo Alto Networks was disclosed.**
- **Nulled:** Focused on credential sharing, cracking tools, and large-scale leaks.
- **Sinister.ly:** Blends technical content with social and hacker culture forums, attracting younger audiences. One of the most active hubs where Python-based tools for automating phishing are widely discussed.
- **Cracked.io:** A hybrid portal combining forum and market features, specializing in online service account sales.
- **KickAss:** A newer forum that has gained traction for being a meeting point for modular malware developers. It also offers custom development services for APT groups.

These forums allow for the free exchange of tools, tutorials, vulnerabilities, and database dumps, along with tailored services.

Main publication categories on the Dark Web

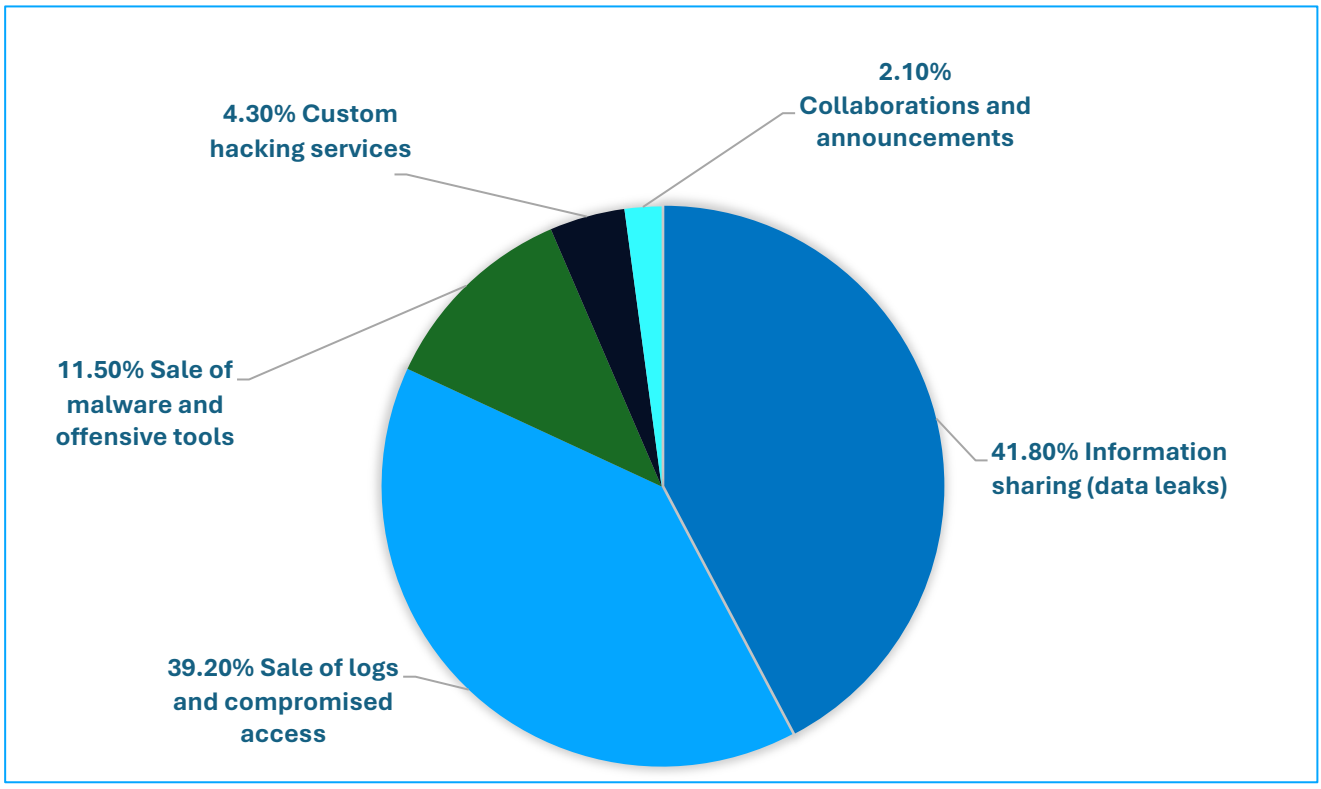


Figure 6 | Main publication categories on the Dark Web in the first half of 2025

Infostealer logs from **Lumma**, **RisePro**, and **RedLine** have maintained a dominant presence, with over **7.7 million credential sets exposed in just the first five months of 2025**. Meanwhile, dumps of compromised payment cards have reached **14.4 million, 80% of which are US-based** cards sold for prices ranging from $5 to $30.

5.3 Underground Markets Active in 2025

- **Abacus Market:** With a simple interface, it is known for selling anonymous SIM cards and identity theft kits. It gained relevance in 2025 due to a growing number of sellers specializing in custom deepfakes. By late June, the platform began experiencing **a series of service disruptions**, which may indicate that the market has been taken down after the publication of this report.
- **Russian Market:** Accepts multiple cryptocurrencies and offers **more than 150,000 stolen credentials daily**. It is particularly known for its 24-hour "log update" service that ensures the credentials are always up to date.
- **Brian's Club:** Following a major security breach in 2019, the platform resurfaced and by 2025 had regained a position **among the top three marketplaces based on card volume**. It is estimated to manage over 10 million unique active records.
- **Exodus Market:** Its strength lies in zero-day exploits and privileged access to enterprise servers in regions such as LATAM and Asia-Pacific. It operates a triple-verification reputation system for vendors.
- **Styx Market:** Specializes in tools for multichannel phishing attacks. In March 2025, it was linked to multiple distribution campaigns of Lumma and RisePro via malicious Excel macros.
- **BidenCash:** Gained popularity by freely publishing over 2 million stolen cards in criminal marketing campaigns in 2022. It continued operations through the sale of high-value credentials until it was dismantled during Operation RapTor.

Below is the **estimated distribution** of the main underground marketplaces active during the first half of 2025, based on their activity volume and relevance within the cybercriminal ecosystem:

Underground marketplaces

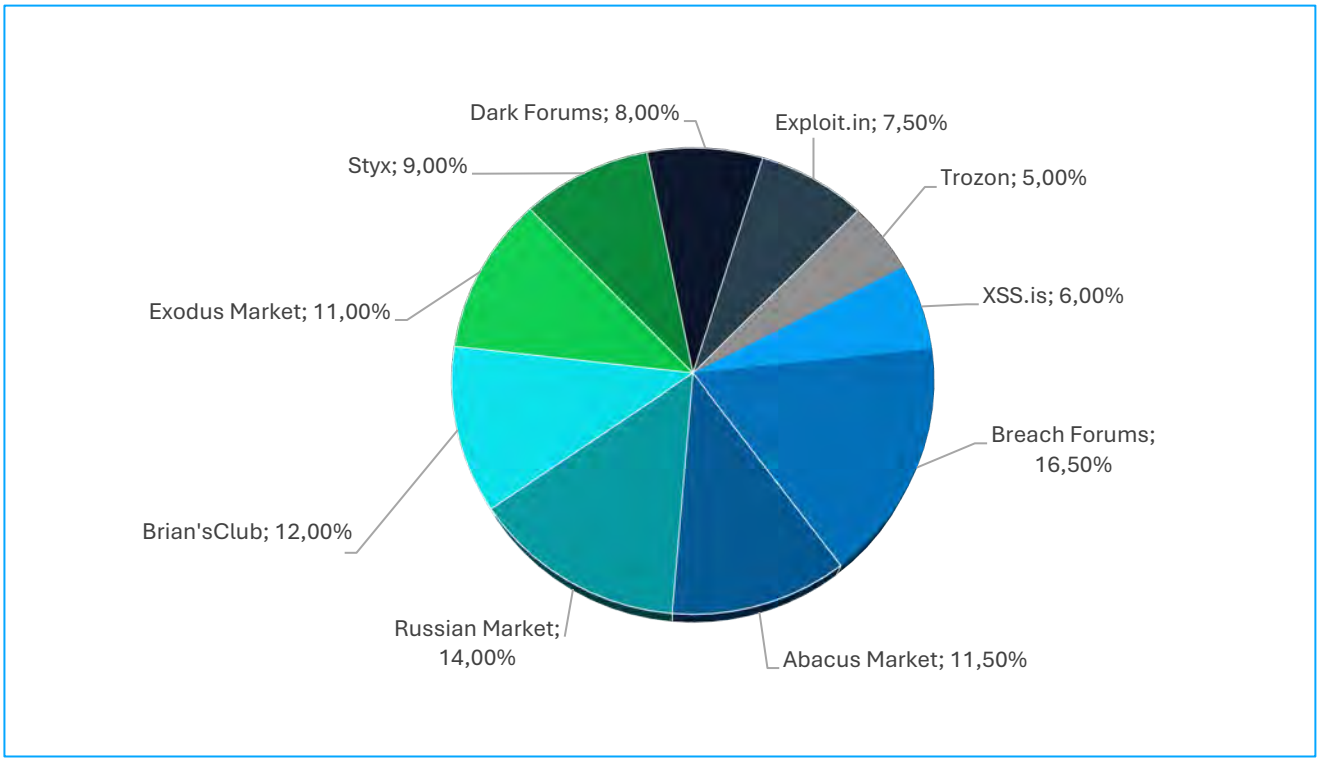


Figure 7 | Main underground marketplaces identified in the first half of 2025

In the first half of 2025, **RansomHub** gained notoriety by absorbing affiliates who had formerly collaborated with other ransomware operations. The group also expanded its footprint across underground forums and marketplaces such as **Styx** and **Brian's Club**. Similar growth patterns were seen in **groups like Storm-0953** and in networks associated with infostealing tools. Among the **15 most active threat actors between the second half of 2024 and the first half of 2025**, **nine maintained some connection to Breach Forums**.

These actors have been responsible for some of the most significant user data exfiltration attacks and breaches targeting major financial institutions in Asia (SOCRadar, 2025). Regarding operational communication, while Telegram remains a key platform, there has been a significant increase in the use of **TOX, SimpleX, and Signal**—all decentralized applications with strong end-to-end encryption. These platforms are gaining popularity due to offering greater privacy, reduced surveillance, and lower risk of law enforcement infiltration or server takedown.

