

CTI Trends

Cyber Threat Intelligence

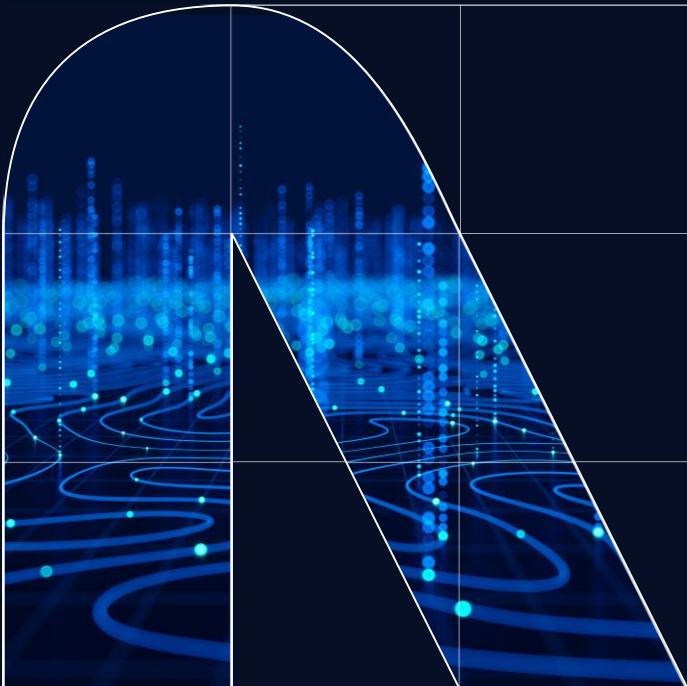
First half of 2026

Index

1. <u>Executive Summary</u>	4
2. <u>Introduction</u>	6
2.1. Purpose of the report	6
2.2. Geographic and temporal scope of the report	6
3. <u>Global Threat Landscape</u>	7
3.1. Geopolitics and cybersecurity	8
3.2. Geopolitics and key actors	9
3.3. Impact of cyberattacks on specific regions and sectors	10
4. <u>Major Global Threats</u>	13
4.1. Notable cyber incidents and major campaigns	14
4.2. Emerging attack trends	16
4.3. Global statistics on security incidents, types of attacks and threat actors involved	17
4.4. Costs of cyberattacks for organizations	19
5. <u>Legal framework and arrests in cybersecurity</u>	20
5.1. Main laws in the field of cybersecurity	21
5.2. Major arrests in the field of cybersecurity	22
6. <u>Dark Web Insights</u>	26
6.1. Law-enforcement pressure and reconfiguration of the underground ecosystem	27
6.2. Active underground forums	28
6.3. Active underground markets	29
7. <u>Threat Actors</u>	32
7.1. Newly identified Threat Actors	33
7.2. Ransomware	34
7.3. Hacktivism	39
7.4. APT	40

Index

8. <u>Tactics, Techniques and Procedures</u>	43
8.1. Description of the most common TTPs used by cybercriminals	44
8.2. Most common entry vectors	48
8.3. Innovation in attacks: new techniques and tactics	49
9. <u>Vulnerabilities</u>	51
10. <u>Future outlook</u>	56
11. <u>References</u>	58



1. Executive Summary

The first half of 2026 has been defined by **an operational acceleration of the attack cycle**, in an environment where cyber pressure is driven by the combination of geopolitics, digital exposure, third-party dependency, rapid exploitation of vulnerabilities, and monetization of compromised identities.

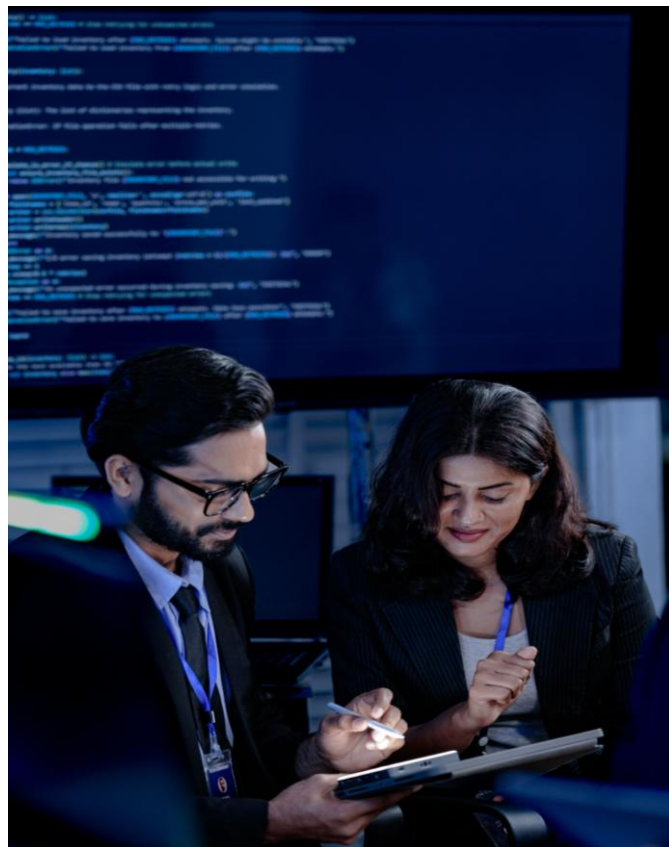
The main difference compared with previous periods has not been the emergence of new threat categories, but **the ability to turn known vectors into faster, more scalable, and harder-to-contain campaigns**.

On the **geopolitical level**, cyberspace has remained a **domain of strategic pressure**. Rivalry between powers has shaped target selection and campaign intensity. The most visible activity has taken the form of DDoS, defacement, leaks, and propaganda; however, strategic risk is also concentrated in less noisy operations: persistent espionage, abuse of suppliers, exploitation of exposed infrastructure, and covert presence in critical sectors.

Global victimology confirms that cyber pressure is not driven only by the volume of available targets, but by the combination of digital exposure, operational criticality, economic value, geopolitical relevance, and the ability to generate indirect impact. **The United States** has maintained the highest visibility, while **public administration** stands out due to its institutional visibility and political pressure.

The **main global threats** have been marked by the continued presence of ransomware, vulnerability exploitation, the use of infostealers, AI-driven social engineering, abuse of cloud/SaaS, and disruptive attacks against critical infrastructure.

In Q1 2026, 2,122 victims were published on data leak sites, the second-highest figure recorded for a first quarter, while **ransomware was present in 48% of the breaches analyzed**, with groups such as **Qilin, Akira, and The Gentlemen** standing out. In addition, vulnerability exploitation has overtaken credential theft as the main initial access vector, reflecting how quickly actors operationalize public flaws.





1. Executive Summary

The economic impact remains systemic in scale. **The global cost of cybercrime has exceeded USD 12.5 trillion annually**, with an average breach cost of USD 4.44 million. At the same time, the decline in the average price of compromised corporate access, now around USD 439 compared with USD 1,427 three years ago, highlights a **deflation of initial access** that expands the pool of actors capable of monetizing intrusions.

The legal framework and law-enforcement action have advanced toward **a more operational response**. The development of the Cyber Resilience Act, the CMMC, new NIST guidance, and regulatory reforms in different regions have reinforced requirements around product security, critical infrastructure protection, suppliers, and incident reporting. In parallel, operations such as **Endgame/SocGhosh, Operation Saffron and Operation Ramz** show greater disruption capacity against criminal infrastructure, although their impact remains temporary in the face of an ecosystem with a high capacity for migration and reconstruction.

The underground ecosystem has maintained a high level of activity despite law-enforcement pressure. Activity has not disappeared following the takedown or seizure of major forums; instead, **it has been redistributed** toward alternative platforms, specialized markets, private communities, and restricted-access channels.

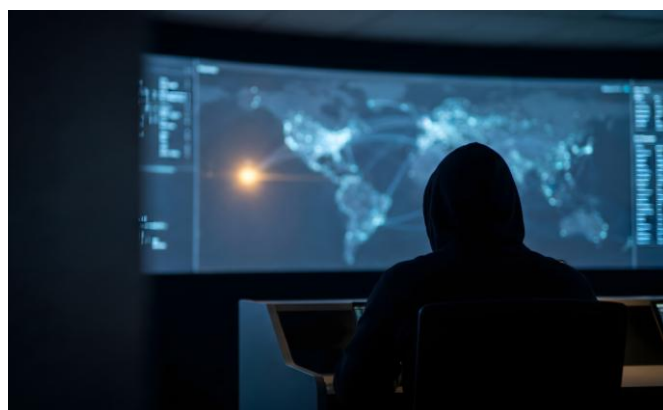
Finally, the vulnerabilities section confirms that defensive prioritization must be based on active exploitation, real exposure, and operational criticality, not only on CVSS severity.

The cases analyzed show that **the risk of a CVE lies in its ability to be quickly integrated into automated, stealthy campaigns focused on persistence, data theft, or operational impact**.

Cybersecurity is consolidating as a systemic challenge where technology, geopolitics, and the abuse of legitimate identities converge. Risk management requires an integrated approach: **contextual behavior-based detection, operational resilience, and strategic anticipation**.

Defensive advantage will depend on the ability to anticipate, correlate, and respond quickly.

Looking ahead to the second half of 2026, **the scenario points to greater offensive automation**, increased exploitation of exposed services, sustained pressure on critical infrastructure, and a criminal ecosystem more concentrated around effective operators, but more distributed across channels and markets.





2. Introduction

2.1. Purpose of the report

This report aims to provide a detailed analysis of the trends, incidents, and relevant developments in the field of Cyber Threat Intelligence (CTI) during the **first half of 2026**. The report addresses the emerging threats that are redefining the cybersecurity landscape, threat actors with notable activity, the most significant cyber campaigns, and the critical vulnerabilities detected during this period. It also identifies recurring patterns and outlines possible future scenarios that may influence risk management and mitigation strategies.

2.2. Geographic and temporal scope of the report

The analysis presented takes a global perspective, making it possible to understand how threats evolve in an interconnected way across different geographic contexts. This broad view facilitates the identification of common dynamics and regional specificities that enrich the understanding of the current cyber environment.

We are operating in an environment marked by relevant changes in threat behavior and by events that have had a significant impact on the digital ecosystem. This timeframe, which **runs from January to June 2026**, is key to anticipating possible future developments and strengthening response capabilities in an increasingly complex environment.

3. Global Threat Landscape



The current global threat landscape confirms the acceleration of trends already consolidated in previous periods, where a transition toward more persistent and less noisy threats was already visible, within a more volatile and fragmented environment.

The dynamics observed in 2026 reflect: greater geopolitical influence, higher offensive speed, greater abuse of digital trust, and increased pressure on critical sectors.

This assessment aligns with the World Economic Forum (WEF), which identifies the acceleration of AI, geopolitical fragmentation, and capability gaps as factors reshaping cyber risk in 2026 ([World Economic Forum, 2026](#)).

This section analyzes the **main factors in the global environment** that, due to their structural scope, shape the evolution of cyber risk and the stability of digital ecosystems.

Predominant structural factors in the global threat landscape in H1 2026



Figure 1 | Most influential risk factors in the global threat landscape during H1 2026.

3.1 Geopolitics and Cybersecurity

Cyber activity during the first half of 2026 shows that cyberspace does not merely accompany conflict, but **is already part of it by design**.

Geopolitics is no longer just a contextual factor and has become an element that shapes cyber activity. Open conflicts, technological rivalries, and competition between blocs influence which sectors are prioritized, which narratives are amplified, and which targets acquire strategic value.

The WEF also notes that **64%** of organizations already incorporate geopolitically motivated cyberattacks into their mitigation strategies, and that **91%** of the largest organizations have changed

their cybersecurity strategy due to geopolitical volatility.

On the other hand, **AI and automation** act as accelerators of the offensive cycle. Their relevance does not lie solely in the emergence of new techniques, but in the ability to make already known attacks faster, more convincing, and more scalable: phishing, fraud, reconnaissance, impersonation, content generation, and support for tool development. During the semester, malware families such as **PROMPTFLUX** and **PROMPTSTEAL** were observed, capable of querying LLM models during execution to adapt their behavior to adapt or

evade detection ([Google Cloud, 2026](#)). North Korean AI-enabled impersonation and **deepfake** operations have also increased, thereby connecting geopolitics, artificial intelligence, and identity abuse, another of the structural factors toward which risk has shifted during the semester.

The real perimeter of organizations is no longer limited to their own infrastructure; it now encompasses distributed digital trust across users and third parties, where **supply chain attacks and the abuse of legitimate access** allow attackers to operate with less technical noise.

Techniques such as **Adversary-in-the-Middle (AitM)**, **session hijacking**, and **MFA fatigue**, designed to steal identities, and coordinated **supply chain** campaigns, such as the **npm package campaign (Shai-Hulud and variants)**, are becoming critical entry vectors into an extended attack surface.

Finally, as part of the global threat landscape, **the exploitation of vulnerabilities** in exposed assets remains a risk factor, as do **ransomware and extortion**, which continue to function as an

economic engine for cybercrime, with a more mature logic.

3.2 Geopolitics and key actors

During H1 2026, the relationship between geopolitics and cybersecurity remains one of the structural axes of the global threat landscape. The main difference this semester is not the emergence of a new type of threat, but the way in which the geopolitical context shapes observed cyber activity.

Political, military, or diplomatic events act as campaign triggers; alliances, sanctions, and **international positioning** influence target selection; and sectors with strategic value acquire greater exposure due to their ability to generate operational, reputational, or political impact.

On the **Iran-Israel/U.S. and Middle East** axis, cyber activity reflects a combination of hacktivist campaigns, actors aligned with state interests, disinformation operations, **DDoS**, **defacement**, and leaks. The observed data reinforces this view: the Middle East appears as one of the areas with the greatest visibility in the sample, especially due to the concentration of activity associated with Israel-Iran and the diversity of observed typologies. This information should be interpreted as a signal of mobilization and narrative pressure, not as an absolute measurement of the actual volume of attacks.

In parallel, the **United States-China** rivalry maintains a less visible, but **strategically** more relevant, profile. In this case, risk does not mainly manifest through noisy campaigns, but through persistent espionage, targeting of telecommunications, military infrastructure, transport, government, and technology providers.

North Korea follows a differentiated logic, where cyberspace operates simultaneously as an espionage tool and a source of state financing. This combination of espionage, financial theft, identity abuse, and covert access reinforces the idea that geopolitical risk does not always take the form of sabotage or direct disruption.



Overall, H1 2026 confirms that geopolitics is not only context, but a factor that triggers campaigns, guides objectives, and amplifies impact. The most visible activity materializes in DDoS, defacement, leaks, and propaganda; however, strategic risk is also found in less noisy operations: espionage, pre-positioning,

abuse of suppliers, exploitation of exposed infrastructure, and persistence in critical sectors. The consequence for organizations is clear: cyber exposure must be analyzed not only from the technical surface, but also from their geographic, sectoral, regulatory, and geopolitical position.