Threat Actors

6. Threat Actors

In the first half of 2025, the cyber threat landscape continued to evolve, shaped by the emergence of new malicious actors, the expansion, and adaptation of ransomware groups, increasingly coordinated hacktivist campaigns, and new tactics observed in APT operations.

6.1 New Actors Identified

The ongoing diversification of threat actors in early 2025 stems not only from the emergence of new cybercriminal groups but also from the consolidation of previously lesser-known actors. This reflects a growing level of professionalization across the threat ecosystem.

Sector 16/S16

Active since January 2025, this group is possibly of Russian origin. It has been linked to other threat actors such as the **Z-Pentest** alliance and the hacktivist group **OverFlame**, consolidating attacks against critical infrastructure—particularly targeting the oil and gas sector as well as water treatment systems. The use of **unauthorized initial access techniques targeting industrial control systems and manipulation of operational parameters** has enabled attacks against organizations in various parts of the world. These include the SCADA system of oil pumps and storage tanks in Texas (U.S.), an Italian industrial water pump manufacturer, and two Spanish companies—one specializing in water treatment and another operating an APCS system at a carbon dioxide plant (Orange Cyberdefense, 2025).

LazurGroup

This France-based group emerged in January 2025 and has focused its activity in Western Europe, primarily in France and Belgium. Its operations combine advanced spear phishing tactics, remote access tools such as Cobalt Strike, and custom-built malware. Additionally, they manage distribution channels and internal coordination through Telegram. Due to its high degree of sophistication and organization, some experts classify it as a hybrid threat group — motivated by both criminal and ideological drivers.

BianLian

Active since 2022, this ransomware group has shifted to a **non-encryption-based extortion model**, relying almost exclusively on data leaks. In 2025, CISA and the FBI issued alerts about a surge in impersonation campaigns where unaffiliated actors posed as BianLian to extort executives via email. These impersonations complicate attribution, but they also reinforce the group's central role in the current threat landscape (CISA, 2025; FBI, 2025).

Rhysida

First identified in 2023, this RaaS group has intensified its activity in 2025. CISA, the FBI, and MS-ISAC updated indicators of compromise and TTPs following multiple attacks targeting education, healthcare, and government institutions. Its decentralized structure and multivector approach present a serious challenge for cyber defense teams (CISA, 2025).

Void Blizzard

Also known as Laundry Bear, this Russian-affiliated group has been active since April 2024, with its operations formally attributed in May 2025. The group primarily uses spear phishing, data exfiltration, and credential theft. Its attacks have targeted critical infrastructure in Ukraine and allied NATO countries, as well as Western governments and special forces, driven by geopolitical motivations (Microsoft Threat Intelligence, 2025; Bleeping Computer, 2025).

There is a clear trend toward **tactical diversification**, including a growing use of **Living-off-the-Land (LotL) tools**. Throughout the rest of the year, increased **collaboration between groups** is expected, along with a stronger convergence between cybercrime and cyberespionage — merging economic and strategic objectives and making attribution more difficult.

6.2 Ransomware Groups

In 2025, the ransomware threat landscape has been reshaped by the rise of new groups demonstrating rapid adaptability and increasingly aggressive tactics. At the same time, established groups have stepped up their game, refining their encryption, evasion, and extortion techniques. This evolution has placed mounting pressure on organizations across all sectors, cementing ransomware as one of the most disruptive and persistent threats in today’s digital ecosystem.

6.2.1 Emerging Groups

In the early months of 2025—especially January and February—a significant volume of ransomware activity was recorded, much of it attributed to known threat actors.

However, by March and April, analysts began detecting the emergence of new groups, some of which appear to be spin-offs from previously dismantled operations. This constant cycle of fragmentation and regrouping underscores the resilience of the ransomware-as-a-service (RaaS) model and highlights how its criminal ecosystem continues to evolve (DarkFeed, 2025).

Figure 8 | Ransomware groups detected in the first half of 2025

6.2.2 Most Active Groups

Criminal activity in this domain has continued to evolve in response to technological changes, defensive advancements, and the growing popularity of the RaaS model. These dynamics have shaped an increasingly volatile threat landscape, where technical innovation, diversified targeting, and decentralized operations play a central role in understanding current ransomware threats.

The following chart highlights the most active ransomware groups during this period and illustrates how their operations have evolved across the first half of 2025 (DarkFeed, 2025).

Top ransomware groups (H1 2025)

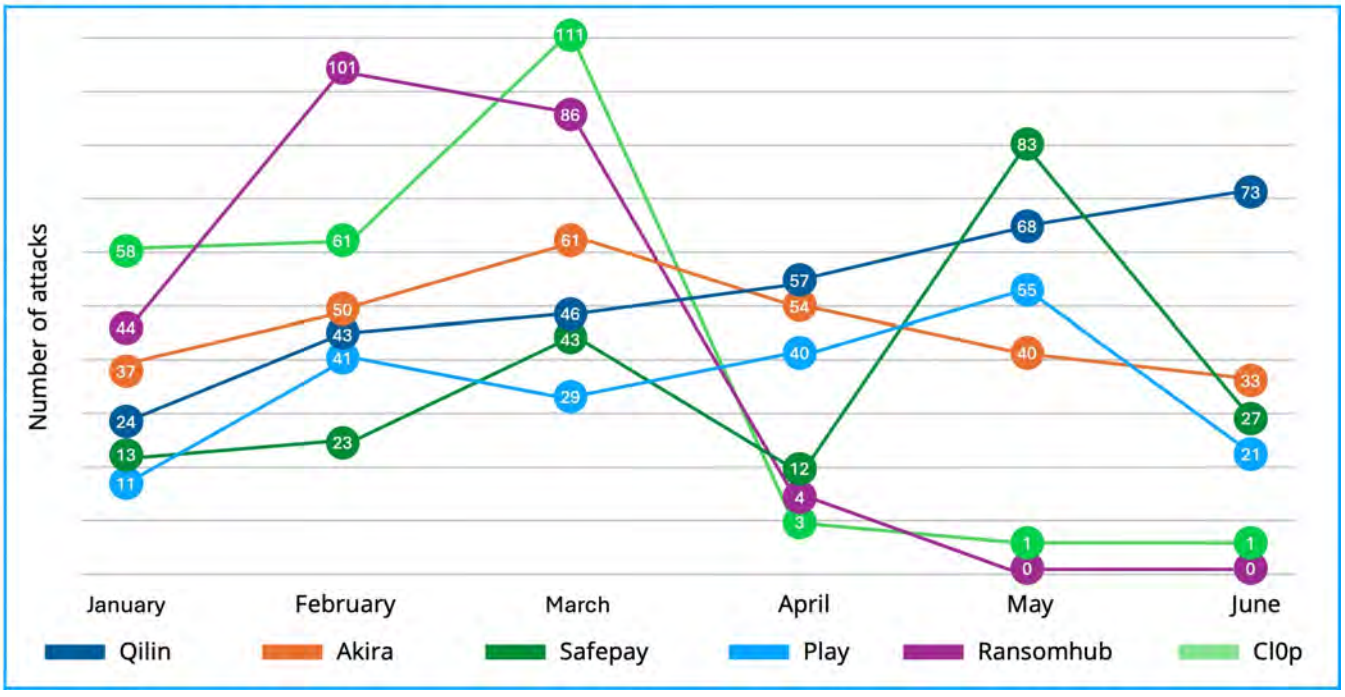


Figure 9 | Activity trends of leading ransomware groups in the first half of 2025

- **RansomHub and Cl0p:** Both groups show very similar attack distribution patterns. Cl0p entered the rankings recently, recording the highest number of ransomware attacks in March (111). Meanwhile, RansomHub, which was one of the most active groups in 2024, experienced a sharp drop in activity in April and disappeared entirely by May and June.
- **Qilin and Akira:** These two groups ranked highest by attack volume. Qilin has emerged as one of the dominant ransomware operators of 2025, fueled in part by the migration of affiliates from RansomHub and a robust technical infrastructure that enables scalable, efficient, and professionalized operations. Akira has maintained a steady and sophisticated presence, solidifying its status as a persistent group with a mature technical infrastructure.
- ***Play and Safepay:*** Play remains among the most active ransomware groups this semester. While not leading in attack volume, it has shifted toward more targeted and technically refined operations, indicating a trend toward greater campaign professionalization. Safepay, meanwhile, has focused its efforts on small and mid-sized businesses and less protected sectors, exploiting common vulnerabilities. Its gradual growth positions it as a group to watch in the second half of 2025, with expectations of rising visibility.

6.2.3 Global Impact

The operations of ransomware groups in 2025 have had a global reach, affecting organizations of all sizes and industries across multiple regions. Although the geographical distribution of attacks varies depending on the group and its strategic targets, there is a clear concentration in highly digitized countries—especially the United States—as well as in critical sectors such as healthcare, education, manufacturing, and financial services.

An analysis of the sectors most affected by ransomware over the past six months, presented in this section, shows that manufacturing continues to be the primary target for cybercriminals worldwide.

This ongoing trend reflects a combination of structural factors that make the sector especially attractive: its heavy reliance on industrial operating systems, increasing connectivity between OT and IT environments, and pressure to maintain the continuity of global supply chains. In such a context, even brief interruptions can translate into multi-million-dollar losses.

In 2025, attackers have refined their techniques, increasingly targeting SCADA systems, hypervisors, and virtualized production environments—a shift that has heightened both the sophistication and impact of ransomware attacks. The following chart illustrates the sectors most affected by ransomware in the first half of 2025, highlighting the continued prominence of the manufacturing sector:

Ransomware attacks by sector (H1 2025)

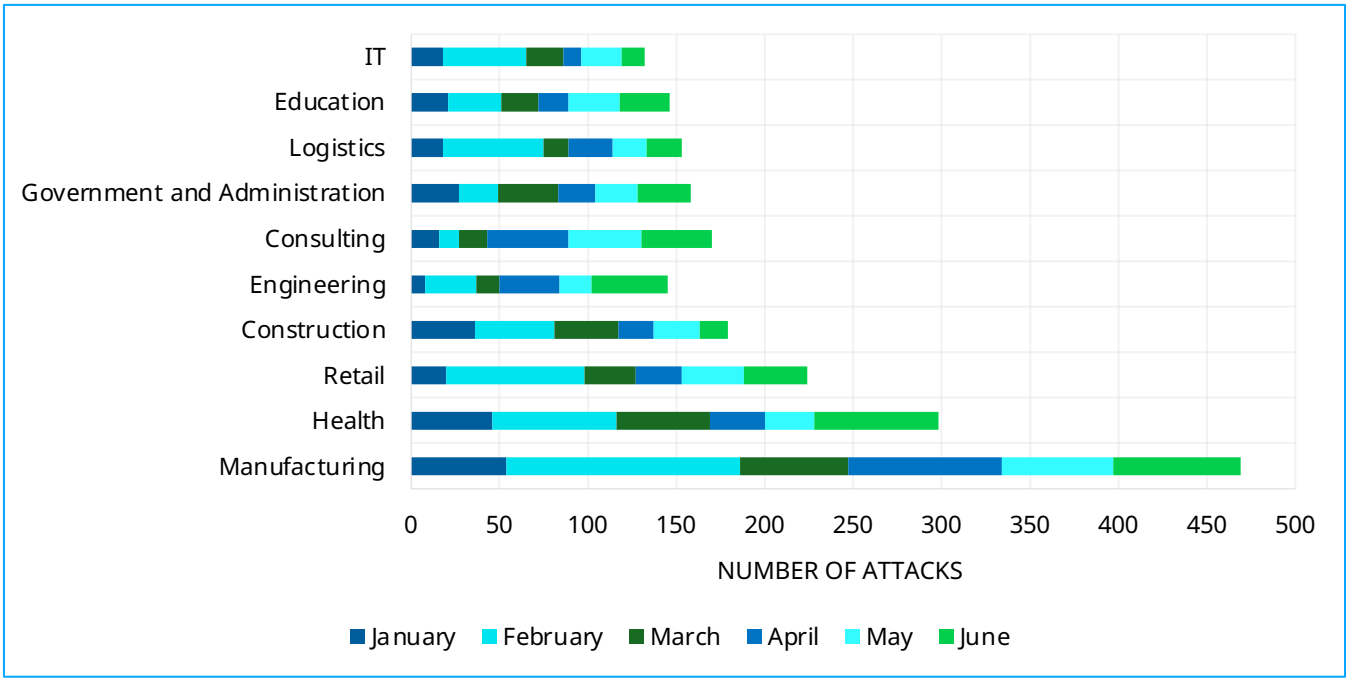


Figure 10 | Most targeted sectors by ransomware in the first half of 2025

On the other hand, the following figure shows the geographical distribution of the countries most affected by this type of attack during the same period:

Most affected countries by ransomware (H1 2025)

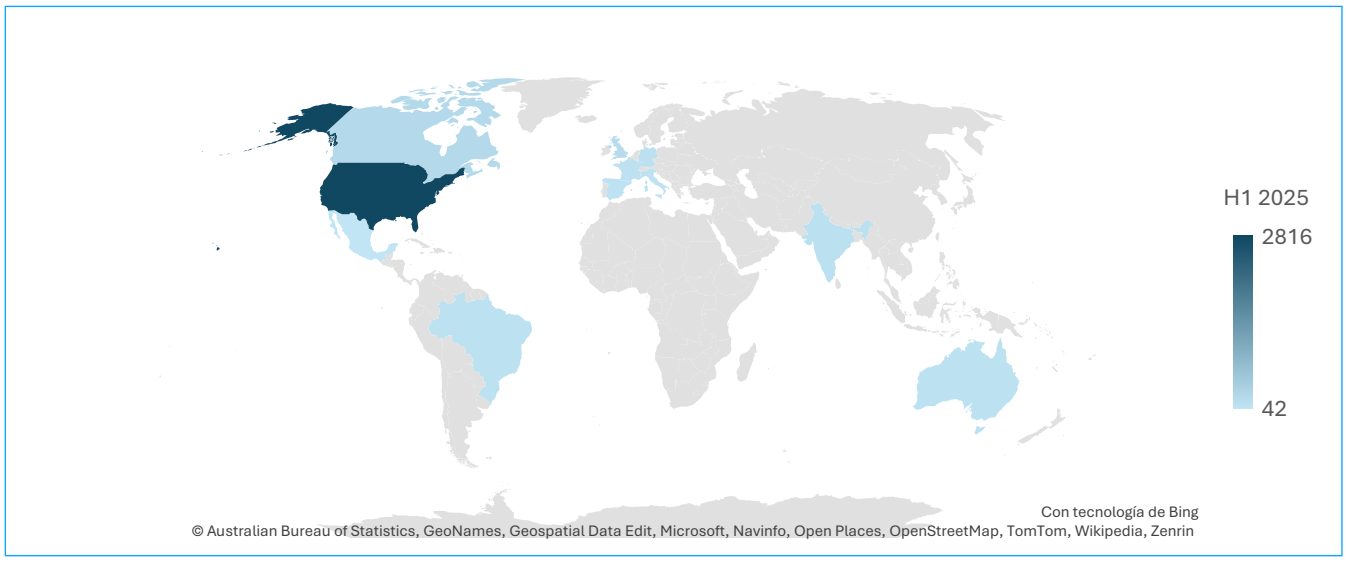


Figure 11 | Countries most affected by ransomware in the first half of 2025

As previously mentioned, the **United States** leads the ranking as the most targeted country, particularly in areas such as critical infrastructure, financial systems, and government networks. It is followed by countries like **India**, which faces significant geopolitical exposure, and nations such as the **United Kingdom** and **Germany**, where the high level of digitalization in industrial and financial sectors has increased their vulnerability.

Meanwhile, the **rise in attacks across South America** may reflect a trend toward expansion into emerging economies, where digitalization is advancing faster than cybersecurity capabilities. In this context, Brazil stands out as one of the most affected countries in the region, concentrating a significant share of attacks, especially in key sectors such as education, healthcare, logistics, and digital services.

In Central America, Mexico has experienced notable activity from groups such as Cl0p, LockBit, and Akira. These operations, primarily motivated by financial gain, have impacted sectors including finance, public administration, and manufacturing—placing Mexico as a new priority target for more sophisticated and persistent ransomware campaigns compared to the rest of the region.

This geographical distribution highlights a clear trend: ransomware actors are prioritizing countries with high technological dependency, interconnected critical infrastructure, and, in many cases, notable gaps in cyber response and resilience capabilities.

6.3 Hacktivists

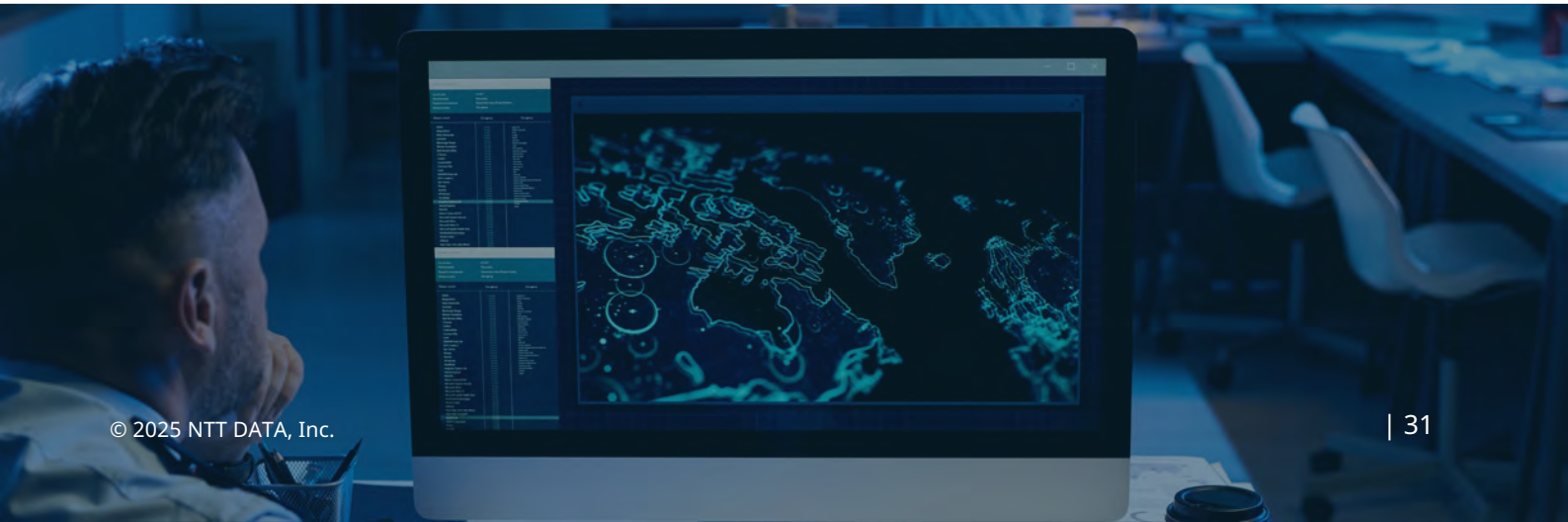
In 2025, hacktivism has seen a notable resurgence, driven by both geopolitical conflicts and global social causes.

This movement has evolved beyond the actions of individuals or small collectives, giving rise to transnational alliances of hacktivist groups that now operate with unprecedented coordination. In many cases, these groups receive tacit or covert support from states that view them as a strategic tool for exerting political pressure without resorting to direct military confrontation.