Global map of cyber pressure by geopolitical context in H1 2026

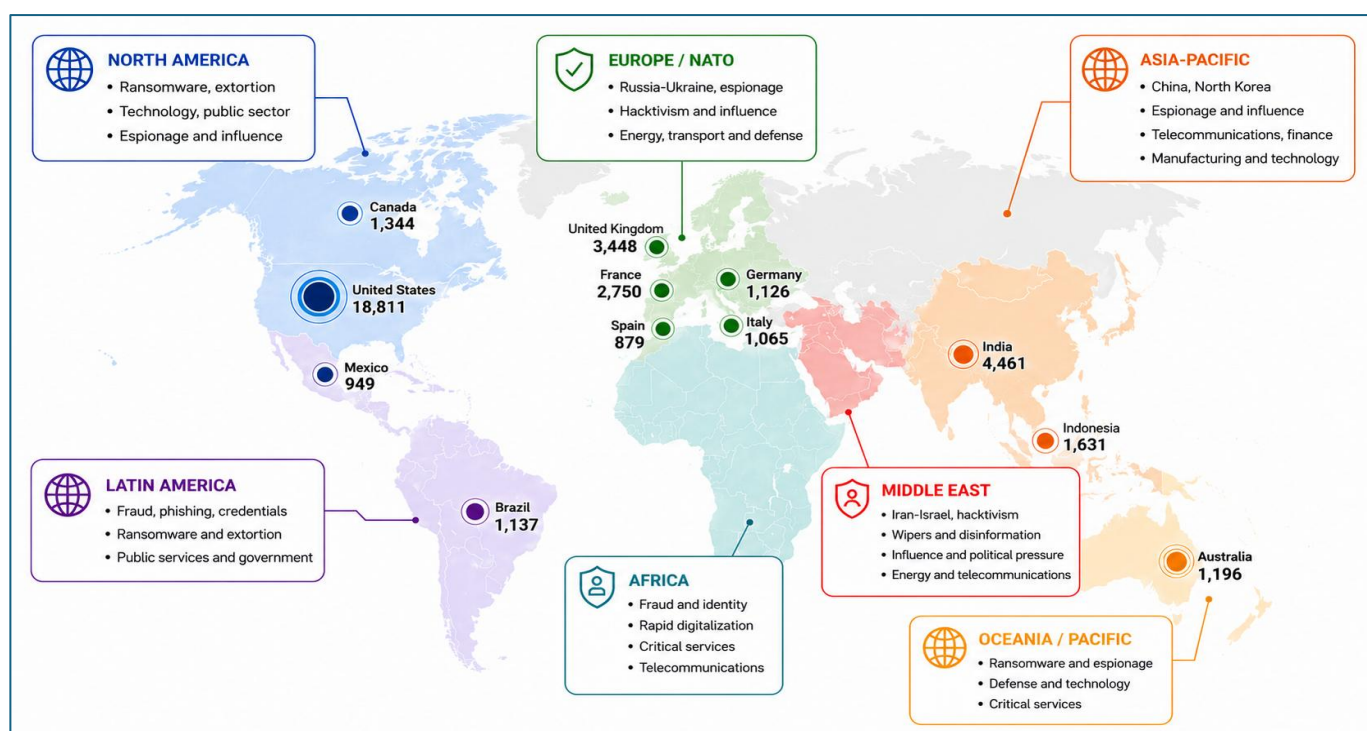


Figure 2 | Global map of cyber pressure and geopolitical context during the first half of 2026.

3.3 Impact of cyberattacks on specific regions and sectors

During H1 2026, **global malicious activity** once again shows that cyber pressure is not distributed solely according to the volume of available targets, but according to the combination of **digital exposure, operational criticality, economic value, geopolitical relevance, and ability to generate indirect impact**.

The data observed places **the United States** as the country with the highest visibility, followed by highly digitalized economies such as **India, the United Kingdom, France, Canada, Australia, Brazil, Germany, Italy, Mexico, and Spain**. This distribution should be interpreted as a signal of exposure and observed activity, not as an absolute measurement of the global volume of attacks.

At the geographic level, the observed pattern confirms that economies with greater dependence on digital services, broad business ecosystems, and presence of critical sectors are subject to greater pressure. The United States maintains outstanding exposure due to its economic, technological, and geopolitical weight; India reflects the impact of accelerated digitalization and its strategic role in the Indo-Pacific; while European countries such as the United Kingdom, France, Germany, Italy, and Spain remain exposed due to their integration into global supply chains, their support for Ukraine, their regulatory weight, and their dependence on digital public services. The presence of Brazil and Mexico also reinforces a relevant trend: Latin America should not be considered a peripheral environment, as it combines monetization of data, phishing,

ransomware, credential theft, and access brokerage.

From a sectoral perspective, attackers prioritize sectors where disruption, a leak, or indirect access can generate impact beyond the compromised entity itself: citizen services, industrial production, financial data, logistics continuity, customer trust, or access to third parties.

Public Administration remains one of the most pressured targets due to its symbolic value, institutional visibility, and role in delivering essential services. The weight of **Manufacturing** confirms sustained pressure on industrial sectors and environments with operational dependencies. Unlike other sectors where impact is concentrated on data or reputation, in manufacturing the risk can extend to production, logistics, OT, and physical continuity.

The **Education, Professional Services, and Information Technology** sectors maintain high exposure for different but connected reasons. Education combines broad attack surfaces, technological heterogeneity, and the high value of credentials, academic data, and research data.

Professional Services and Information Technology also act as trust nodes: consulting firms, SaaS providers, integrators, *cloud* platforms, and technology companies can become indirect access paths to third parties.

In **Finance, Retail, and Healthcare**, the motivation combines direct monetization, fraud, sensitive data, and reputational pressure. Finance remains a natural target due to the economic value of its assets and the trust that underpins the service; Retail and digital commerce concentrate exposure to fraud, credentials, and web availability; and Healthcare maintains a differentiated criticality due to data sensitivity and low tolerance for disruption.

Overall, H1 2026 victimology shows a relevant shift: the victim should no longer be analyzed only as the attacked organization, but as part of an ecosystem of dependencies. Impact can extend to third parties and connected sectors. Therefore, the countries and sectors most visible in the landscape do not only represent higher activity volume, but also a greater concentration of strategic, economic, and operational value.



Sectors with greatest cyber exposure and impact in H1 2026

Sector	Observed attacks	Exposure	Impact	CTI assessment
Public administration	9,454	Very high	High	High institutional visibility, citizen services, and political pressure; recurring target for DDoS, hacktivism, espionage, and leaks.
Manufacturing	5,478	High	Very high	IT/OT dependency, operational continuity, and supply chains; high impact in the event of disruption or extortion.
Education	5,271	High	Medium-high	Broad attack surface, reusable credentials, and lower defensive maturity; attractive target for data and access theft.
Finance and insurance	5,154	High	Very high	Direct monetization, fraud, sensitive data, and customer trust; high value for extortion and identity abuse.
Professional and technical services	5,123	High	High	Indirect access to clients, consulting firms, integrators, and critical providers; relevant supply chain vector.
Information / technology	5,097	Very high	Very high	SaaS, cloud, APIs, tokens, and third-party amplification capability; very high exposure and impact.
Retail	3,773	Medium-high	Medium-high	Payments, credentials, fraud, web availability, and customer data; high exposure due to transaction volume.
Health and social care	2,959	Medium-high	Very high	Sensitive data, operational urgency, and low tolerance for disruption; critical impact on continuity of care.
Transportation and logistics	2,078	Medium	High	Mobility, trade, and physical continuity; relevant impact during crises or regional disruptions.
Construction	1,284	Medium	Medium-high	Projects, contractors, sensitive documentation, and third-party dependency; growing supply chain risk.

Table 1 | Sectors with the greatest exposure, impact, and observed cyber activity during the first half of 2026.





4. Major Global Threats

During the first half of 2026, the global threat landscape was marked by intense and, at the same time, sustained activity. The level of coordination across campaigns is higher, and threat actors are increasingly capable of combining espionage, ransomware, and disruption techniques in long-range operations.

This period has confirmed a trend toward attacks that are more costly and harder to detect, driven largely by the integration of artificial intelligence into the attack lifecycle. Geopolitics has become further consolidated as a structural risk factor, capable of shaping both the nature of threats and the ability to coordinate response at the international level.

4.1. Notable cyber incidents and major campaigns

The first half of 2026 has left a set of high-impact incidents that confirm the operational maturity of today's threat actors. The most significant campaigns have targeted sectors of strategic value, such as healthcare, industry, and government, combining stealthy intrusion techniques, massive data exfiltration, and extortion as a pressure mechanism. Convergence between state actors and organized cybercrime groups has become more evident, making both attribution and coordinated response more difficult in most cases.

At **NTT DATA's Cyber Threat Intelligence Department**, we have documented some of the most relevant cyber incidents of the first half of 2026, selected for their representative value of the main threats observed during this period.

Victims	Sector	Attacker	Country / region affected	Origin of attacker	Date of incident	URL
Polish power grid	Energy and critical infrastructure	Electrum	Poland	Russia	January 2026	Source
Government and military entities (CEE)	Government and defense	APT28 GRU Unit 26165	Central and Eastern Europe	Russia	January 2026	Source
Indian government institutions	Government and defense	APT36 Transparent Tribe	India	Pakistan	January 2026	Source
French Ministry of Economy	Government and finance	Unknown	France	Unknown	February 2026	Source
Telecommunications operators in Singapore	Telecommunications	UNC3886	Singapore	China	February 2026	Source
Telus	Telecommunications	ShinyHunters	Canada	Global	March 2026	Source
Stryker	Technology and healthcare	Handala	Global	Iran	March 2026	Source
European Commission	Government	TeamPCP	European Union	Eastern Europe	March 2026	Source
FBI	Government and security	Unknown	United States	China	April 2026	Source

Victims	Sector	Attacker	Country / region affected	Origin of attacker	Date of incident	URL
Booking	Tourism	Unknown	Global	Unknown	April 2026	Source
Medtronic	Technology and medicine	Unknown	Global	Unknown	April 2026	Source
Foxconn – North American factories	Industry	Nitrogen Ransomware Gang	United States / Global	Unknown	May 2026	Source
Trellix	Cybersecurity	RansomHouse	Global	Russia	May 2026	Source
Instructure (Canvas)	Education	ShinyHunters	Global	Global	May/June 2026	Source

Table 2 | Major cybersecurity incidents in the first half of 2026.

At the same time, the first half of 2026 has shown a more fragmented and specialized threat ecosystem. A growing number of actors are combining automation and the exploitation of development environments with hybrid motivations, mainly geopolitical and financial, to operate with greater reach, persistence, and impunity.

Cyberattack campaigns in H1 2026 grouped by objective

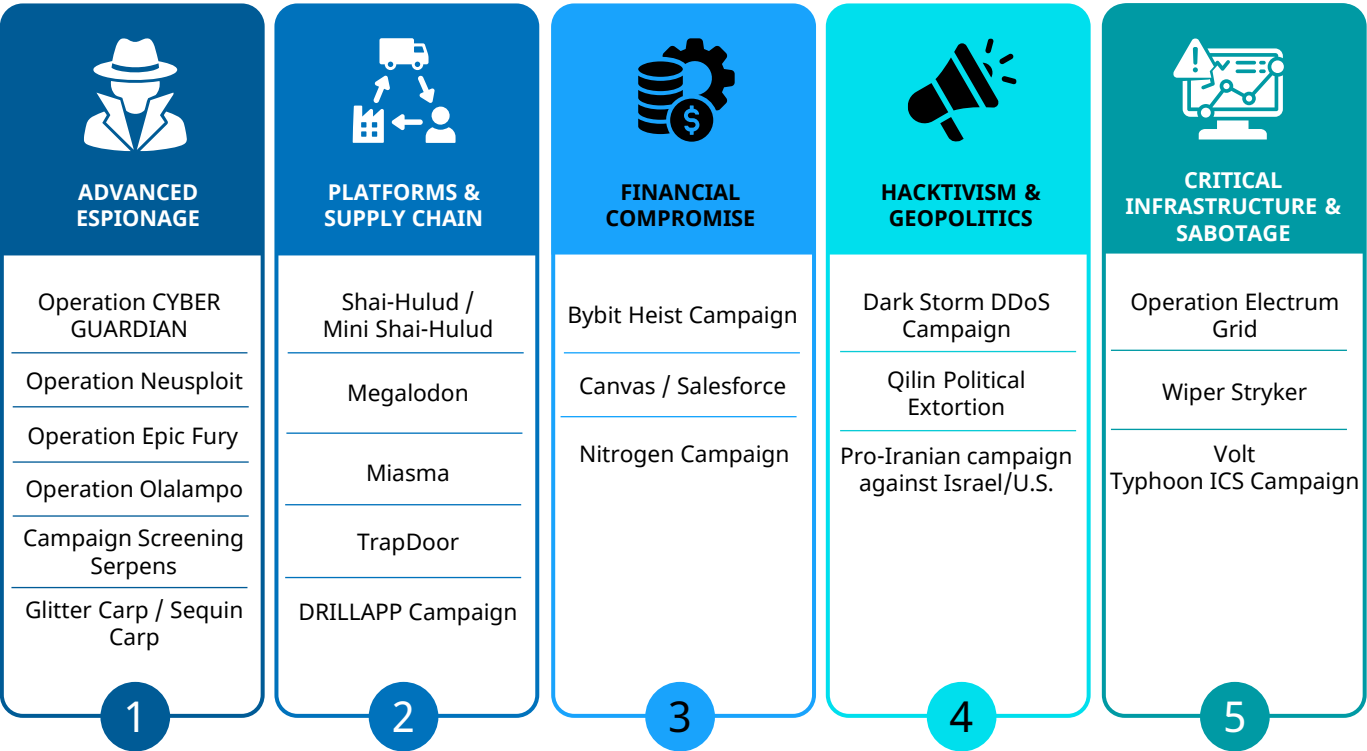


Figure 3 | Major campaigns detected in the first half of 2026.

4.2 Emerging attack trends

During the first half of 2026, a continued evolution in the offensive capabilities of threat actors has been observed, marked by shorter compromise times, greater reliance on obtaining and using legitimate identities, and the exploitation of artificial intelligence capabilities.

In this context, the following technical and operational trends have been identified as defining features of cyberspace activity during this first half of the year:

4.2.1 Credential compromise as the main access vector

Although vulnerability exploitation has become the leading initial access vector in 2026, the abuse of compromised credentials, authenticated sessions, and valid tokens remains a central mechanism for consolidating access, moving laterally, and maintaining persistence. Threat actors have reduced the need to exploit vulnerabilities at every stage of the intrusion, but they continue to rely on legitimate identities through techniques such as Adversary-in-the-Middle, advanced phishing, session hijacking, token theft, or OAuth abuse.

This trend has resulted in low-profile intrusions that are difficult to detect through standard controls.

4.2.2 AI-driven social engineering

Artificial intelligence has continued to act as a key operational enabler, particularly in the generation of highly personalized social engineering campaigns tailored to each target. It has also seen broad adoption in the automation of fraudulent emails, lure creation, falsification of corporate communications, and generation of multilingual content. The effectiveness of these operations has increased significantly due to their scalability and personalization capabilities.