Today, the global hacktivist landscape has intensified with the formation of alliances between groups involved in geopolitical conflicts. **AnonSec**, traditionally associated with data leak campaigns, has coordinated decentralized attacks on critical infrastructure and disinformation campaigns, consolidating a collaborative network with pro-Palestinian groups such as **Mr. Hamza, Ghosts of Gaza, Handala Hack, Sylhet Gang-SG, and Moses Staff**. These actors share a strong anti-Western stance, particularly targeting the United States, Israel, and more recently, India. India, has responded with its nationalist group **Indian Cyber Force**, conducting attacks against countries like Pakistan and China.

On another front, **DieNet and DragonForce Malaysia** have also intensified operations against U.S. interests, aligning themselves with Islamic and anti-imperialist causes. In the pro-Russian camp, **NoName057(16)** has emerged as the most active group, leading DDoS campaigns against Ukraine and its allies. This group collaborates with others such as **Killnet and Anonymous Sudan** to target government, financial, and transportation sites across Europe.

The growing coordination among these groups reveals a trend toward the professionalization of hacktivism. Their operations increasingly rely on structured organizations and defined strategic goals.



Hacktivist group alliances

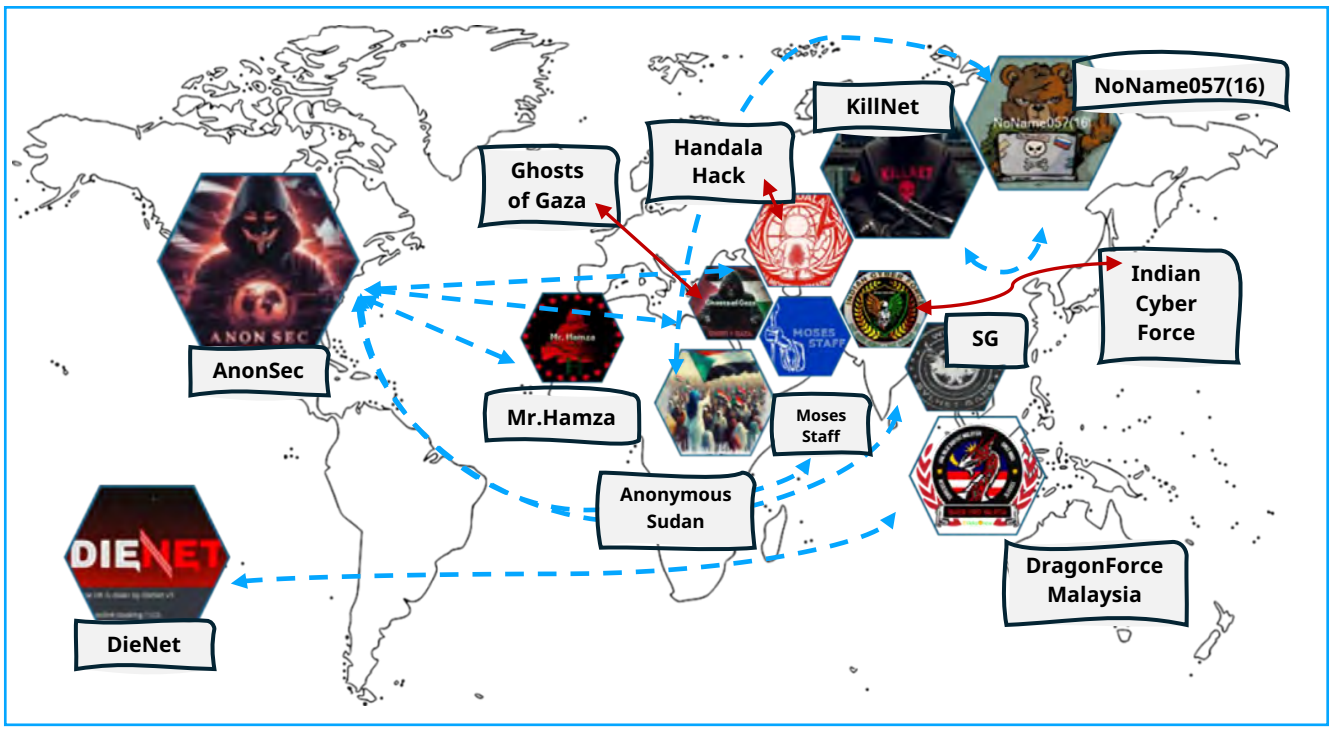
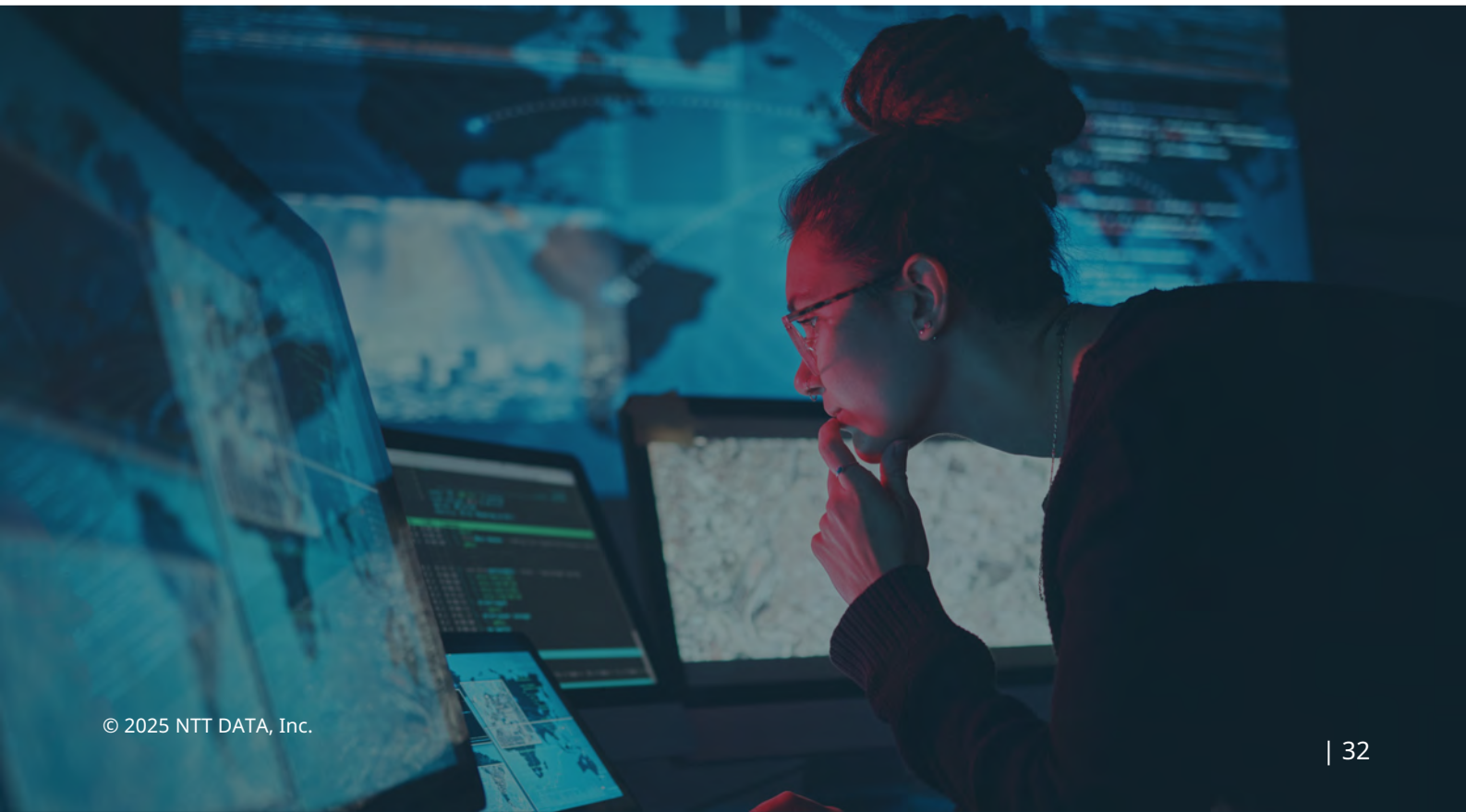


Figure 12 | Hacktivist group alliances by major geopolitical conflicts.

Initially, hacktivism was limited to symbolic demonstrations or low-impact digital protests. Today, it has evolved into a **strategic tool in the geopolitical arena**, with meticulously planned operations that often align with state or ideological interests. This transformation complicates the global cybersecurity landscape by blurring the lines between digital activism, intelligence operations, and state-driven cyberconflict.



6.4 APT

During the first half of 2025, global APT groups intensified their activity by enhancing both the technical sophistication and persistence of their campaigns. The following section outlines the main trends observed across different regions and among state-sponsored actors:

- **Russian APTs**, as noted earlier in this report, maintained an aggressive strategy focused on three fronts: diplomatic cyberespionage, disruption of critical services, and disinformation operations.

  - Sandworm deployed the new "ZEROLOT" wiper in Ukraine, aiming to disrupt energy operators by propagating through group policies in Active Directory and RMM tools.

  - Sednit (APT28) expanded its well-known **RoundPress Operation** (initially targeting Roundcube) to also affect email platforms such as Horde, Zimbra, and MDaemon, exploiting XSS and zero-day vulnerabilities. One of the most relevant was **CVE-2024-11182**, used against Ukrainian entities. Additionally, zero-day exploits such as **CVE-2024-9680** (Mozilla Firefox) and **CVE-2024-49039** (Microsoft Windows) were identified, reinforcing Sednit's offensive technical profile.

  - Gamaredon, with an exclusive focus on Ukraine, sustained a high volume of attacks, continuously updating its implants and obfuscation techniques. It introduced PteroBox, a file stealer that abuses Dropbox as an unconventional exfiltration channel.

  - Meanwhile, pro-Russian hacktivist groups like **NoName057(16)**, **Cyber Army of Russia Reborn**, and **Solntsepyok** continued conducting DDoS and data-leak campaigns targeting European media and governments. In some cases, operational convergence with APT campaigns was observed, reusing previously mentioned vulnerabilities for initial access—an indication of increasing professionalization within the hacktivist ecosystem.

- In **China, APT groups** have intensified their focus on critical infrastructure and government networks, particularly in Europe and Asia. Analysts observed consolidation of shared tooling among state-sponsored groups, along with integration of new backdoors and evasion techniques.

  - APT41 and **Earth Baku** maintained campaigns targeting OT infrastructure and networking devices, using ShadowPad and new variants like "VELVETSHELL."

  - DigitalRecyclers employed the HydroRShell backdoor in combination with KMA VPN tunneling to infiltrate European organizations and maintain covert access.

  - PerplexGoblin launched "NanoSlate," an advanced C++ malware used against Central European government institutions.

  - These **APT groups** demonstrated advanced coordination in exploiting routers, Cisco Nexus switches, and enterprise proxies to gain initial access and establish stealthy, long-term persistence within targeted networks.

- **Iranian APTs** operated along two distinct lines of effort: cyberespionage campaigns and targeted attacks specifically directed at Israeli entities.

  - MuddyWater and **Lyceum** used legitimate remote administration software to gain initial access in spear-phishing campaigns aimed at Israeli manufacturing and infrastructure sectors.

  In a coordinated operation, **BledeFeline** was observed collaborating with MuddyWater, sharing persistence mechanisms.

  - CyberToufan, an emerging actor linked to hacktivist activities, combined data leaks, system wiping, and media manipulation.

- **North Korean APTs** remain focused on diplomatic espionage and large-scale cryptocurrency theft to fund the regime.
  - **DeceptiveDevelopment** expanded its use of job lures and platforms like WeaselStore to infect blockchain developers and IT professionals.
  - **TraderTraitor** was linked to the attack on Safe{Wallet}, compromising its supply chain and resulting in the theft of over $1.5 billion in digital assets.
  - The return of **Kimsuky** and **Andariel** has been reported, with campaigns targeting South Korean and Asia-Pacific diplomatic entities.

NTT DATA's Cyber Threat Intelligence Department produced an estimate based on public reports and open-source intelligence to classify APT campaigns from the semester according to their predominant motivation.

APT activity classified by motivation in each region during the first half of 2025

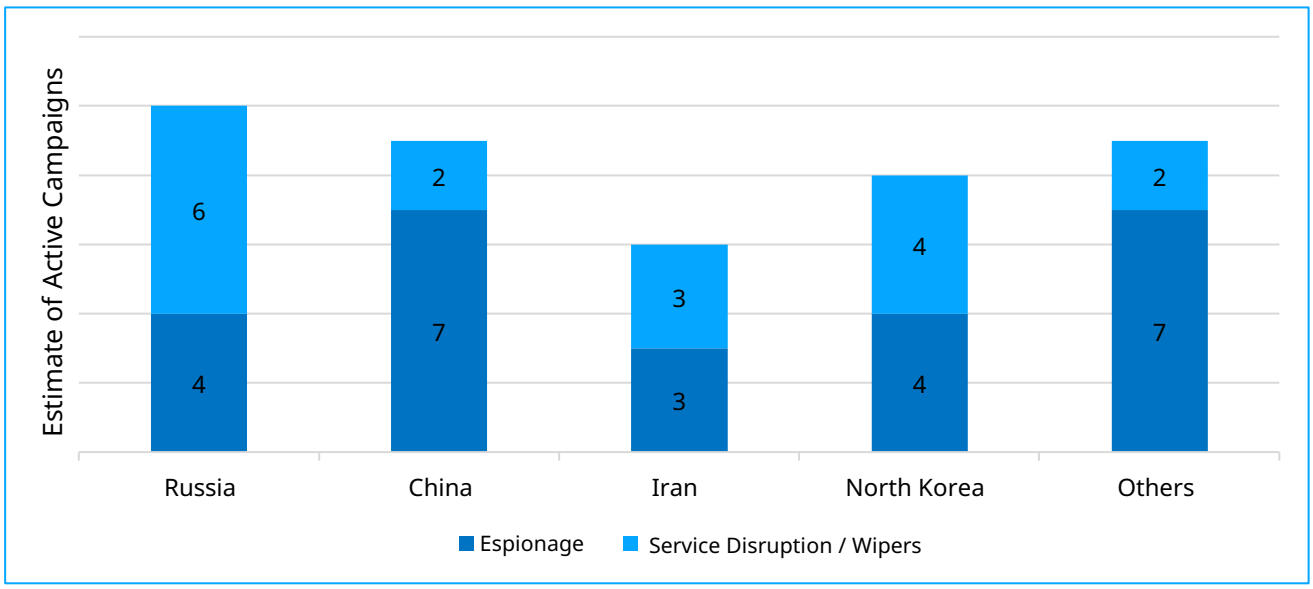


Figure 13 | APT group activity by region classified by motivation in the first half of 2025

The analysis highlights a more destructive trend among actors like Russia and Iran, compared to espionage-centered approaches from China, North Korea, and South Asian groups. This segmentation enables the identification of distinct operational patterns by region and supports the anticipation of potential tactical evolutions depending on the geopolitical context.

Tactics, Techniques, and Procedures (TTPs)

7. Tactics, Techniques, and Procedures (TTPs)

Tactics, Techniques, and Procedures (TTPs) are a foundational approach to understanding the strategies used by malicious actors in the cyber threat landscape. Identifying these patterns not only strengthens an organization's defensive posture but also enables proactive risk anticipation and mitigation.

7.1 Description of the Most Common TTPs Used by Cybercriminals

During the first half of 2025, phishing remained the primary initial access technique. Threat actors used vishing, malicious links and attachments, and Business Email Compromise (BEC) attacks. Additionally, a wider range of commercial and open-source remote access tools was observed, including **SplashTop, Atera, TeamViewer, AnyDesk, LogMeIn, ScreenConnect, QuickAssist, TightVNC**, and the **Level RMM platform**.

The following table highlights the most observed MITRE ATT&CK techniques in the first half of 2025:

Tactics	MITRE ATT&CK ID	Description
Reconnaissance (TA0043)	T1590 – Gather Victim Network Information	Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data as well as specifics regarding its topology and operations.
	T1595.002 – Active Scanning: Vulnerability Scanning	Adversaries may perform vulnerability scans on an organization's public-facing infrastructure to identify potential weaknesses that could be exploited.
Initial Access (TA0001)	T1598.004 – Phishing for Information: Spearphishing Voice	In an observed campaign, adversaries impersonated IT support over the phone and instructed users to initiate a QuickAssist session.
	T1598.003 – Phishing for Information: Spearphishing Link	Adversaries may send spearphishing messages with a malicious link to elicit sensitive information that can be used during targeting.
	T1598.002 – Phishing for Information: Spearphishing Attachment	Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information that can be used during targeting.
	T1190 - Exploit Public-Facing Application	Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network.
	T1078 – Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
Execution (TA0002)	T1059.001 – Command and Scripting Interpreter: PowerShell	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.
	T1047 – Windows Management Instrumentation	Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads.
	T1053 – Scheduled Task/Job	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.

Tactics	MITRE ATT&CK ID	Description
Persistence (TA0003)	T1098 – Account Manipulation	Adversaries may manipulate accounts to maintain and/or elevate access to victim systems.
	T1136.001 – Create Account: Local Account	Adversaries may create an account to maintain access to victim systems.
	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Adversaries established persistence by embedding IP addresses into the TitanPlus registry key.
	T1133 – External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network.
	T1546.008 – Event Triggered Execution: Accessibility Features	Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features.
Privilege Escalation (TA0002)	T1134 – Access Token Manipulation	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls.
Defense Evasion (TA0005)	T1562.001 – Impair Defenses: Disable or Modify Tools	Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities.
	T1562.004 – Impair Defenses: Disable or Modify System Firewall	Adversaries may disable or modify system firewalls to bypass controls limiting network usage.
	T1564.008 – Hide Artifacts: Email Hiding Rules	Adversaries may use email rules to hide incoming or outgoing messages in the mailbox of a compromised user.
	T1070.001 – Indicator Removal: Clear Windows Event Logs	Adversaries may clear Windows Event Logs to hide the activity of an intrusion and hinder forensic analysis.
	T1112 – Modify Registry	Adversaries may interact with the Windows Registry as part of a variety of other techniques to aid in defense evasion, persistence, and execution.
Credential Access (TA0006)	T1003 – OS Credential Dumping	Adversaries may dump credentials from various sources to facilitate lateral movement.
	T1528 – Steal Application Access Token	Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.
Discovery (TA0007)	T1046 – Network Service Discovery	Adversaries may use tools such as advanced port scanners to perform network scanning.
	T1057 – Process Discovery	Adversaries may attempt to get information about running processes on a system.
	T1018 – Remote System Discovery	Adversaries may attempt to discover information about remote systems using commands such as "net view".
	T1082 – System Information Discovery	DiscoveryAn adversary may attempt to get detailed information about the operating system and hardware.
	T1016 – System Network Configuration Discovery	Adversaries may use commands such as "ifconfig" and "net use" to identify network connections.
	T1087.001 – Account Discovery	Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system.

Tactics	MITRE ATT&CK ID	Description
Lateral Movement (TA0008)	T1021.001 – Remote Services: Remote Desktop Protocol	Adversaries may use valid accounts to log into a computer using the Remote Desktop Protocol (RDP).
	T1021.006 – Remote Services: Windows Remote Management	Adversaries may use Valid Accounts to interact with remote systems using Windows Remote Management (WinRM).
Command and Control (TA0011)	T1219 – Remote Access Tools	An adversary may use legitimate remote desktop and support software to establish an interactive command and control channel to target systems within networks.
	T1105 – Ingress Tool Transfer	Adversaries may transfer tools or other files from an external system into a compromised environment.
	T1572 – Protocol Tunneling	Adversaries may tunnel network communications to and from a victim system using a separate protocol, such as SMB, to avoid detection or enable access to otherwise unreachable systems.
Exfiltration (TA0010)	T1048 – Exfiltration Over Alternative Protocol	Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel, such as WinSCP.
Impact (TA0040)	T1486 – Data Encrypted for Impact	Adversaries may modify the lifecycle policies of a cloud storage bucket to destroy all objects stored within.
	T1490 – Inhibit System Recovery	Adversaries may disable system recovery features such as volume shadow copies.
	T1489 – Service Stop	Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.