4.2.3. Even faster vulnerability exploitation

The time between vulnerability disclosure and active exploitation has continued to shrink. Threat actors have demonstrated a growing ability to automatically identify vulnerable systems and deploy mass campaigns within hours. The main affected assets include perimeter devices, third-party components, and applications exposed to the Internet.

4.2.4 Focus on cloud and SaaS environments

Cloud and SaaS environments remain a priority attack surface. Observed intrusions have increasingly focused on the abuse of privileged accounts, synchronization between services, and insecure configurations.

The increased use of legitimate channels for information exfiltration continues to make it harder to distinguish between legitimate and malicious activity.

4.2.5 Cyber espionage targeting technological innovation

Cyber-espionage activity has shown growing interest in technology sectors, intellectual property, strategic information, and artificial intelligence. Campaigns involving prolonged access and advanced persistence mechanisms have been observed, primarily aimed at collecting information discreetly. This trend reflects the growing importance of technological and economic advantage from a geopolitical perspective.

4.2.6 Disruptive attacks against critical infrastructure

The generation of operational impact against critical infrastructure and its services continues to increase in importance.

To achieve this, technical capabilities are combined with economic, political, or reputational pressure objectives. Targeted campaigns have been observed using ransomware, wipers, and DDoS techniques to generate cascading effects. This trend reflects an evolution from models focused on information collection toward hybrid operations with greater disruptive potential.

4.3 Global statistics on security incidents, types of attacks and threat actors involved

During the first half of 2026, activity associated with ransomware has remained among the main threats in the global cybersecurity landscape, in a context marked by the evolution and reorganization of the criminal ecosystem. The observed data reflects **sustained activity at historically high levels**, accompanied by operational consolidation among the most active groups.

4.3.1 Security Incidents

Ransomware has remained the main driver of high-impact incidents. During the first quarter of 2026, **2,122 victims were published on data leak sites**, the second-highest figure ever recorded for a first quarter. Although this represents a **12.2% decrease** compared with the all-time high reached in the fourth quarter of 2025 ([Check Point Research, 2026](#)), the data continues to reflect sustained activity at very high levels.

This evolution confirms the consolidation of ransomware as one of the most **persistent** and disruptive threats in the current threat landscape.

4.3.2 Types of attacks and predominant vectors

Ransomware was present in **48% of breaches** analyzed globally during 2026 ([Verizon, 2026](#)), compared with 44% in the previous period, consolidating its position as the vector with the greatest operational and economic impact. **Infostealers** have become the most active malware variant, with more than **155,000 detections recorded** in early 2026 ([SentinelOne, 2026](#)), mainly used as a mechanism for environment preparation and credential theft. Meanwhile, **DDoS attacks** have maintained a significant presence in the technology sector, with a **45% share** at network-layer level ([Radware/GlobeNewswire, 2026](#)), retaining a tactical and complementary role in disruption operations.

Regarding entry vectors, vulnerability exploitation has surpassed credential theft as the main initial access route, being present in **31% of breaches**.

This reflects how quickly attackers operationalize publicly disclosed vulnerabilities. The fact that the number of confirmed ransomware victims has **increased by 53%** ([Check Point Software / StockTitan, 2026](#)) confirms the pattern of professionalization and intensification of activity.



Security incidents

2,122

victims published on data leak sites during the first quarter of 2026.

-12.2%

variation compared with the all-time high recorded in the fourth quarter of 2025.



Types of attacks and predominant vectors

48%

of breaches analyzed globally are related to ransomware during the first quarter of 2026.

+155,000

infostealer detections recorded in early 2026.

45%

of network-layer attacks correspond to DDoS in the technology sector.

From the perspective of technological evolution, **artificial intelligence configuration files** have consolidated as a new supply chain risk, requiring the same level of scrutiny as third-party code dependencies. In addition, credentials for accessing artificial intelligence models are also being actively collected at scale. This vector confirms that **the adoption of artificial intelligence** by organizations is expanding the exposure surface as quickly as it is deployed, without necessarily keeping pace with the security controls associated with it.

4.3.3 Threat actors and ecosystem dynamics

The criminal ecosystem has shown a relevant shift compared with the fragmentation observed in the previous semester, especially in the ransomware landscape. After a year of sustained growth, the trend has reversed: **the ten most active ransomware groups have accounted for 71.1% of published victims** ([Check Point Research, 2026](#)).

This consolidation does not imply a reduction in activity at the global level, but rather a **reorganization of the RaaS model** toward more capable operators that absorb more affiliates.

Likewise, notable **resilience in the credential-theft market** has been observed despite dismantling actions. Despite disruptions against major operators, the ecosystem has been able to continue growing. **Infostealers** exfiltrated more than **1.8 billion credentials** ([Shattered.io / DeepStrike, 2026](#)) including, in pairs, corporate and personal email accounts with their corresponding passwords. This pattern confirms that disruptions generate temporary impact, but are not able to stop **the adaptability** of underground markets, which turn to new malware families.

Overall, statistics from the first half of 2026 reflect a criminal ecosystem that is more concentrated around ransomware, more resilient in credential theft, and more capable of rapidly reorganizing around actors with greater operational capacity.

Global statistics by type of attack in 2026

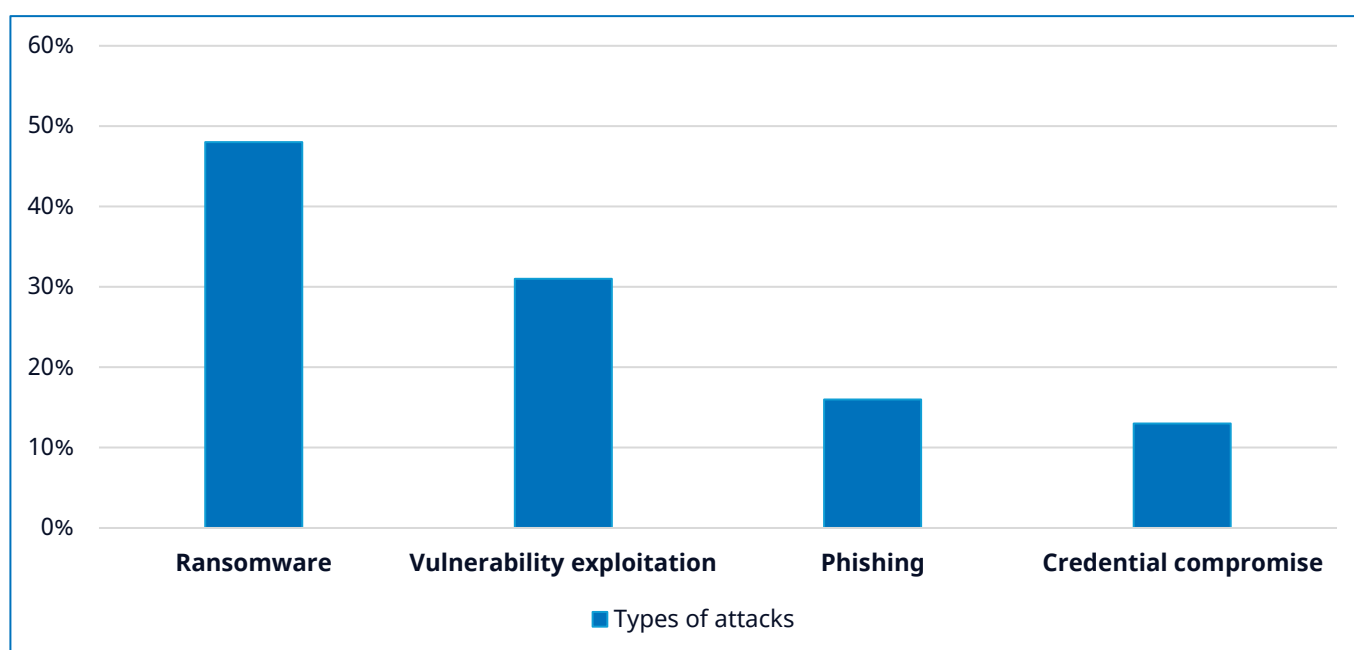


Figure 4 | Frequency of attacks by type during 2026 ([Verizon, 2026](#))

4.4 Costs of cyberattacks for organizations

The first half of 2026 has confirmed that cybercrime now operates as a parallel economy on a scale comparable to that of major industrial powers, with a global impact that **exceeds USD 12.5 trillion annually** (Aftra, 2026). This figure would place any country among the largest economies in the world, far ahead of most national GDPs.

During the period, ransom payment dynamics have shown a contradictory pattern: **while the volume of attacks increases, victims' behavior is becoming more resistant**. The percentage of affected organizations that agreed to pay now stands at only between 20% and 28%. These are the lowest figures recorded to date, compared with rates that, just a couple of years ago, exceeded 60–70% (SOSRansomware, 2026). Even so, money continues to flow to attackers. In the case of blockchain, tracked payments have reached USD 820 million globally, distributed across a much larger number of incidents, but with lower individual amounts. This trend confirms a clear shift in the criminal business model toward volume rather than value. Although ransomware groups continue to demand very high amounts, the average effective payment stands at **USD 592,000**, with a median of **USD 325,000** (SecurityToday, 2026), figures well below the amounts that usually receive greater media attention.

The true cost rarely matches the ransom demanded. Therefore, **costs arising from operational disruption, system recovery, legal obligations, regulatory notifications, and reputational damage** have continued to carry more weight than the amount paid as ransom.

In this regard, geography continues to show notable differences. The United States leads the global ranking with an average breach cost of **USD 10.22 million** (StationX, 2026). This is the highest figure ever recorded for the country, driven by increasingly costly regulatory penalties and litigation. In second place, the Middle East remains one of the regions with the greatest economic exposure globally, with **USD 7.29 million** per incident (StationX, 2026). The global average breach cost stood at **USD 4.44 million** (StationX, 2026), notably below the U.S. figure, with Europe remaining below that average thanks to more mature regulatory frameworks and more standardized incident response processes across its organizations. This geographic gap reflects both regulatory differences and varying levels of maturity in each region's detection and containment capabilities.

Finally, the underground economy that sustains this entire ecosystem has become drastically cheaper during the semester. Access to a compromised corporate network has seen a **price drop of nearly 70%**. It currently costs an average of **USD 439**, compared with **USD 1,427** just three years ago (Crypto-Economy, 2026).

This deflation is driven by automation, the use of AI-assisted tools during reconnaissance phases, and the oversupply of credentials stolen through infostealers. Access to cybercrime is becoming democratized, significantly expanding the pool of actors capable of monetizing an intrusion, even with limited technical capabilities.

A woman with dark, curly hair is shown from the waist up, wearing a dark blue pinstriped blazer over a blue t-shirt and blue jeans. She is holding a tablet in her left hand and looking off to the side with a slight smile. The background is a blurred office interior with large windows and modern lighting. In the bottom right corner, there is a white graphic overlay consisting of a grid and a large arc.

5. Legal framework and arrests in cybersecurity

For NTT DATA's Cyber Threat Intelligence Department, it is considered essential to analyze the security and cybersecurity laws approved, as well as the operations carried out by law-enforcement agencies worldwide during the first half of 2026.

This analysis makes it possible to assess countries' commitment to regulating current and emerging technologies, as well as the joint efforts of legislative, judicial, and law-enforcement mechanisms to strengthen digital resilience and combat illicit activities in cyberspace.

5.1 Main laws in the field of cybersecurity

In the first half of 2026, the cybersecurity legal and

regulatory framework continued to advance toward an approach based on operational resilience, product security, critical infrastructure protection, reporting obligations, and supervision of technology providers.

Among the most relevant developments are the continued development of the **Cyber Resilience Act** in the European Union, the update of the European sanctions regime against cyberattacks, the progressive implementation of the CMMC in the United States, the publication of new NIST and CERT-In guidance, the entry into force of the reform of China's **Cybersecurity Law**, and the application in Australia of obligations for smart devices and ransomware payment reporting.

Continent	Regulation	Institution	Reference
Europe	Delegated Regulation (EU) 2026/881. Development of the Cyber Resilience Act.	European Commission / EUR-Lex	EUR-Lex - Delegated Regulation (EU) 2026/881
Oceania	Smart Devices Rules 2025. Minimum requirements for smart devices.	Department of Home Affairs / Government of Australia	Australian Department of Home Affairs - Security Standards for Smart Devices
Canada	Bill C-8 / An Act Respecting Cyber Security. Protection of critical cyber systems.	Government of Canada / Public Safety Canada	Public Safety Canada - Royal Assent of Bill C-8
North America	CMMC Phase 1. Cybersecurity maturity for DoD providers.	U.S. Department of Defense / DoD CIO	DoD CIO - Cybersecurity Maturity Model Certification
North America	NIST SP 800-172 Rev. 3 / 172A Rev. 3. Enhanced protection of sensitive information.	NIST / CSRC	NIST CSRC - SP 800-172 Rev. 3; NIST CSRC - SP 800-172A Rev. 3
Asia	Reform of China's Cybersecurity Law. Update of the compliance and sanctions regime.	National People's Congress / Government of China	Library of Congress - China: Amended Cybersecurity Law Takes Effect
Latin America	Decree 941/2025 and Provision 1/2026. National cybersecurity governance in Argentina.	National Executive Branch / National Cybersecurity Center / Official Gazette of Argentina	Official Gazette - Decree 941/2025; Official Gazette - CNC Provision 1/2026

Table 3 | Laws approved or applicable in the first half of 2026.

These developments reinforce the connection between regulation and real-world threats. The new obligations are aimed at reducing exploitable attack surfaces, improving asset visibility, and raising security requirements for providers, digital products, and critical infrastructure. This confirms a trend toward more operational frameworks, where compliance is increasingly linked to the ability to prevent, detect, respond to, and recover from advanced threat actors.



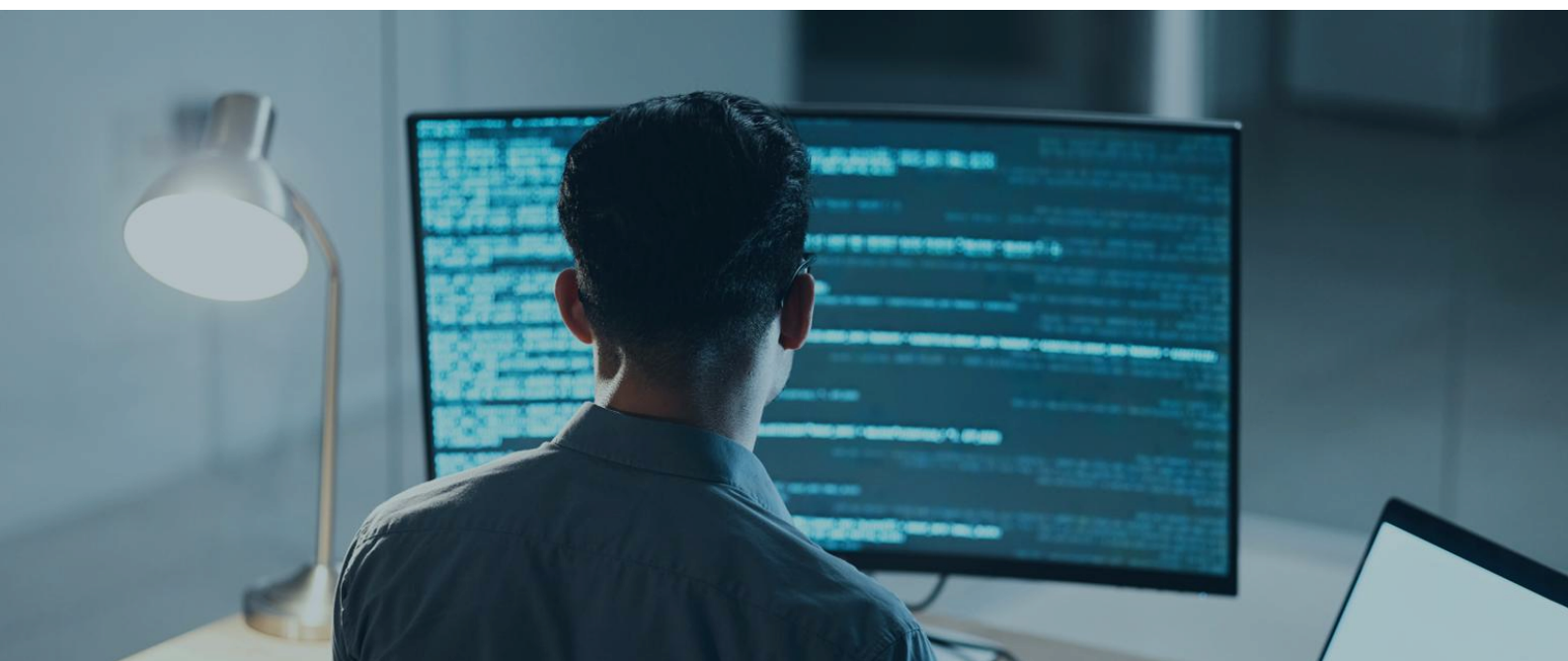
5.2 Major arrests in the field of cybersecurity

During the first half of 2026, international law-enforcement and judicial cooperation against cybercrime remained highly active. The most relevant operations focused on neutralizing criminal infrastructures used for phishing, malware, ransomware, DDoS, financial fraud, criminal VPN services, botnets, and residential proxy networks.

These actions, coordinated by organizations such as INTERPOL, Europol, Eurojust, the U.S. Department of Justice, national police forces, and national cybersecurity centers, reflect a consolidated trend toward operational disruption models, where technical intelligence, cross-border cooperation, and infrastructure seizure are key to reducing the operational capacity of criminal groups.

Operation	Threat group or sector	Security forces and agencies	Results	References
Operation Ramz	Phishing, malware, and online fraud	INTERPOL and authorities from 13 MENA countries	201 arrests , 382 suspects identified, 3,867 victims located, and 53 servers seized .	INTERPOL Press Release
First VPN / Operation Saffron	Criminal VPN used for ransomware, intrusions, and activity concealment	Europol, Eurojust, and authorities from France, the Netherlands, Ukraine, and other countries	33 servers dismantled and search/questioning of a suspect in Ukraine.	Europol / Eurojust
KimWolf Botnet	DDoS-for-hire / IoT botnet	DOJ, FBI, DCIS, Canadian authorities, and international partners	Arrest in Canada of the alleged administrator; KimWolf had allegedly infected more than one million devices .	DOJ Press Release
Residential proxy botnet	Botnet / residential proxies	Dutch Police and NCSC-NL	Dismantling of a botnet involving at least 17 million infected devices and around 200 servers in the Netherlands.	NCSC-NL / Politie.nl
FIOD hosting takedown	Hosting infrastructure linked to cyberattacks and sanctions evasion	FIOD and Dutch authorities	2 arrests and more than 800 servers seized in an investigation into support for sanctioned entities.	FIOD
Spain-France banking CaaS	Phishing, smishing, and banking fraud under a Crime-as-a-Service model	Spanish National Police, Europol, Hanover Police, and French authorities	3 arrests , EUR 1.5 million in cryptoassets located, and more than EUR 4 million in losses identified.	Ministerio del Interior
Operation KRATOS 2	Illegal streaming and organized digital crime	Europol and European authorities	29 arrests , nine criminal groups dismantled, and more than 27,000 illegal URLs removed.	Europol
Operation Endgame / SocGhosh	Malware, Initial Access Broker, ransomware enablement	Dutch Police, Canada, United States, Germany, Europol, and Eurojust	Cleanup of 14,971 infected WordPress sites , dismantling of infrastructure associated with SocGhosh, and action against a network linked to Evil Corp.	Politie.nl; Operation Endgame

Table 4 | Major operations to dismantle cybercriminal gangs carried out in H1 2026.



Featured case: Operation Endgame and the offensive against SocGholish

In June 2026, a new phase of **Operation Endgame** targeted the **SocGholish** infrastructure, also known as **FakeUpdates**, a malware operation used to compromise legitimate websites and facilitate subsequent infections.

The action was coordinated by authorities from the Netherlands, Canada, the United States, Germany, and other international partners, with support from Europol and Eurojust.

The **Operation** made it possible to clean **14,971 infected WordPress sites** and deactivate **106 servers and domains** linked to the criminal infrastructure. This volume makes the case one of the most relevant actions of the semester against malware distributed through compromised legitimate websites.

The relevance of the case lies not only in the volume of intervened infrastructure, but also in the role of **SocGholish** as an enabler of initial access. This type of malware makes it possible to compromise legitimate users through fake browser update warnings and can serve as an entry point for credential theft, deployment of additional tools, or campaigns associated with ransomware.

In addition, the case connects to high-profile actors. Dutch police link **SocGholish** to **Evil Corp**, a group historically associated with malware, financial fraud, and ransomware operations.

This reinforces the value of **Operation** as an action against cybercrime-enabling infrastructure, not only against a specific malware family. In strategic terms, **Operation Endgame** shows the evolution of law-enforcement operations toward large-scale cleanup and disruption actions.



By remediating thousands of compromised websites and deactivating associated infrastructure, **authorities reduce the infection surface available to operators, hinder the continuity of active campaigns, and force actors to rebuild part of their technical ecosystem.**

Complementary case: Operation Saffron and the dismantling of First VPN

Another relevant **Operation** during the semester was **Operation Saffron**, targeting **First VPN**, a service promoted on Russian-speaking cybercrime forums as a tool to maintain anonymity and avoid cooperation with authorities.

Europol indicated that this service appeared in virtually all major cybercrime investigations supported by the agency in recent years.

The **Operation** enabled the seizure of 33 servers distributed across several countries and the search and questioning of a suspect in Ukraine. The case is notable because First VPN was used by actors linked to ransomware, data theft, malicious scanning, and DDoS attacks, meaning that its dismantling affected a cross-cutting anonymization layer of the criminal ecosystem.

Regulation, disruption, and operational impact

The first half of 2026 confirms a relevant evolution in the way states and international organizations address cybercrime. The legal framework is moving toward more technical and verifiable obligations, while law-enforcement operations show greater capacity to act against complex and distributed criminal infrastructures. This dual trend reflects a shift in approach: institutional response is no longer limited to pursuing specific attacks, but seeks to reduce the structural capacity of actors to operate, scale, and monetize their campaigns.

The new regulations analyzed during the semester reinforce areas directly related to the main threats observed in recent years: product security, critical infrastructure protection, supplier oversight, incident response, sensitive information protection, and reduction of exploitable vulnerabilities. This approach is particularly relevant in a context where criminal groups increasingly depend on supply chains, compromised legitimate services, exposed devices, stolen credentials, and third-party infrastructure to sustain their operations.

In parallel, law-enforcement operations during the semester show greater maturity in disrupting the criminal ecosystem.

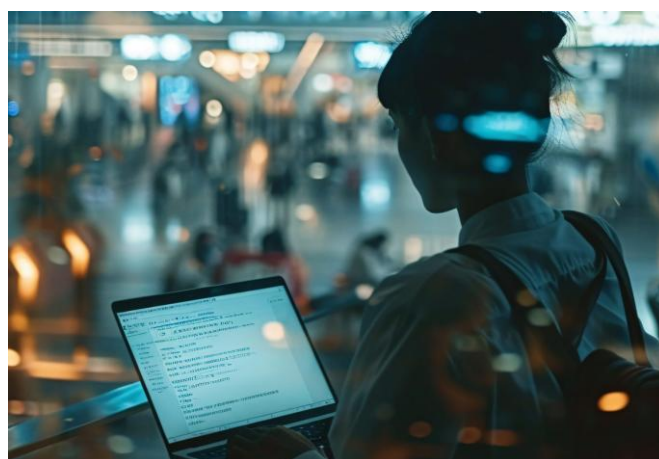
Cases such as **Operation Endgame / SocGhosh**, linked to infrastructure used to compromise thousands of websites and associated with actors such as **Evil Corp**, show that authorities are prioritizing cybercrime-enabling services.

The cleanup of compromised websites, seizure of servers, dismantling of criminal VPN services, neutralization of botnets, and identification of operators make it possible to simultaneously affect multiple campaigns, rather than being limited to a single victim or incident.

This evolution is significant because many criminal operations depend on shared services: anonymization infrastructure, malware, initial access, hosting, botnets, and fraud networks. When a law-enforcement **Operation** impacts one of these components, the effect can extend to several campaigns and force actors to migrate, rebuild infrastructure, or modify their procedures.

Although these actions do not eliminate the threat, they do increase the operational cost of cybercrime and temporarily reduce its capacity. In addition, the information obtained during takedowns can feed new investigations and improve visibility into relationships between actors, services, and infrastructure.

Overall, the semester shows growing convergence between regulation, technical intelligence, and law-enforcement action, consolidating a more coordinated response to an increasingly distributed and professionalized criminal ecosystem.



6. Dark Web Insights



During the first half of 2026, the **underground ecosystem maintained a high level of activity**, but under growing law-enforcement and operational pressure. The **seizure of forums, closure of services** used by criminal actors, and operations against enabling infrastructure did not reduce demand for stolen data, credentials, compromised access, or offensive tools, but they did accelerate the fragmentation of the ecosystem ([SOCRadar, 2026a](#); [U.S. Department of Justice, 2026](#)).

The period was marked by greater distrust of large centralized hubs. Actors, sellers, and affiliates continued to migrate toward alternative forums, private channels, Telegram, invitation-only communities, and markets specializing in logs, credentials, initial access, and fraud services. In this context, reputation, actor-to-actor verification, and the ability to operate in less visible spaces became key elements for sustaining criminal activity ([SOCRadar, 2026](#)).

A greater presence of **artificial intelligence** was also observed in conversations and offerings within underground communities. Its use appears mainly linked to automation, content generation for phishing, social engineering, analysis of stolen data, and support for tool development, although real capabilities, experimentation, and exaggerated commercial claims still coexist ([Sophos, 2026](#)).

6.1 Law-enforcement pressure and reconfiguration of the underground ecosystem

The first half of 2026 was marked by new actions against platforms used for the trade of stolen data and criminal services. The most relevant case was the dismantling of **LeakBase**, a U.S.-led and internationally coordinated operation that affected one of the largest forums for the sale of stolen information.

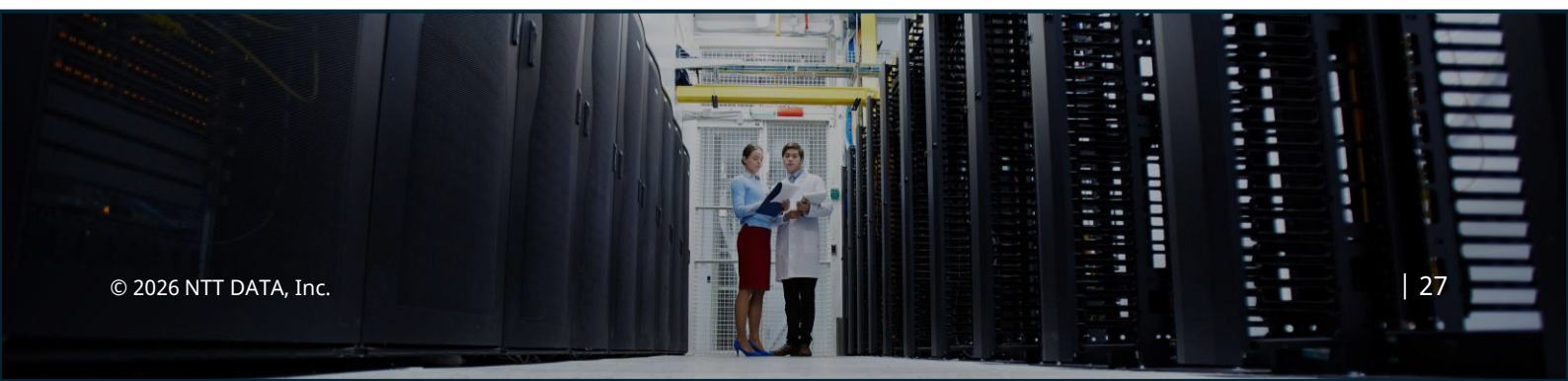
According to the U.S. Department of Justice, **LeakBase had more than 142,000 members and over 215,000 private messages**, and allowed its users to sell information obtained from stolen databases, credentials, and other illicit data ([U.S. Department of Justice, 2026](#)).

The operation enabled the seizure of domains, forum data, accounts, posts, private messages, and technical records, increasing the risk for users and sellers who had used the platform. Beyond the closure of the forum, the main impact lies in the loss of trust: when a centralized platform falls under law-enforcement control, internal information can feed subsequent investigations and expose relationships between actors, buyers, sellers, and infrastructure ([U.S. Department of Justice, 2026](#)).

In parallel, the seizure of **RAMP**, a forum historically associated with ransomware and related services, reinforced the perception that even specialized spaces with high operational value can be reached. SOCRadar notes that between 2025 and early 2026, several dominant forums were disrupted, including **LeakBase, RAMP, and BreachForums**, reflecting a reconfiguration of the ecosystem toward more segmented platforms and private channels ([SOCRadar, 2026a](#)).

The result is not the disappearance of criminal activity, but its redistribution. Pressure on major forums accelerates the shift toward alternative spaces, reduces trust in administrators and sellers, and forces actors to diversify their communication, sales, and recruitment channels.

For CTI monitoring, this implies a more dispersed, less visible environment that is increasingly dependent on reputation, private access, and continuous tracking of migrations.



6.2 Active underground forums

During the first half of 2026, activity on underground forums remained active, although more distributed than in previous periods. Following the disruption of consolidated platforms, part of the activity shifted toward Russian-speaking technical forums, leak communities, marketplace discussion spaces, and private channels used for the sale of access, credentials, tools, and criminal services ([SOCRadar, 2026](#)).

The most relevant forums during the period can be grouped into three major categories:

- **Russian-speaking technical forums**

Platforms such as **Exploit.in** and **XSS** remained relevant spaces for actors with greater technical specialization, particularly around exploits, initial access, malware, offensive services, and the sale of compromised information. Both forums are among the main spaces monitored in 2026, together with other environments such as **BHF** and **DamageLib** ([SOCRadar, 2026a](#)).