Table 4 | Most common TTPs in the first half of 2025

Based on the evolution of these TTPs and current threat trends, **the second half of 2025 is expected** to bring an increase in the **abuse of legitimate tools**, **more sophisticated evasion techniques**, broader use of **automated and AI-driven scripts**, and **heightened persistence** in hybrid environments with expanded attack surfaces.

The MITRE ATT&CK framework not only supports a clearer understanding of these threats but also offers a practical approach for mitigation efforts.

7.2 Most Common Entry Vectors

In this context, and considering that ransomware remains one of the most persistent and profitable threats, current trends in entry vectors can be summarized as follows (Check Point Research, 2025):

Edge Devices	Infostealers	Cloud Environments
The growing use of **IoT devices, wearables, and remote work hardware** has expanded the attack surface, making these endpoints less protected and easier to monitor.	This type of malware used to steal sensitive data is now mainstream and among the most active threats. Its **ease of deployment**, boosted by the rise of **Malware-as-a-Service** (MaaS) and **creative distribution methods**, has increased its use during the initial access phase of ransomware and APT campaigns. (Lumma Stealer – PupkinStealer – FormBook)	The adoption of **hybrid and multi-cloud** infrastructure continues to rise and faces challenges such as **configuration management** and **API security**. These factors position cloud environments as an easily accessible entry vector.
Business Email Compromise	**Denial of Service (DoS)**	**Man-in-the-Middle (MitM)**
Surge in BEC attacks enhanced by generative AI. **Financially motivated**, this threat vector ranks among the most damaging. Techniques are **evolving rapidly**, **with a strong focus on targeting critical sectors**. (Cartier, 2025)	**Real-time, automated, and adaptive attack** patterns are increasingly effective at evading defenses. More efficient use of **IoT botnets**. Use of DoS/DDoS as a **distraction tactic** to mask other attacks. Growth in attacks against **critical infrastructure.** Increased accessibility through **DDoS-as-a-Service platforms**. (Cloudflare – X)	**Exploitation of vulnerabilities in next-generation** networks by intercepting and decrypting traffic in 5G and WiFi 6E environments. Rise in attacks against **SCADA systems and industrial IoT devices.** Increased MitM attacks via **mobile apps.** Tactics are more sophisticated and often linked to **APT** campaigns.

Table 5 | Most common entry vectors in the first half of 2025.

While new intrusion techniques continue to emerge, traditional entry vectors remain persistently effective. **Phishing** continues to be the most widely used method to deceive users and gain initial access. **Remote attacks**, the use of **compromised credentials**, and the **exploitation of vulnerabilities**—including zero-day vulnerabilities—remain key entry points. These techniques are constantly evolving and becoming more sophisticated.

7.3 Attack Innovation: New Techniques and Tactics

The following section highlights some of the most disruptive techniques observed, detailing their mechanisms, associated campaigns, and what differentiates them from previous methods:

AI Tool Installers as Malware Distribution Vectors

This technique is based on hiding malware inside fake installers for AI tools. These malicious executables impersonate popular software, including productivity assistants and text or image generators, taking advantage of the growing interest in generative AI.

- It has been observed in real-world campaigns distributing ransomware (CyberLock), remote control malware (Lucky_Gh0st), and the **newly identified threat known as Numero** (Cisco Talos Intelligence, 2025).
- What makes this tactic innovative is its use of widespread interest in AI, combining social engineering with advanced packaging techniques.
- Unlike previous campaigns based on attachments or scripts, these samples include fake installation interfaces to make the download appear legitimate.

MFA Bypass via Reverse Proxies and OAuth Manipulation

This technique allows attackers to intercept authentication tokens and take control of sessions protected by MFA. It works by creating fake websites that replicate real login flows and redirect traffic through reverse proxies such as Evilginx2 (Google Cloud, 2025).

- It has been used in real campaigns by the APT group ColdRiver targeting NGOs, journalists, and Western government entities.
- What makes this tactic especially dangerous is its ability to **fully impersonate the authentication flow without requiring local malware**. It can extract both credentials and valid tokens in real time.
- Compared to previous attacks that required endpoint infection, this technique is entirely remote, harder to trace, and highly effective even in MFA-protected environments.

Dual-Function Browser Extensions

These browser extensions provide legitimate functions (such as document editing or web analytics) while simultaneously performing covert activities like cookie exfiltration, keylogging, or connecting to remote command channels.

- DomainTools (2025) identified over 30 such extensions in the Chrome Web Store used in active campaigns (DomainTools, 2025).
- This technique is innovative because it uses functional tools as a Trojan horse, building real trust with users. Additionally, distribution via official stores allows them to bypass common security checks.
- These differ from traditionally malicious extensions because they operate as expected, which prolongs their lifespan and reduces the likelihood of users uninstalling them.

"Crime-as-a-Service"

- Crime-as-a-Service (CaaS)Underground platforms have begun offering on-demand hacking and spam services (SOCRadar, 2025), such as DDoS campaigns, SMS flooding, or mass spam attacks. These services come with SaaS-like dashboards, technical support, and country-based targeting.
- Detected in Russian-speaking markets since May, they stand out for their ease of use and immediate deployment. They even include tutorials for attackers with little experience (SOCRadar, 2025).
- These platforms enable low-skilled actors to conduct operations that were previously exclusive to APT groups or well-resourced adversaries. Their operational maturity is what makes this innovation stand out.
- Compared to older forums like Genesis Market, this new generation offers fully automated operations without direct interaction between the parties.

Chaos RAT

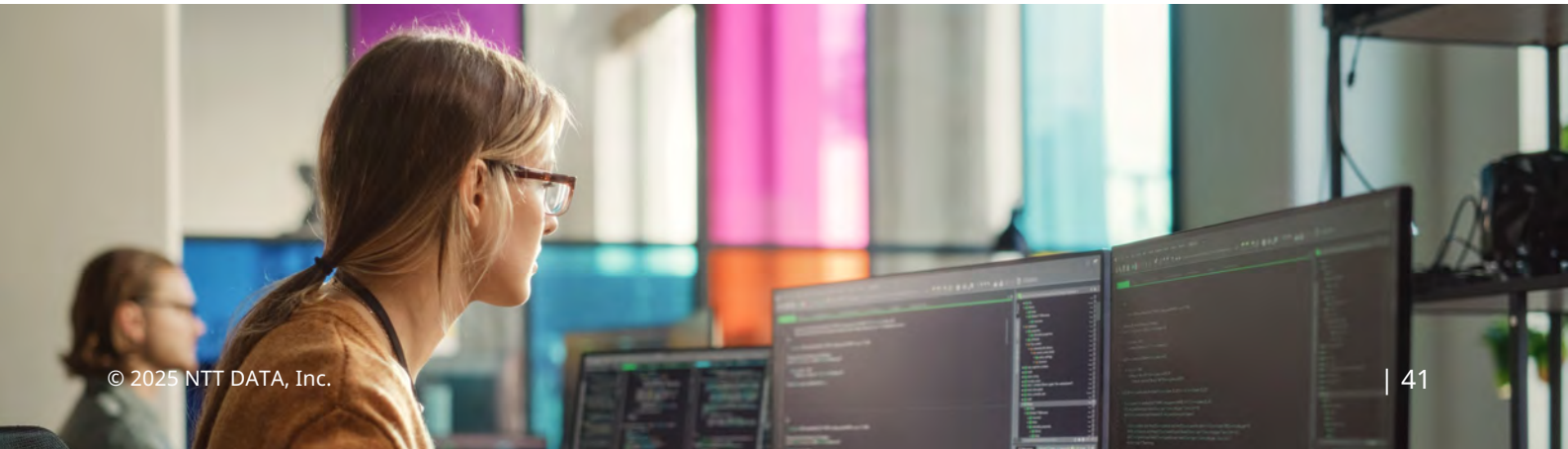
The latest version of Chaos RAT features a modular architecture, custom encryption in the C2 channel, stealthy installation, and persistence across Windows, Linux, and even IoT environments (Acronis, 2025).

- Researchers observed it in May during campaigns that remain unattributed. The malware is designed to operate as a complete offensive platform, capable of deploying payloads on demand and executing remote commands across compromised networks.
- Its most critical advantage is the ability to remain undetected for extended periods and to resist common containment techniques, such as process whitelisting.
- Compared to traditional RATs like njRAT or Quasar, Chaos behaves like a full offensive framework, offering total control over the target environment.

In addition to all the techniques described above, the **Cyber Threat Intelligence Department** has observed an emerging trend in the use of multi-component malware. Although this tactic is not new, **it has played a more active role in recent campaigns**. This type of malware is characterized by being divided into multiple fragments and delivered sequentially via encrypted messaging channels. Each fragment is harmless on its own, but when assembled on the target machine, they form a complete malicious payload.

Its resurgence points to the use of alternative distribution channels, including encrypted messaging services like Telegram and Signal. The main risk lies in its stealth and persistence, which require improvements in behavior-based detection systems and contextual analysis.

This technical evolution reinforces the need to continuously adapt defensive capabilities to TTPs that are increasingly segmented, modular, and difficult to correlate in real time.



Vulnerabilities

8. Vulnerabilities

The first half of 2025 has confirmed the ongoing presence of a persistent and sophisticated threat related to critical vulnerabilities, which continue to serve as one of the primary entry points for cyberattacks on a global scale.

Over these six months, a high level of activity has been observed in the identification and active exploitation of critical vulnerabilities, with a clear trend targeting enterprise environments, industrial infrastructures, and mobile devices.