- **Discussion, reputation, and marketplace communities**

Dread maintained its role as one of the main discussion spaces within the darknet ecosystem, with functions similar to a social forum where marketplaces, vendor reputation, scam alerts, platform takedowns, and operational changes are discussed. These types of communities not only concentrate criminal activity, but also act as a mechanism of trust and validation between actors ([SOCRadar, 2026](#)).

- **English-speaking forums for leaks, cracking, and credentials**

Forums such as **Cracked**, **DarkForums**, **CryptBB**, and **Altenen** continued to appear in investigations and monitoring of activity related to leaked credentials, combo lists, stealer configurations, automated tools, exposed databases, and fraud services. These spaces tend to attract profiles with different levels of technical capability and function as entry points for less sophisticated actors, but also as

distribution channels for data useful in subsequent campaigns ([SOCRadar, 2026a](#); [CloudSEK, 2026](#)).

Overall, the semester confirms that activity does not disappear after the takedown or seizure of major forums, but is redistributed toward alternative platforms and communities with different levels of access.

This reconfiguration, which began in late 2025 and consolidated during the first half of 2026, reduces direct visibility into certain operations and increases the importance of monitoring secondary spaces, private channels, and specialized communities.

Following the disruption of consolidated platforms, part of the activity shifted toward technical forums, leak communities, and channels for the sale of criminal services.

Active underground forums and spaces in H1 2026

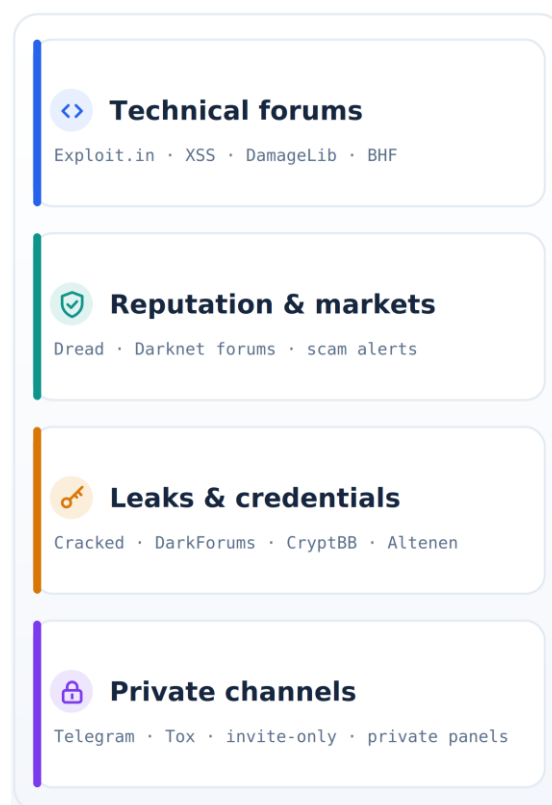


Figure 5 | Main types of active underground forums and spaces during the first half of 2026.

Main publications on the dark web in H1 2026

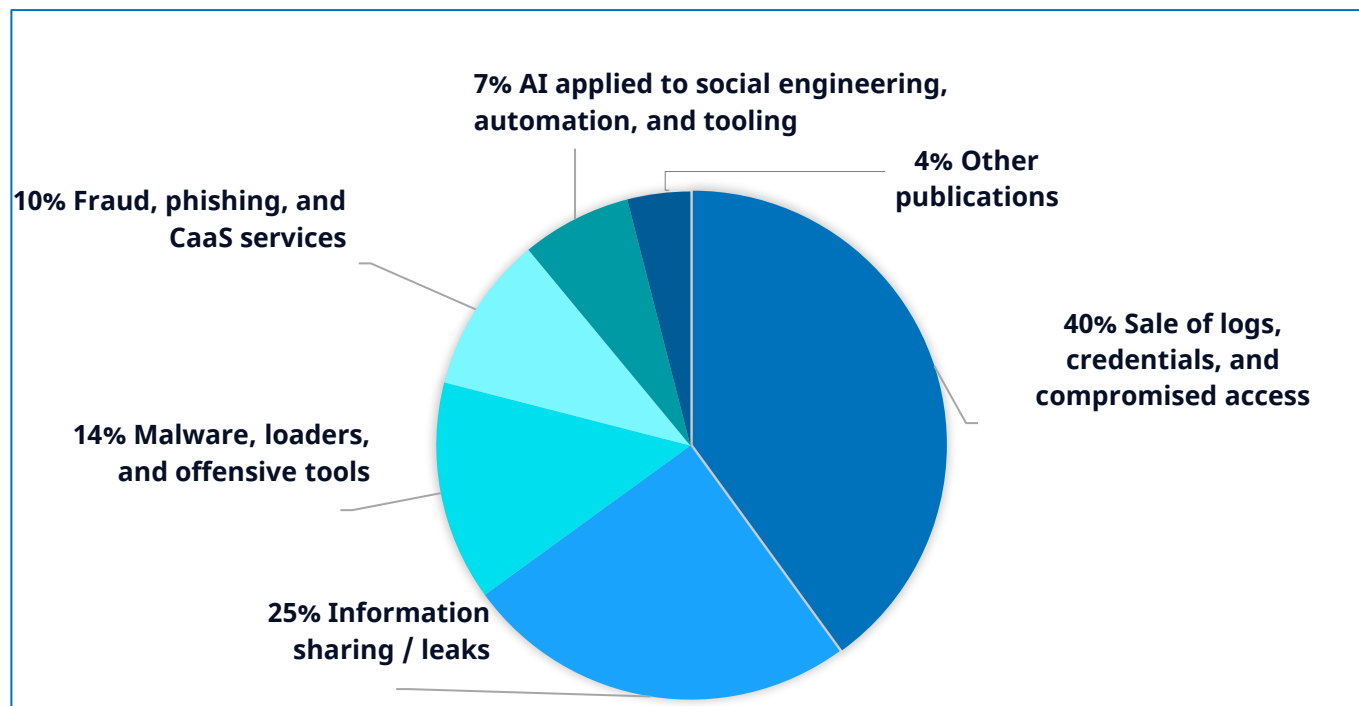


Figure 6 | Main categories of publications on the dark web in the first half of 2026.

The estimated data shows an underground ecosystem increasingly oriented toward the monetization of credentials, infostealer logs, and compromised access. Although information sharing and leaks remain relevant, they are losing relative weight compared with markets more specialized in initial access, fraud, offensive tools, and criminal services.

During the first half of 2026, a growing presence of publications linked to artificial intelligence was also observed, especially in automation, phishing content generation, social engineering, and support for tool development, although real adoption continues to coexist with effective capabilities, experimentation, and exaggerated commercial claims ([SOCRadar, 2026b](#); [Sophos, 2026](#)).

6.3 Active underground markets

During the first half of 2026, the underground market ecosystem remained active, although with a more fragmented and specialized structure. Law-enforcement disruptions, forum closures, and

instability in some markets did not reduce criminal activity, but instead favored redistribution toward platforms focused on credentials, infostealer logs, initial access, payment data, and fraud services ([SOCRadar, 2026b](#); [BreachSense, 2026](#)).

Markets focused on credentials and logs remain particularly relevant. Platforms such as **Russian Market** continue to play a central role in the sale of stolen credentials, cookies, browser data, corporate access, and records from infostealers. This model reinforces the connection between underground markets, initial access brokers, and subsequent fraud, intrusion, or ransomware campaigns ([SOCRadar, 2026b](#); [BreachSense, 2026](#)).

In parallel, carding and financial fraud markets retained a relevant role within the ecosystem. **BriansClub** continued to appear as a historic reference in the sale of compromised payment cards, while markets such as **STYX Market** remained active in fraud, phishing, illicit financial services, and operational support tools.

Although carding has lost some prominence compared with stealer logs and corporate access, it remains a structural category within the digital criminal economy (SOCRadar, 2026b).

The consolidation of markets with a broader or more specialized focus on intrusion services was also observed. Platforms such as **TorZon Market**, **Exodus Marketplace**, **Vortex Marketplace**, **Anubis Market**, **FreshTools**, and **WeTheNorth Market** appear in intelligence sources as relevant spaces for tracking stolen data, tools, access, fraudulent services, and distributed criminal activity. Their relevance varies over time, but they reflect an ecosystem in which sellers migrate quickly when a market falls, loses trust, or becomes less operational (SOCRadar, 2026b; DeepStrike, 2026).

The main trend during the semester is functional specialization. Markets no longer act only as generalist buy-and-sell platforms, but as **nodes within a broader criminal chain**: some facilitate credentials, others provide initial access, others concentrate compromised cards, and others offer fraud services or offensive tools. This division allows actors with different levels of sophistication to access criminal resources under increasingly professionalized models.

At the operational level, this fragmentation makes it necessary to expand monitoring beyond dominant markets. Actors alternate between marketplaces, forums, private channels, and closed services to reduce exposure, maintain reputation, and ensure commercial continuity. Therefore, underground market monitoring should focus not only on specific platforms, **but also on data flows, vendors, product categories, and migrations between spaces.**

Role of underground marketplaces in H1 2026

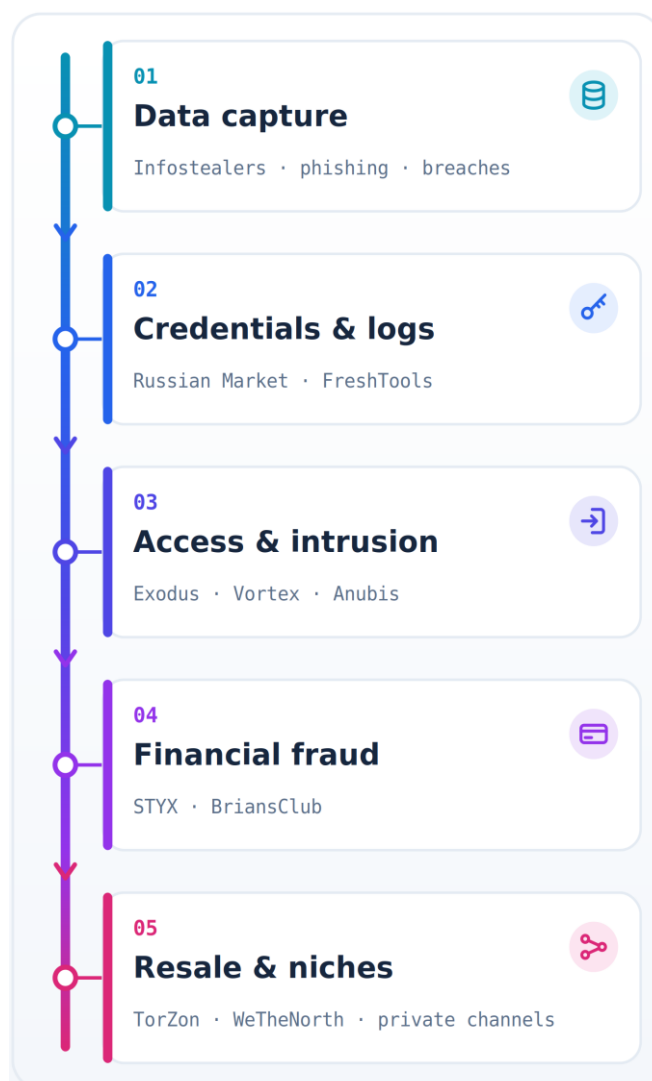


Figure 7 | Role of the main underground marketplaces within the criminal chain during the first half of 2026.



Although carding has lost some prominence compared with stealer logs and corporate access, it remains a structural category within the digital criminal economy.

The estimated distribution of the main underground sales platforms active during the first half of 2026 is shown below, based on observed activity volume, criminal specialization, and relevance within the ecosystem.

Underground sales platforms in H1 2026

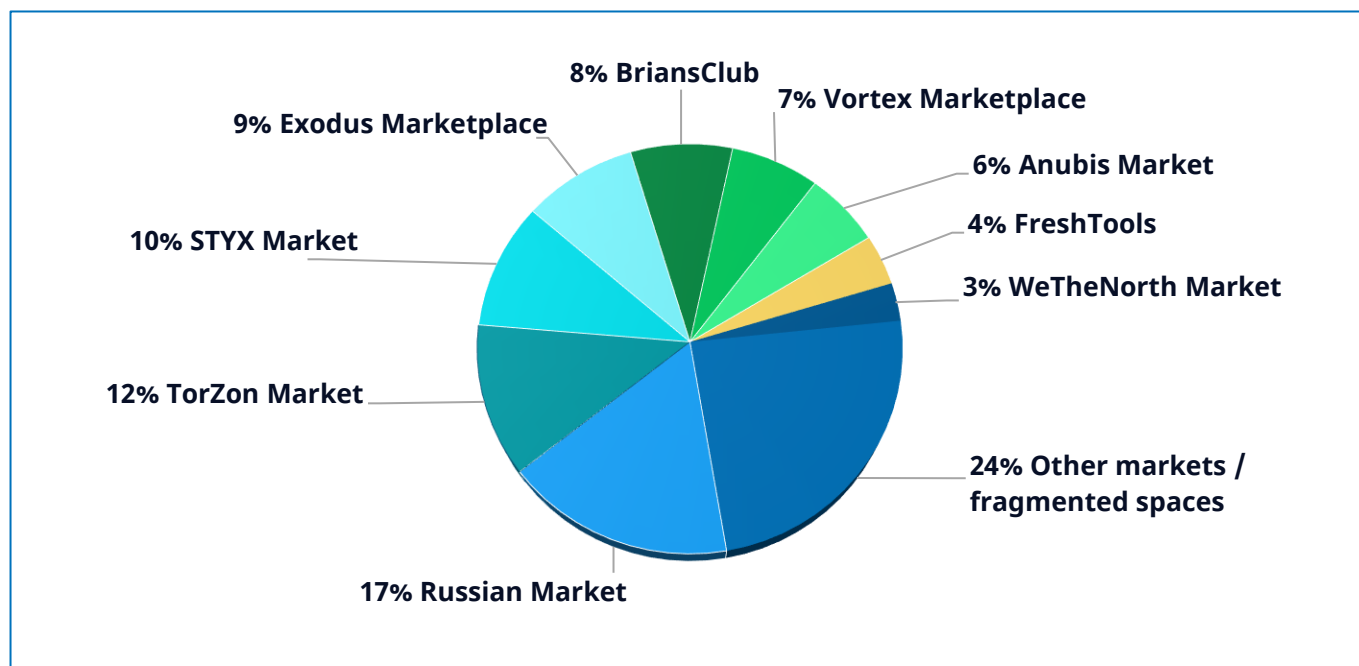


Figure 8 | Main underground sales platforms identified in the first half of 2026.

The estimated distribution reflects a more fragmented and functionally specialized underground market ecosystem. **Russian Market** remains particularly important due to its focus on credentials, stealer logs, cookies, and corporate access, while **STYX Market, Exodus Marketplace, and TorZon Market** concentrate activity related to fraud, access, tools, and criminal services.

The weight of “other markets / fragmented spaces” highlights the loss of centrality of major marketplaces and the shift toward niche platforms, private channels, and shorter-lived services.

A person with glasses and a beard is seen in profile, working at a desk with multiple computer monitors. The room is dimly lit with a blue tint. The person's hands are on a keyboard. A coffee cup is on the desk. In the background, another person is visible. A white geometric graphic, consisting of a semi-circle and a grid, is overlaid in the bottom right corner.

7. Threat Actors

The semester has confirmed a more hybrid and difficult-to-attribute ecosystem, where **cybercrime, espionage, and hacktivism converge in techniques, infrastructure, and objectives.**

Selective exfiltration, advanced social engineering, and abuse of legitimate services have predominated, while small, agile groups and temporary alliances sharing TTPs have proliferated, amplifying the impact of their operations.

7.1 Newly identified threat actors

The previous semester's report highlighted the growing **diversification** of the threat ecosystem and the emergence of increasingly specialized actors. The new groups identified during this period reflect that evolution through differentiated operational profiles ranging from strategic **cyber espionage** activity to **information theft campaigns aimed at fraud**. Their activity shows a **more fragmented** landscape, in which emerging actors develop specific capabilities to achieve concrete objectives, whether obtaining sensitive intelligence or illicitly monetizing compromised data. Likewise, **the collection and exfiltration of information** continued to consolidate as one of the main operational objectives, regardless of the final motivation of the actors involved.

Diaoyu

Detected in February 2026, **Diaoyu** is a threat actor linked to **cyber espionage** activities and allegedly aligned with **Chinese** state interests. The group has carried out campaigns targeting government organizations, research entities, and strategic organizations in at least 37 countries, compromising more than 70 institutions through the use of customized malware and advanced persistence and evasion techniques.

Its activity is characterized by long-running operations aimed at obtaining sensitive intelligence, leveraging covert infrastructure and tools developed specifically to avoid detection. Although definitive attribution remains limited, several indicators point to a highly sophisticated operation with significant resources, reinforcing the hypothesis of state backing.

Despite the recent public exposure of its activities, there is no evidence that the group has ceased operations, meaning it continues to be considered an active threat to government organizations and strategic sectors globally ([Shenouda, 2026](#)).



Insomnio

Also publicly identified in February 2026, **Insomnio** is a threat actor **specialized in the distribution of Android malware** through social engineering campaigns targeting mobile device users. Its activity focuses on impersonating legitimate applications and using fraudulent websites to induce victims to install malicious applications capable of collecting credentials, financial information, and other sensitive data.

The group stands out for its use of adaptable distribution infrastructure and rapid rotation of malicious domains and resources to hinder detection and blocking. Although its known activity has mainly focused on information theft, the observed capabilities suggest an evolution toward broader mobile fraud and account compromise operations.

Its emergence reinforces the growing trend of emerging actors exploiting the Android ecosystem as a primary vector for access to sensitive information and illicit monetization ([Shenouda, 2026](#)).

7.2 Ransomware

Ransomware activity during the first half of 2026 has confirmed the consolidation of a highly **competitive** ecosystem, characterized by the maturity of the **Ransomware-as-a-Service (RaaS)** model, affiliate mobility, and growing adaptability among the main operators.

The persistence of campaigns at a global scale, the emergence of new actors capable of gaining relevance quickly, and the continuity of strategies based on double extortion reflect an increasingly **professionalized** landscape. In this context, ransomware groups have maintained their focus on organizations and sectors where operational disruption, reputational pressure, and the value of compromised information maximize monetization opportunities ([DarkFeed, 2026](#)).

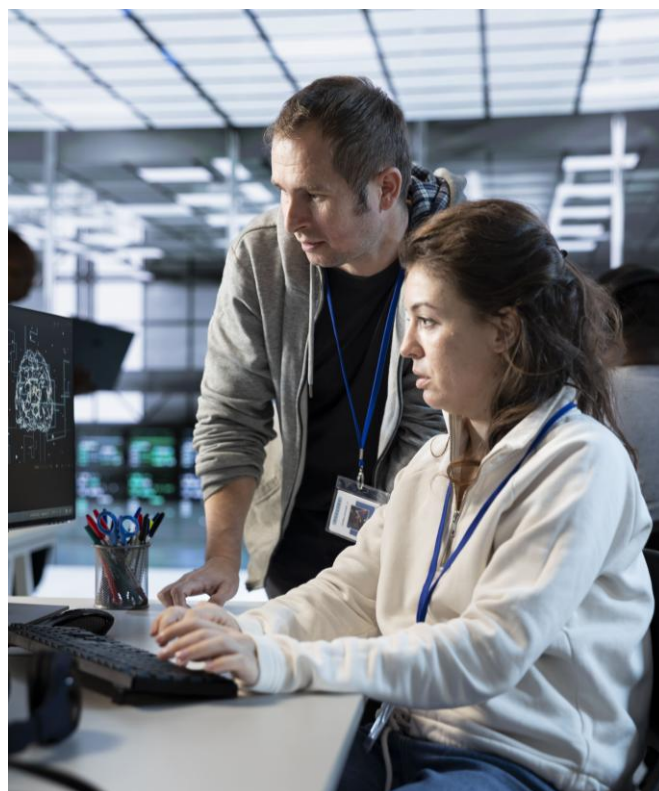
7.2.1 New groups

The temporal distribution of new actors observed

during the first half of 2026 reflects a particularly dynamic and fragmented ecosystem, with a constant incorporation of groups throughout the period. The first months of the year were marked by the emergence of multiple actors with still limited or emerging profiles, suggesting a low barrier to entry and high rotation within the criminal landscape.

March and, especially, April concentrated the highest number of newly identified groups, evidencing a phase of strong proliferation and operational diversification, with the coexistence of actors linked to initial access campaigns and more specialized intrusion operations. From May onward, a reduction in the volume of new entries was observed, although the groups detected showed a more defined operational identity and greater orientation toward already consolidated extortion and monetization models.

Overall, the semester confirms the continuity of a trend characterized by the atomization of the threat ecosystem, the rapid emergence of new actors, and the consolidation of increasingly flexible and adaptable structures, where the permanence of groups is less relevant than their ability to integrate into broader criminal networks and leverage previously established tools and operating models.



New ransomware groups in H1 2026

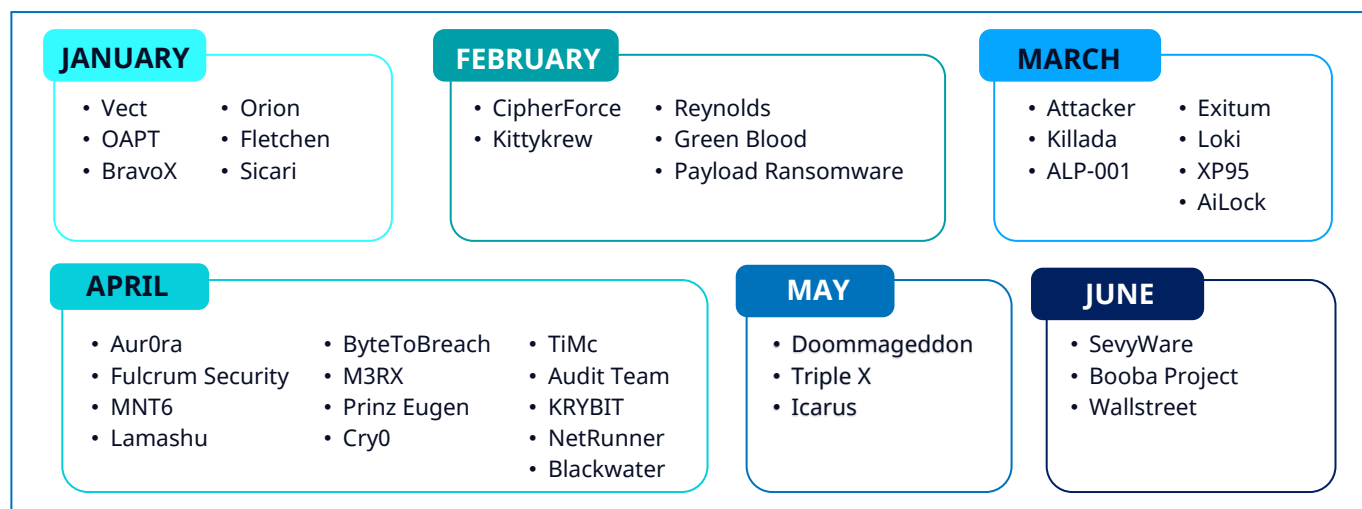


Figure 9 | Ransomware groups detected in the first half of 2026.

This semester, **CipherForce** stands out as one of the new ransomware groups that emerged during February 2026. Despite its recent appearance, the collective quickly positioned itself within the criminal ecosystem by publishing multiple victims on its leak platforms. Its evolution highlights the increasing ease with which new actors can enter the ransomware landscape by leveraging tools, infrastructure, and criminal services already available in the underground market. Rather than representing technical innovation, **CipherForce** exemplifies the continuous renewal of the digital extortion ecosystem, where emerging groups can achieve operational visibility in increasingly short timeframes thanks to the reuse of capabilities previously developed by other collectives.



7.2.2 Most active groups

Ransomware activity during the first half of 2026 has shown a highly dynamic ecosystem, characterized by frequent changes in operational leadership and growing competition among groups to attract affiliates and maintain visibility. Unlike previous periods, no single actor has managed to monopolize activity throughout the semester, with continuous rises, declines, and replacements observed among the main operators. This volatility reflects an increasingly mature RaaS market, where adaptability is becoming as important as technical sophistication.

- **Qilin:** maintained global leadership for much of the semester and continues to be one of the most relevant actors in the ransomware ecosystem. However, after reaching its highest activity level in March, it experienced a progressive reduction in operations during the following months. Its position confirms the strength of its operating model, although the gradual loss of activity suggests growing competition from emerging groups.
- **The Gentlemen:** showed the most consistent evolution of the semester. After beginning the period with moderate activity levels, it recorded sustained growth until becoming the most active group in June.

This trajectory reflects a progressive expansion of capabilities and operational consolidation that places it among the most relevant emerging actors in the current landscape. It has stood out as representative of a generation of smaller, but highly active operators. Its presence reinforces the trend toward greater fragmentation of the ransomware landscape, where emerging groups take advantage of spaces left by traditional actors to gain relevance and expand their operations.

- **DragonForce:** stood out for experiencing one of the fastest growth rates observed during the semester. Its activity increased steadily until May, reaching levels comparable to the main operators in the ecosystem. Its activity illustrates the growing professionalization of organized cybercrime and the trend toward criminal structures capable of integrating affiliates, resources, and infrastructure under increasingly flexible models.

- **Akira:** maintained a relevant presence throughout the semester, although with a downward trend after reaching its peak in March. The progressive reduction in its activity suggests a relative loss of prominence compared with more dynamic operators, although it remains one of the groups with the greatest continuity within the ransomware ecosystem.
- **LockBit:** showed an irregular evolution, characterized by limited activity at the beginning of the semester and a gradual recovery during the final months. Its rebound in June shows that, despite law-enforcement and operational pressure suffered in previous periods, the brand continues to retain influence and presence within the global ransomware landscape ([DarkFeed, 2026](#)).

Top ransomware groups in H1 2026

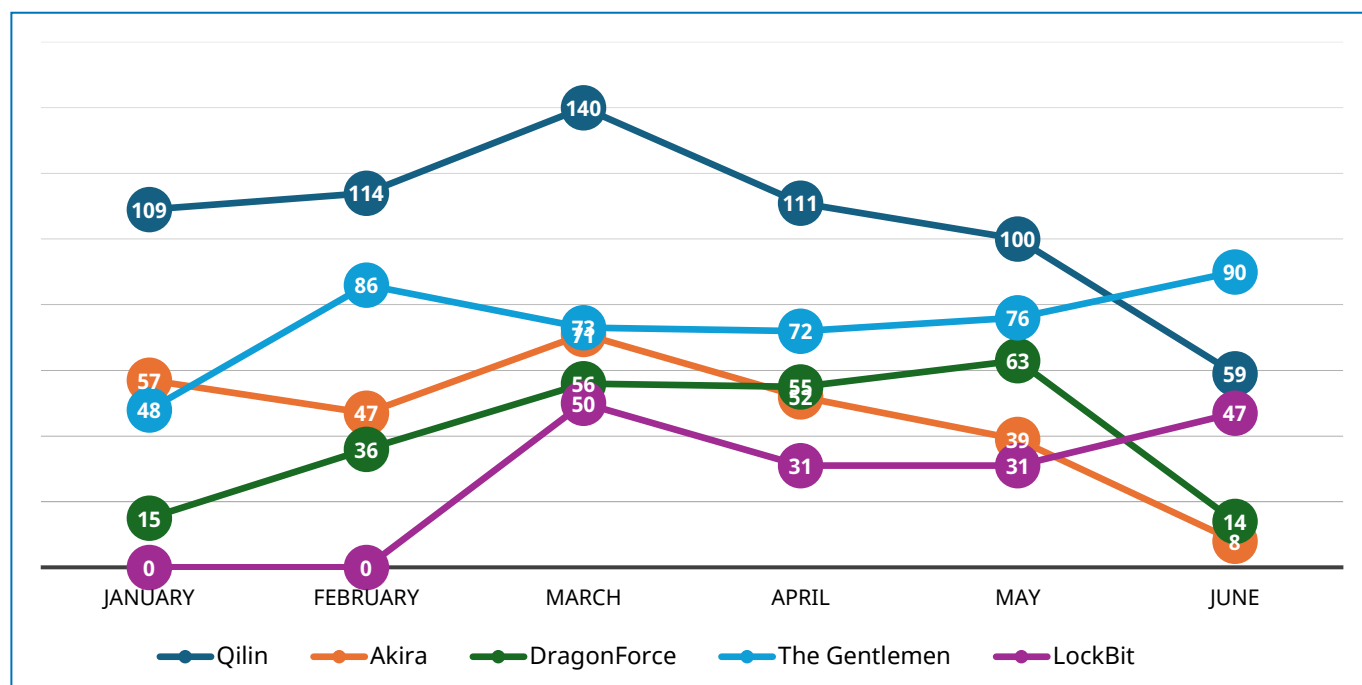


Figure 10 | Activity of the most active ransomware groups in the first half of 2026.

7.2.3 Global impact

The geographic distribution of victims during the first half of 2026 confirms the continuity of a trend already observed in previous periods: ransomware activity continues to be concentrated mainly in developed economies, with a clear predominance of **the United States** and a sustained presence in **Western Europe**.

The United States remained the main target throughout the semester, accumulating 1,838 victims and recording figures far above the rest of the countries, consolidating itself as the main global focus of ransomware activity. In second place are **the United Kingdom, Canada, Germany, and Italy**, which have maintained a constant presence among the most affected countries. Spain and France also recorded relevant activity, confirming that Western Europe remains one of the regions

most exposed to this type of threat due to its high level of digitalization and concentration of high-value organizations.

The data also shows progressive diversification toward other regions. India, Thailand, Japan, and Australia appear repeatedly among the most affected countries, while Brazil maintains a notable presence in Latin America. Although volumes are lower than those observed in North America and Europe, their recurrence shows the increasingly global reach of campaigns.