Between January and June, **NTT DATA's Cyber Threat Intelligence Department** monitored approximately 7,664 published CVE vulnerabilities, 285 of which were classified as critical, and at least 105 were actively exploited in the wild. This figure highlights the agility of threat actors in leveraging newly disclosed vulnerabilities and reinforces the urgent need to accelerate patching cycles and implement continuous monitoring strategies.

The following is a month-by-month analysis of the **most relevant critical vulnerabilities during the period**, based on their technical impact, real-world exploitation, or effects on critical sectors.

• January:

In January 2025, **517 vulnerabilities** were identified, including **22** classified as **critical** and **20 that were actively exploited**. These vulnerabilities marked the beginning of a year characterized by increased targeting of network platforms and Linux environments, known for their ease of exploitation and integration into automated attack tools.

Key vulnerabilities identified:

- **CVE-2024-12084 (rsync):** Heap overflow, widely exploitable in Linux environments.
- **CVE-2025-0060 / 0061 (SAP BusinessObjects):** Remote code execution in corporate BI platforms.
- **CVE-2024-40891 / 40890 (Zyxel):** Injection vulnerabilities in networking devices, used by botnets.

Main impacts:

- Exploitation of network infrastructures
- Data theft and unauthorized access to core enterprise systems.
- The dominance of automated attacks and the rapid integration into exploit kits underscore the need for robust network segmentation and continuous monitoring.

• February:

In February 2025, **1,558 vulnerabilities** were identified, **33** of which were **critical** and **16 actively exploited**—marking a significant increase over the previous month. These vulnerabilities primarily affected network infrastructures and cloud-native environments, reflecting a shift toward more dynamic and harder-to-defend targets.

Key vulnerabilities identified:

- **CVE-2024-11218 (containers/Red Hat):** Container escape, actively exploited.
- **CVE-2025-0890 (Zyxel):** New vulnerability in widely deployed routers.
- **CVE-2025-21198 (Microsoft Exchange): Critical vulnerability in enterprise email systems, with active exploitation.**
- **CVE-2024-45569 (Qualcomm):** Vulnerability in Exynos chipsets, exploited in mobile devices.

Main impacts:

- Remote access to corporate systems
- Control over IoT devices
- Leakage of sensitive information from end-user environments
- The active exploitation of vulnerabilities in widely deployed infrastructures highlights the ongoing challenge of maintaining a consistent cybersecurity posture

• March:

In March 2025, **1,032 vulnerabilities** were identified, **43** of which were **critical** and **24 actively exploited**. This month saw increased exploitation of vulnerabilities in commonly used enterprise solutions, including file transfer systems and web development tools. The near-immediate publication of proof-of-concept (PoC) code significantly raised the risk level.

Key vulnerabilities identified:

- **CVE-2023-13124 (SAP NetWeaver Visual Composer):** Vulnerability allowing unauthorized upload of malicious binaries in SAP environments via the Metadata Uploader component. Exploitation has been documented in campaigns targeting enterprise systems heavily dependent on this platform, compromising integrity and availability.
- **CVE-2023-3161 (CrushFTP):** Authentication bypass in versions prior to 11.3.1, actively exploited. Enables unauthenticated access through a vulnerability in HMAC validation, granting full system control. Related to ransomware campaigns targeting financial institutions and managed service providers.
- **CVE-2025-0603 (Aviatrix Controller):** Remote command execution through manipulation of API parameters (*cloud_type*). The active exploitation of this vulnerability presents a significant risk in multicloud and hybrid environments used in critical operations.

Main impacts:

- Exploitation of exposed servers
- Persistence in systems and privilege escalation.

• April:

In April, **1,381 vulnerabilities** were identified, including **57 classified as critical and 13 that were actively exploited**. This month was notable for the diversity of affected products and the targeted exploitation of edge devices and microservices environments.

Key vulnerabilities identified:

- **CVE-2025-22457 (Ivanti EPMM):** Unauthenticated remote access on mobile platforms.
- **CVE-2025-30215 (NATS.io):** Remote code execution in microservices middleware.
- **CVE-2024-51138/51139 (DrayTek):** Vulnerabilities in widely used routers.

- ## May:

In May 2025, **1,549 vulnerabilities** were identified, including **44** classified as **critical** and **17 that were actively exploited.** The most relevant vulnerabilities targeted key security products and mobile platforms, consolidating a trend toward highly targeted and persistent attacks.

Key vulnerabilities identified:

- **CVE-2025-40595 (SonicWall):** Active exploit targeting firewalls and perimeter devices.
- **CVE-2025-22252 (Fortinet):** Unauthenticated RCE in widely deployed solutions.
- **CVE-2025-31219 (Apple):** Zero-day in Apple systems.
- **CVE-2025-0203 (Ivanti Connect Secure/Policy Secure):** Buffer overflow in widely used ZTA gateways, allows unauthenticated arbitrary code execution. Its exploitation has been linked to ransomware groups targeting government and telecommunications sectors due to the critical nature of access it enables.

Main impacts:

- Initial Access
- Persistence within corporate networks
- Exposure of mobile user data

- ## June:

A total of **1,426 vulnerabilities were identified in June, including 81 classified as critical and at least 17 that were actively exploited**.
June registered significant activity involving VoIP devices, Linux servers, and mobile devices, signaling a continued focus on critical environments with large attack surfaces.

Key vulnerabilities identified:

- **CVE-2025-30507 (CyberData SIP):** RCE in industrial VoIP devices.
- **CVE-2025-49087 (Red Hat/Perl-FCGI):** RCE in Linux web environments.
- **CVE-2025-23107 (Samsung Exynos):** Exploited in attacks against mobile devices.

Main impacts:

- Threats to critical voice infrastructure, web servers, and Android/iOS ecosystems
- Reinforces the need for complete visibility over connected devices, where most users remain unaware of existing vulnerabilities and the associated risks

Vulnerability and exploitation trends (H2 2024 – H1 2025)

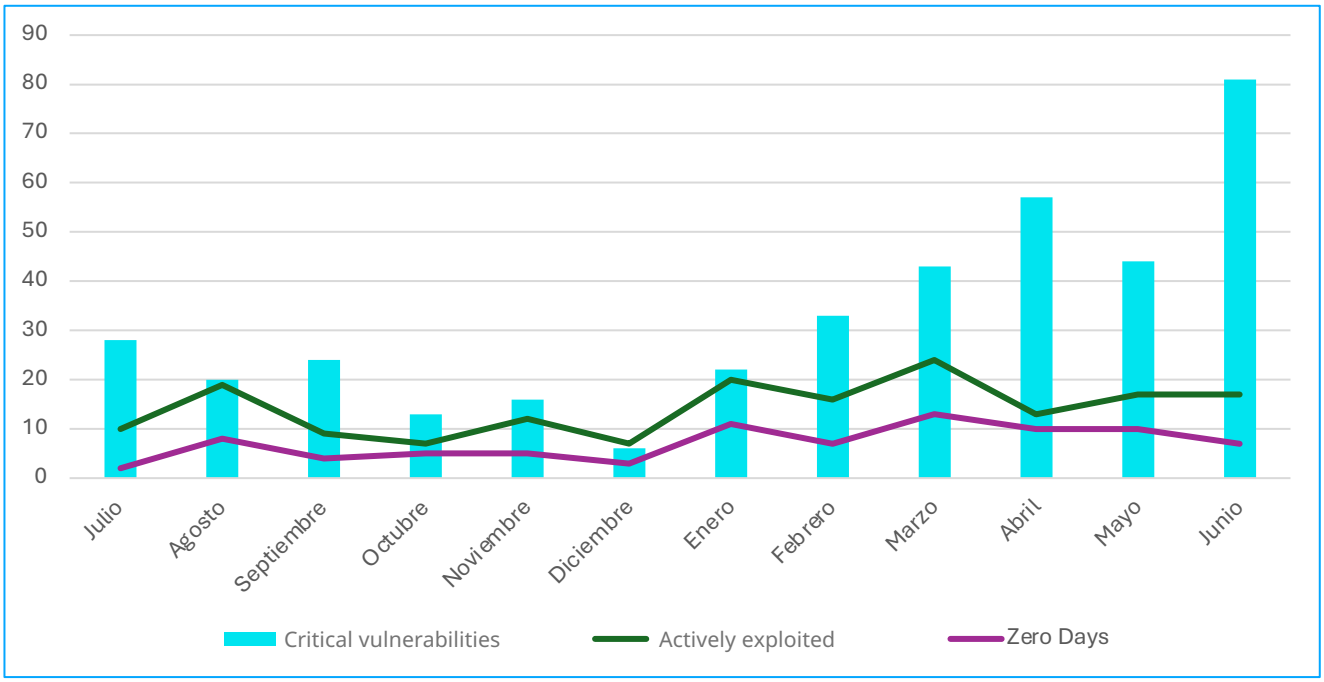


Figure 14 | Exploitation and presence of critical vulnerabilities (H1 2025 vs. H2 2024)

Vulnerability and Exploitation Trends:

- During the first half of 2025, **threat actors increasingly adopted a strategy** of **exploiting critical vulnerabilities immediately after public disclosure**, especially those with published PoCs. Threat actors significantly increased the rate of active exploitation in the first half of 2025 compared to the total number of published critical vulnerabilities in the second half of 2024.

The operational focus has centered on:

- Exposed network systems and **edge devices** such as routers, firewalls, and remote access solutions.
- **OT environments and industrial devices**, where vulnerabilities pose a more disruptive and critical threat to ongoing operations.
- **Cloud-native infrastructure and containers**, where complexity in management is exploited to escalate privileges and maintain persistence.
- **Mobile platforms and widely adopted chipsets**, such as Exynos and Apple SoC, increasingly targeted for their role in identity management and data access.

There is **growing evidence that ransomware and APT groups** have become increasingly sophisticated, aligning their campaigns with vulnerability disclosure schedules and reducing technical preparation time with automated exploitation tools.