Overall, the semester's trend maintains a dual pattern: strong concentration of victims in the United States and the main Western economies, together with expansion into new regions driven by the maturity of the RaaS model and operators' ability to run simultaneous campaigns at international scale ([DarkFeed, 2026](#)).

Countries most affected by ransomware in H1 2026

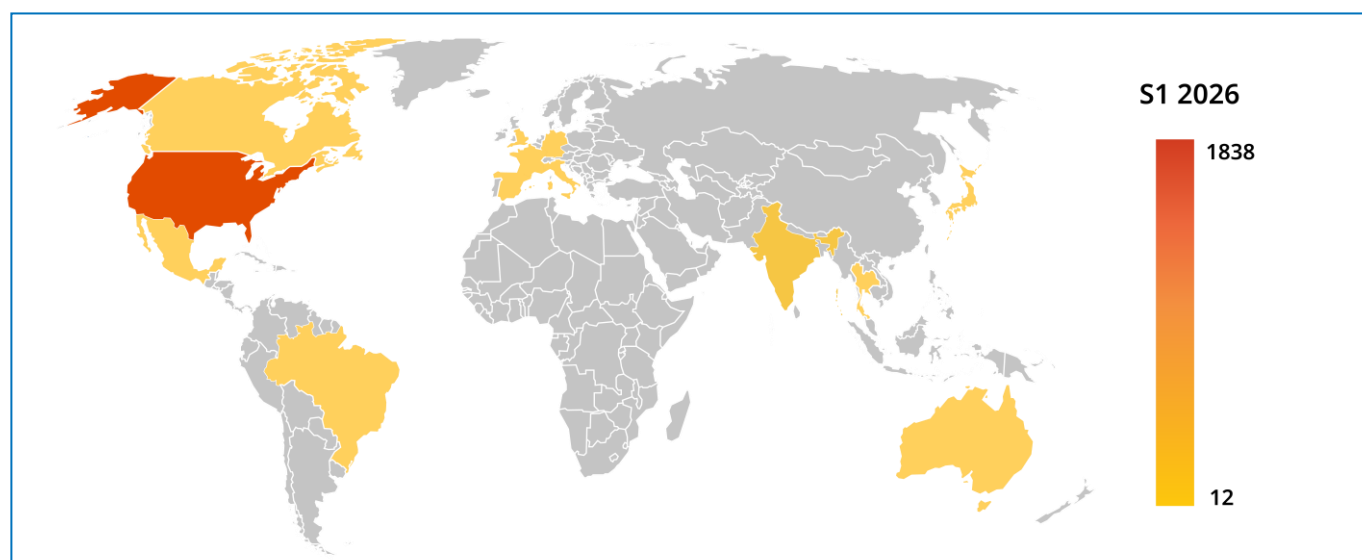
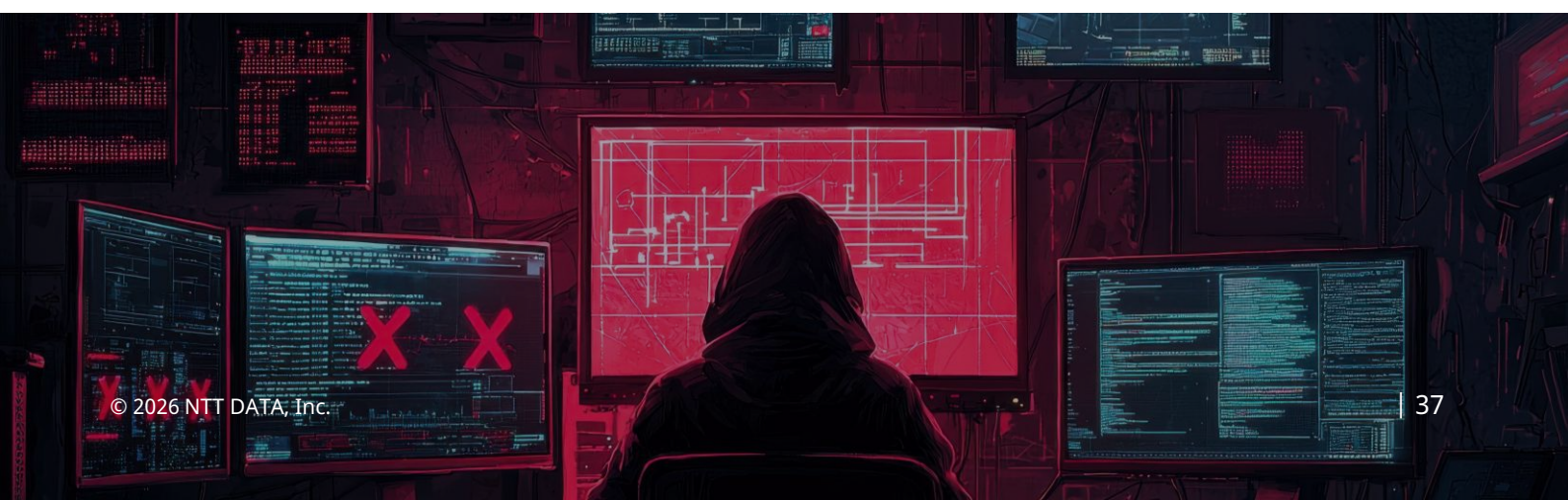


Figure 11 | Countries most affected by ransomware in the first half of 2026.



On the other hand, the **sectoral analysis** for the first half of 2026 confirms the continuity of a trend already observed in previous periods: **ransomware groups** continue to focus their efforts on sectors where operational disruption generates immediate economic impact and increases pressure to negotiate.

Consulting remained the most affected sector throughout the semester, recording the highest victim volumes on a consistent basis. Its attractiveness lies in access to sensitive information, third-party service management, and the potential multiplier effect that an intrusion can generate across multiple organizations.

Manufacturing, healthcare, and construction formed a second block of especially affected sectors. Manufacturing maintained sustained pressure throughout the period, reinforcing the trend toward the targeting of industrial environments and critical production chains. The **healthcare sector** also recorded high and consistent activity, especially during the central part of the semester, reflecting the high coercive value associated with organizations that have low tolerance for service disruption. Similarly, **construction** continued to be

a recurring target, driven by increasing digitalization and reliance on projects with tight operational deadlines.

IT services also maintained a stable presence among the most affected sectors, while **retail, finance, and education** recorded more localized activity peaks. Although their overall volume was lower than that of the leading sectors, their recurring presence shows that operators continue to target organizations capable of generating economic impact, access to third parties, or reputational pressure.

From a structural perspective, the semester shows a consolidation of the target-selection strategies observed in previous years. Rather than significantly expanding the range of affected sectors, operators have continued to prioritize those where disruption costs, data sensitivity, or time pressure increase the likelihood of payment. In this regard, the semester's evolution reinforces the trend toward increasingly selective campaigns focused on operational impact, anticipating the continuity of this pattern throughout the rest of 2026.

Ransomware attacks by sector in H1 2026

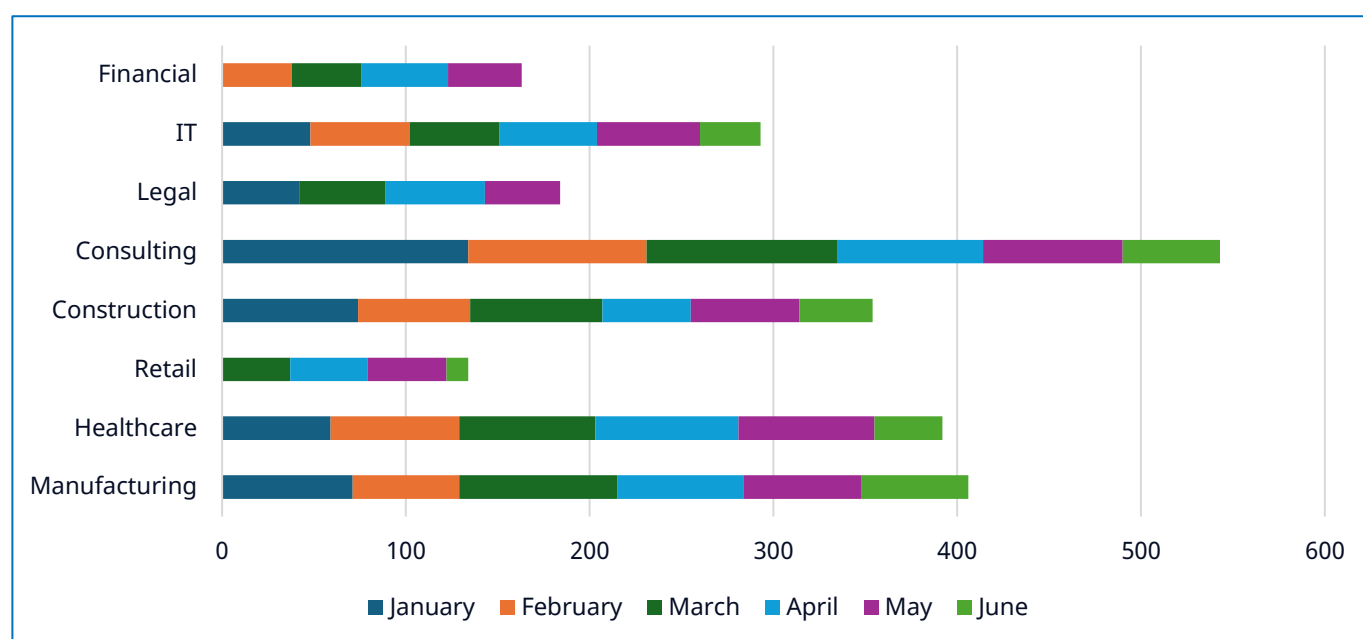


Figure 12 | Sectors most affected by ransomware in the first half of 2026.

7.3 Hacktivism

During the first half of 2026, a consolidation of the **hacktivist** phenomenon has been observed as a tool of **geopolitical** pressure, characterized by greater coordination among collectives, rapid mobilization capacity, and a growing orientation toward operational and reputational impact rather than prolonged espionage operations. Recorded activity confirms that hacktivism continues to evolve toward more organized and visible models, capable of reacting quickly to international events and amplifying their impact through coordinated campaigns ([Orange Cyberdefense, 2026](#)).

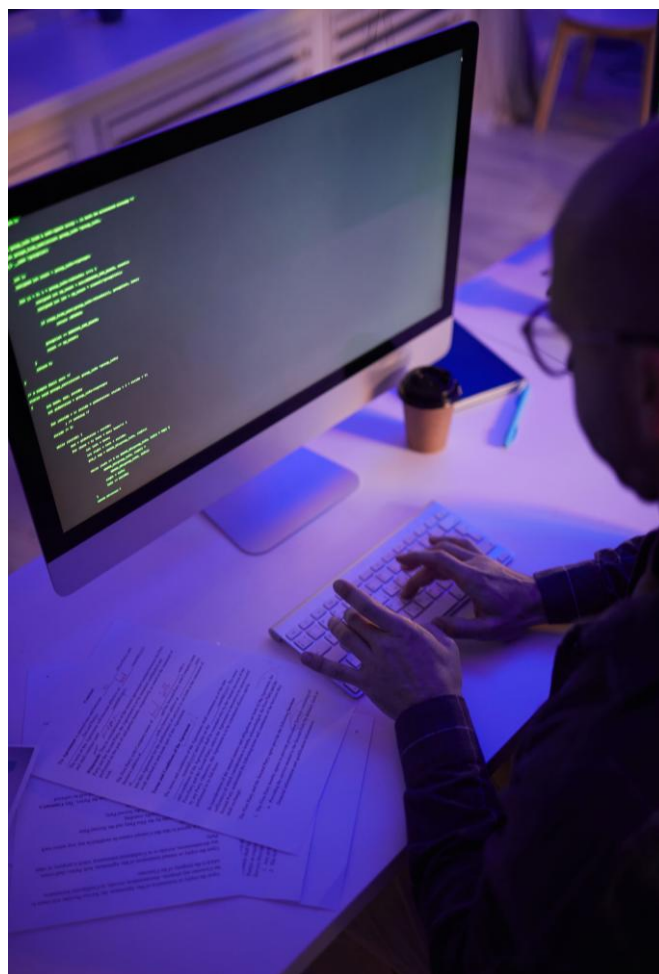
The ecosystem has continued to organize around defined regional and ideological blocs. The pro-Russian environment has maintained a central role, led by collectives such as **NoName057(16)** and supported by actors such as **DeNet**, which have continued to conduct campaigns against government organizations, critical infrastructure, and entities linked to Western countries and NATO. In parallel, groups aligned with the Palestinian cause and other political-religious currents, including **Handala**, **Cyber Islamic Resistance**, **Nation of Saviors**, **Liwa Mohammad**, **Team Fearless**, and **313 Team**, have increased their visibility by exploiting the main areas of tension in the Middle East and reinforcing the ideological dimension of contemporary hacktivism.

At the same time, an activity axis has consolidated in Asia-Pacific and northern Africa, where collectives such as **RipperSec**, **Sylhet Gang-SG**, **Keymous Plus**, and **Moroccan Black Cyber Army** have participated in international campaigns. Likewise, groups such as **DarkStorm** have acted as connector elements between different regional ecosystems, facilitating the spread of narratives, claims, and shared objectives, and reinforcing a flexible cooperation model that makes it possible to increase the reach of operations without requiring centralized structures ([SOCRadar, 2026c](#)).

Observed activity during the semester has confirmed a profile mainly oriented toward disruption and symbolic pressure, with a

predominance of DDoS attacks, defacements, data leaks, doxing, and psychological and reputational pressure campaigns. The rapid execution of these actions and their high public visibility have made temporary service disruption and media impact the main indicators of success for these collectives, above technical persistence or prolonged access to compromised networks ([Fortinet, 2026](#)).

Overall, the **evolution of hacktivism toward a more coordinated, globalized ecosystem closely linked to the international geopolitical context** has been confirmed. Growing collaboration between collectives and their ability to synchronize campaigns against critical infrastructure, public bodies, and **strategic** entities reinforce the risk of higher-impact actions, especially in scenarios of heightened political or military tension ([PowerDMARC, 2026](#)).