This tactical shift underscores a critical need to shorten average patching times, deploy rapid mitigation measures (such as access control lists and network segmentation), and strengthen proactive threat intelligence—particularly in industrial, telecommunications, and critical service sectors.

Future Outlook

9. What to Expect in the Second Half of 2025

The second half of 2025 is projected to be a logical—and likely intensified—continuation of the trends observed in the first six months of the year. During the first half of the year, the threat landscape was characterized by a high volume of vulnerabilities—many of them zero-days—and their active exploitation by threat actors in real-world campaigns. This pattern indicates an acceleration in the window between vulnerability disclosure and its offensive use.

Threat actor activity was especially intense in the first half of the year, with **RansomHub** and **Cl0p** emerging as the leading ransomware groups in 2025 to date. While the visibility of groups like **LockBit** has decreased, others such as **Akira** and **Qilin** have remained firmly within the top five in terms of reported campaigns, solidifying a highly professionalized business model. These groups—or potential offshoots—are expected to remain active and **scale up their operations as periods of increased fiscal and budgetary pressure approach in corporate environments.**

At the same time, an emerging trend has taken shape: the **fragmentation of the cybercriminal ecosystem.** New coalitions of hacktivist groups—often opportunistic or ideologically driven—have emerged in response to escalating geopolitical polarization, particularly **surrounding the conflict between Israel and Gaza**.

This has elevated Western government agencies, NATO country infrastructures, and entities with Israeli-linked interests to **high-priority targets**. This trend is expected to persist or even intensify in the coming months.

Meanwhile, the underground ecosystem is also undergoing significant transformation.

Recent arrests, the **shutdown of BreachForums**, and **the fall of Archetype—the largest dark web drug market**—have created instability that is reshaping the power dynamics among actors and platforms. A r**ebound effect** is being observed: **disruptions in the deep layers of cybercrime are beginning to surface**. The emergence of groups dedicated to extorting other collectives, exposing former partners, or interfering in rival campaigns may trigger an increase in insider leaks, doxing campaigns, and visibility disputes in clandestine forums.

Adding to this is the ongoing professionalization of cybercrime. The availability of accessible tools, technical collaboration environments, and a shadow economy that views digital crime as a means of income have contributed to a monthly increase in the number of operational groups. As many of these actors now operate with business-like structures, **the volume and technical sophistication of attacks are expected to rise in the second half**.

In this context, reinforcing early detection mechanisms for vulnerabilities and applying adaptive prioritization models will be essential to reduce the time between flaw identification and effective mitigation. It will also be critical to monitor the threat landscape not only in its technical behaviors (TTPs) but also in its social and geopolitical dimensions to anticipate the evolution of campaigns driven by ideological polarization or rivalries between criminal groups.

Ongoing monitoring of the underground ecosystem will be equally vital: the developments occurring in these layers over the coming months may serve as a prelude to new campaigns, tools, or large-scale breaches that could directly impact the global corporate and government landscape.

References

- Cartier, M. (March 3, 2025). *Business Email Compromise Statistics 2025*. Hoxhunt. https://hoxhunt.com/blog/business-email-compromise-statistics
- CERT-EU. (2025). *Threat Landscape Q1 & Q2 2025 Reports*[RG1] [SS2] . https://cert.europa.eu/publications/threat-intelligence/2025
- Check Point Research. (January 14, 2025). *5 Key Cyber Security Trends for 2025*. Check Point. https://blog.checkpoint.com/research/5-key-cyber-security-trends-for-2025
- CISA. (November 20, 2024). *#StopRansomware: BianLian Ransomware Group.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a
- CISA. (April 30, 2025). *#StopRansomware: Rhysida Ransomware*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
- Cloudforce One. (May 21, 2025). *Cloudflare participates in global operation to disrupt Lumma Stealer*. Cloudflare. https://www.cloudflare.com/es-es/threat-intelligence/research/report/cloudflare-participates-in-joint-operation-to-disrupt-lumma-stealer/
- CrowdStrike. (2025). *CrowdStrike Global Threat Report 2025*. https://www.crowdstrike.com/global-threat-report/
- Cyber News Centre Team. (July 4, 2025). *The State of APAC Cybersecurity: CNC Intelligence Overwatch Report - July 2025*. Cyber News Centre. https://www.cybernewscentre.com/the-state-of-apac-cybersecurity-cnc-intelligence-overwatch-report-july-2025/
- Cybersecurity Ventures. (2025). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybersecurity Ventures. https://cybersecurityventures.com/cyberwarfare-report-intrusion/[RG3]
- CYFIRMA. (May 9, 2025). *PupkinStealer : A .NET-Based Info-Stealer*. CYFIRMA. https://www.cyfirma.com/research/pupkinstealer-a-net-based-info-stealer/
- DarkFeed. (2025). *Here's a look at the most active ransomware groups of 2025* [X's posts]. X. https://x.com/ido_cohen2
- DarkFeed. (2025). *New Ransomware Group* [X's posts]. X. https://x.com/ido_cohen2
- Department for Science, Innovation and Technology, Home Office and Feryal Clark MP. (April 10, 2025). *Cyber Security Breaches Survey 2025*. Gov.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/
- Yoachimik, O. and Pacheco, J. (April 27, 2025). *Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare's 2025 Q1 DDoS Threat Report*. Cloudflare. https://blog.cloudflare.com/es-la/ddos-threat-report-for-2025-q1/

- FBI. (March 6, 2025). *Mail Scam Targeting Corporate Executives Claims Ties to Ransomware.* Internet Crime Complaint Center. https://www.ic3.gov/psa/2025/psa250306-2#:~:text=March%206%2C%202025-,Mail%20Scam%20Targeting%20Corporate%20Executives%20Claims%20Ties%20to%20Ransomware,come%20from%20a%20ransomware%20group.
- Federal Ministry of the Interior. (2025). *Protecting the 2025 Bundestag elections from hybrid threats and disinformation*. Federal Ministry of the Interior. https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/disinformation-election-artikel.html
- Fox, J. (December 23, 2024). *Top Cybersecurity Statistics 2025*. Cobalt. https://www.cobalt.io/blog/top-cybersecurity-statistics-2025/
- Franceschi-Bicchierai, L. (May 23, 2025). *Mysterious hacking group Careto was run by the Spanish government, sources say*. TechCrunch. https://techcrunch.com/2025/05/23/mysterious-hacking-group-careto-was-run-by-the-spanish-government-sources-say/
- Fry, C. (2025). *The Cost of a Cyber Attack in 2025 on SMEs*. Robinson https://www.robison.co.uk/cost-of-a-cyber-attack-2025/
- Gatlan, S. (May 27, 2025). *Russian Laundry Bear cyberspies linked to Dutch Police hack*. BleepingComputer. https://www.bleepingcomputer.com/news/security/russian-void-blizzard-cyberspies-linked-to-dutch-police-breach/
- Group-IB. (2025). *Hi-Tech Crime Trends Report 2025*. https://www.group-ib.com/landing/high-tech-crime-trends-2025/
- Hitachi Cyber. (January 17, 2025). *Cyber Threat Landscape in 2025: Trends and Challenges*. Hitachi. https://hitachicyber.com/cyber-threat-landscape-in-2025-trends-and-challenges/
- Identity Defined Security Alliance. (2025). *2025 Identity Security Landscape Report*. https://www.idsalliance.org
- KrakenLabs. (2025). *Threat Context Monthly Reports (January–May 2025)*. Outpost24. https://outpost24.com/blog
- Márquez, J. (May 24, 2025). *SecurityMysterious hacking group Careto was run by the Spanish government*. Xataka. https://www.xataka.com/seguridad/misterioso-grupo-hackers-careto-se-encontraba-agente-inesperado-gobierno-espana-techcrunch
- Zang X. (April 22, 2025). Infostealer Malware FormBook Spread via Phishing Campaign – Part I. Fortinet. https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign-part-i

- Microsoft Threat Intelligence. (May 27, 2025). *New Russia-affiliated actor Void Blizzard targets critical sectors for espionage*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/
- Microsoft Threat Intelligence, Microsoft Digital Crimes Unit and Microsoft Security Experts [MTI, MDC & MSE]. (May 21, 2025). *Lumma Stealer: Breaking down the delivery techniques and capabilities of a prolific infostealer*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/
- Miliefsky, G. (March 13, 2025). *The true cost of cybercrime: Why global damages could reach $1.2 to $1.5 trillion by end of 2025*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com
- Newman, L.H. (March 11, 2025). *What Really Happened With the DDoS Attacks That Took Down X*. Wired. https://www.wired.com/story/x-ddos-attack-march-2025/
- Orange Cyberdefense. (2025). *Sector 16 Group*. Orange. https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Sector16/Sector16Group.pdf
- Stamford, C. (August 28, 2024). *Gartner Forecasts Global Information Security Spending to Grow 15% in 2025*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025
- SOCRadar. (May 22, 2025). *Top 10 Deep Web and Dark Web Forums*. https://socradar.io/top-10-deep-web-and-dark-web-forums/
- Tamzid, A. (May 23, 2025). *Cybercrime statistics and financial impact*. Bright Defense. https://www.brightdefense.com/resources/cybercrime-statistics/
- Toulas, B. (May 1, 2025). *Pro-Russia hacktivists bombard Dutch public orgs with DDoS attacks.* BleepingComputer. https://www.bleepingcomputer.com/news/security/pro-russia-hacktivists-bombard-dutch-public-orgs-with-ddos-attacks/
- World Economic Forum. (January 13, 2025). *Global Cybersecurity Outlook 2025*. https://www.weforum.org/reports/global-cybersecurity-outlook-2025
- Yilmaz, E. and Yildirim, E. (May 10, 2025). *Cyber threats to cost $10.5T by 2025 as cybersecurity investments surge*. AA News. https://www.aa.com.tr/en/science-technology/cyber-threats-to-cost-105t-by-2025-as-cybersecurity-investments-surge/3563268


NTT DATA