Hacktivist group supernodes

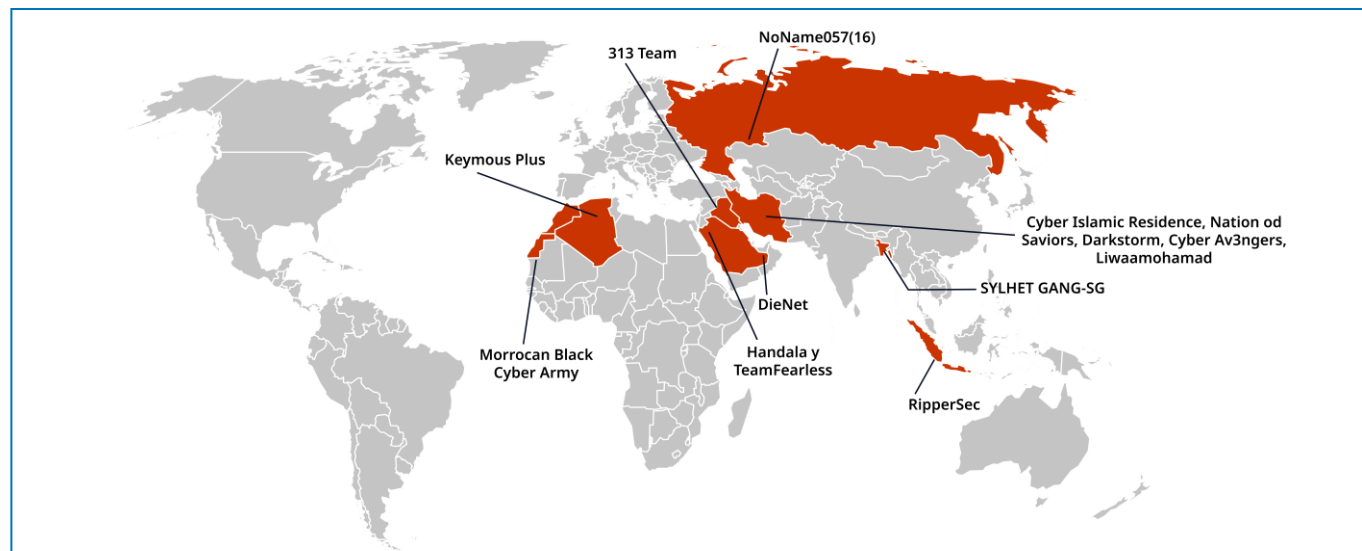


Figure 13 | Hacktivist connector groups by geographic location.

7.4 APT

During the first half of 2026, the pattern identified in the previous period has deepened and been confirmed: geopolitical and state agendas have aligned, and target selection by APT groups has become more explicit. In addition, the progressive reduction in the exploitation window for **N-day** vulnerabilities and the incorporation of artificial intelligence into the development of offensive tools should be highlighted. (ESET, 2026)

• Russian APTs

The first half of the year reflected the continued Russian pressure on Ukraine and European states, with an unprecedented destructive extension against critical NATO infrastructure. **Sandworm** was responsible for the most relevant episode of the period by deploying the **DYNOWiper** wiper against a Ukrainian energy company, representing the first confirmed deployment of destructive malware by a Russia-aligned actor against an EU member state.

Subsequently, it expanded its activity against government, energy, and logistics entities in Ukraine with new malware families such as **ZeroRays** and **NaughtyWipe**. Meanwhile, **Sednit (APT28/Fancy Bear)** exploited vulnerability CVE-2026-21509 less than 24 hours after its disclosure. This was a multi-stage campaign targeting Ukrainian government organizations, EU institutions

and maritime transport entities in Poland, Slovenia, Turkey, Greece, and the United Arab Emirates.

Another Russian APT group with a stronger presence this semester was **Gamaredon**. Its activity was characterized by mass spear-phishing campaigns, intensive use of customized malware, and the incorporation of new stealers and tunneling services aimed at tactical espionage. In parallel to state actors, the pro-Russian hacktivist ecosystem remained active with DDoS campaigns and information leaks marked by lower operational convergence and greater fragmentation in execution than in previous periods.

• Chinese APTs

The campaigns identified during the semester showed a diversification of objectives determined directly by Beijing's geopolitical agenda, prioritizing economic and political intelligence operations. The groups with the highest activity observed were: **Mustang Panda (Twil Typhoon)**, **Salt Typhoon**, **FamousSparrow**, and **NegativeGlimmer**.

FamousSparrow activity was related to maritime and energy resources across Latin America and, in particular, Venezuela. **NegativeGlimmer** compromised a South Korean AI and robotics company, aligned with

priorities of *Made in China 2025*. The Chinese APT ecosystem has been marked by an increase in **AitM** techniques and the exploitation of edge devices and software supply chains to achieve initial access and conduct low-profile operations.

- **Iranian APTs**

During the first half of 2026, Iranian APT activity combined espionage operations with destructive capabilities, mainly targeting Israeli organizations. The three most prominent groups were: **Rusty Boots**, **MoKhargosh**, and **MOON Badr**.

Rusty Boots is a recently active group that used a **bootkit wiper** to completely disable Israeli devices. **MoKhargosh** focused on cyber-espionage operations using **GoKhargosh** as its main backdoor, together with some variants that include destructive capabilities. **MOON Badr** is another group responsible for **spear phishing** campaigns using malicious content to distribute its own backdoor, **MOON Agent**.

Overall, these operations reflect a greater emphasis on persistence, with strategic sectors and government organizations in the Middle East remaining the main targets.

- **North Korean APTs**

Groups linked to North Korea maintained a high level of activity, combining espionage and financial operations. Actors such as **Kimsuky**, **Lazarus**, and **Golden Chollima** focused their campaigns on

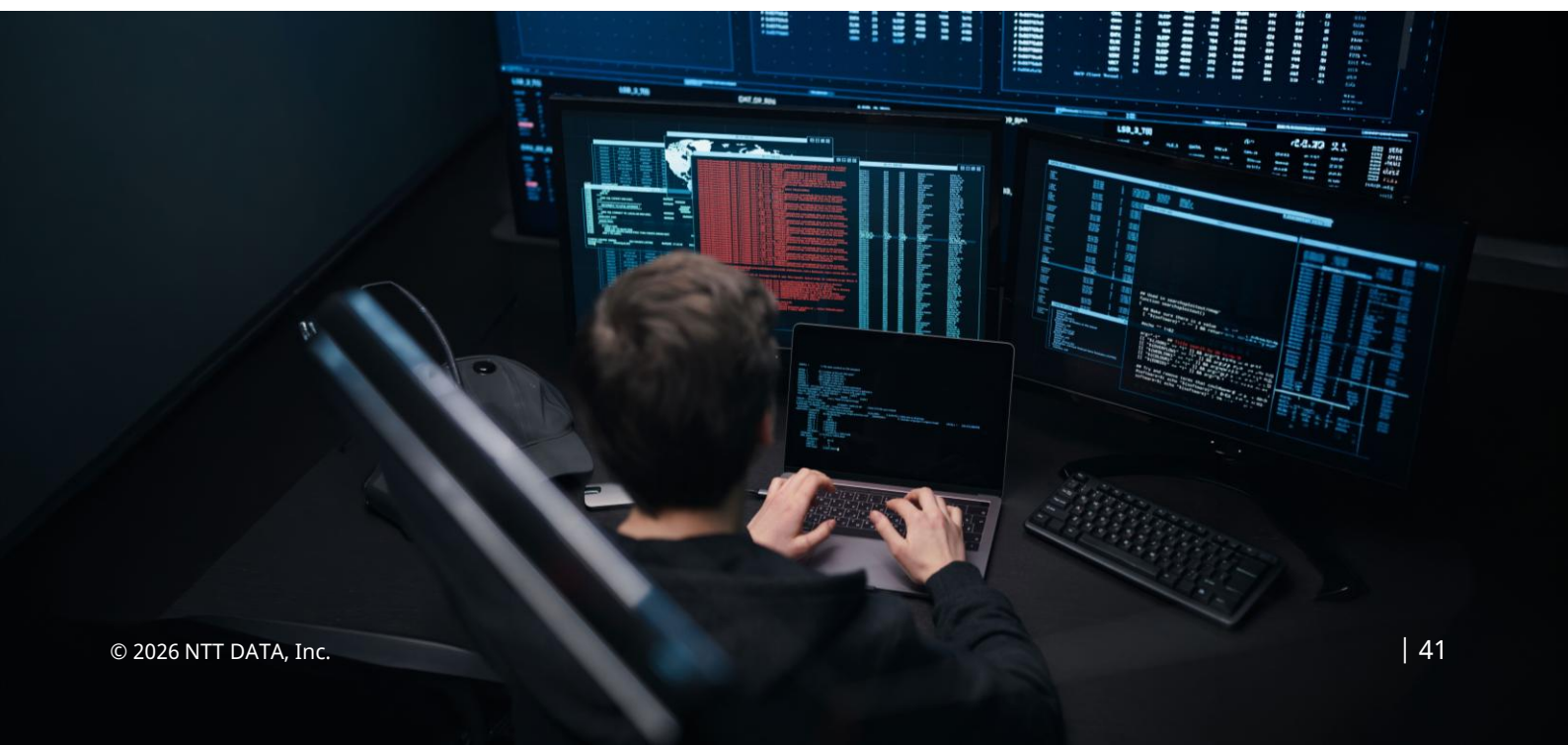
government, diplomacy, technology, and especially the cryptocurrency sector.

Kimsuky carried out intrusions by sending targeted emails attaching the well-known **FPSpy** malware, as well as the **KLogEXE** keylogger, primarily to map networks and collect credentials.

For its part, **Lazarus** focused its efforts on exploiting **zero-day** vulnerabilities and compromising software supply chains, such as the **axios** npm package in **Operation DangerousPassword** or **Operation DreamJob**, to obtain privileges, deploy backdoors, and exfiltrate high-value assets, including cryptoassets. The **Golden Chollima** group was capable of carrying out a six-month social engineering operation that resulted, in April 2026, in the theft of USD 285 million from the DeFi Drift platform.

Overall, these actors have continued to perfect their capabilities through the use of shared tools, more sophisticated infection chains, and better coordinated campaigns.

This evolution consolidates a combined operational model of cyber espionage, sabotage, and illicit financing activities, with the dual objective of hindering detection and attribution while increasing the impact of their operations.



Below are the key trends that shaped the period:

Key trends observed in APT groups in H1 2026

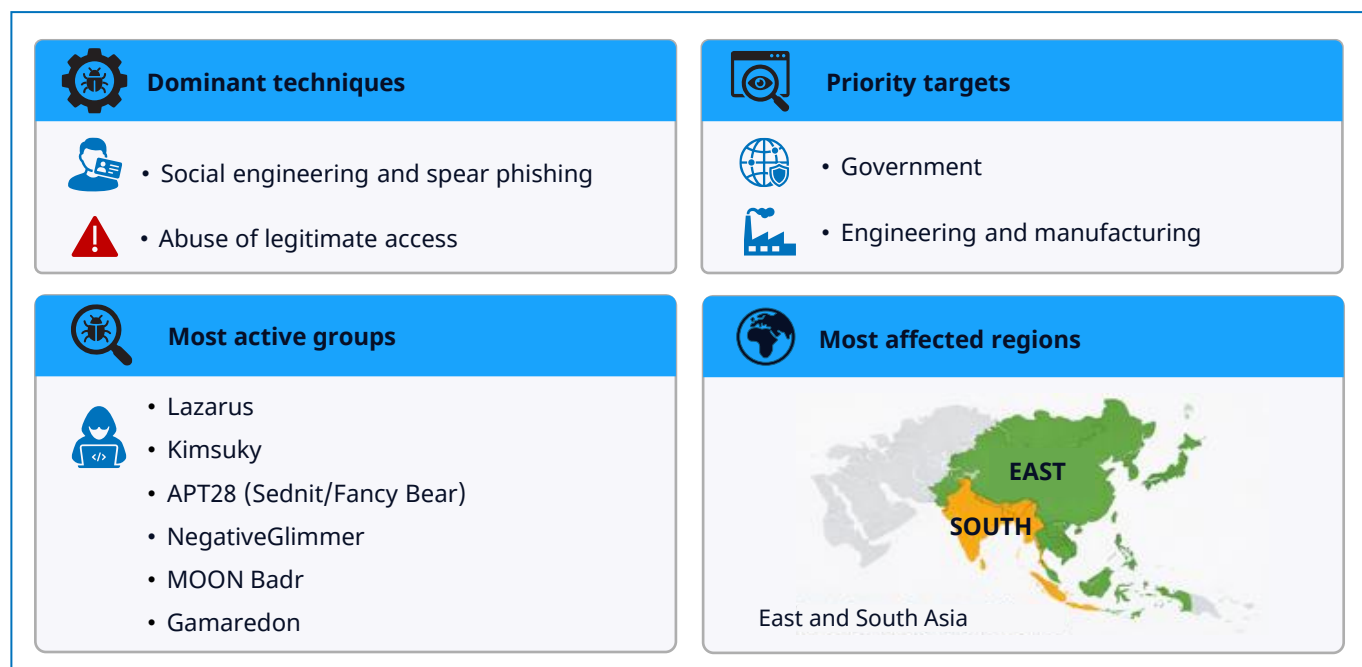


Figure 14 | Key trends for APT groups during the first half of 2026.

The analysis of the first half of 2026 reflects the continuity of persistent espionage campaigns by APT groups mainly linked to China, North Korea, and groups in Southeast Asia. In contrast, a greater disruptive and destructive component also stands out among actors mainly linked to Russia and, to a lesser extent, Iran.

This operational differentiation, shaped by the geopolitical context, makes it possible to identify regional patterns and anticipate an evolution toward longer-lasting and stealthier intrusions aimed at obtaining strategic advantages in the medium and long term.



8. Tactics, Techniques and Procedures (TTPs)



During the first half of 2026, NTT DATA's Cyber Threat Intelligence team has continued to track the evolution of the tactics, techniques, and procedures (TTPs) used by financially motivated cybercriminal activity and by actors with geopolitical motivations. The conclusion is one of **continuity, but with an important nuance**: the technical repertoire has added very few genuinely new elements, but the way in which it is used has changed noticeably. What matters is no longer only which technique is used, but the speed, scale, and automation with which known TTPs are chained together, an orchestration that AI is beginning to support on a routine basis.

Financially motivated cybercrime maintains its dominance, accounting for more than 70% of global interactive intrusions. On this basis, ransomware, multiple extortion, abuse of legitimate identities, and exploitation of exposed infrastructure continue to underpin most campaigns.

Two phenomena have been observed that reinforce each other and distinguish this semester from 2025: **an unprecedented compression of the timeline** from access to exfiltration into minutes or hours, rather than days, and **the conversion of initial access into a commodity** supplied by specialized intermediaries ([Mandiant, 2026](#); [Check Point Research, 2026](#)).

8.1 Description of the most common TTPs used by cybercriminals

Compared with the end of 2025, the TTP catalogue remains within the known boundaries of MITRE ATT&CK; what has changed is the relative weight of each technique and the logic behind their combination. Across more than one million malware samples, **eight out of ten** of the most prevalent techniques seek to remain unnoticed, evade defenses, sustain persistence, or maintain a discreet control channel ([Picus Security, 2026](#)): a shift from the fast and noisy "predatory" attack to the low-profile, persistent "parasitic" infection.

Three shifts concentrate the change:

1

Process injection (T1055) **tops the ranking for the first time (30%)**, while sandbox evasion (T1497) and masquerading (T1036) enter among the dominant techniques, indicating that anti-analysis is gaining ground.

2

Credential theft is no longer merely a preliminary step and has become an objective in itself: **theft from browsers and password managers (T1555) already appears in one in four samples (23%)**.

3

Encryption for impact (T1486) **falls from 21% to 12.94%, a relative decrease of 38%**, confirming ransomware’s shift from “encrypting” to “stealing and extorting” (Picus Security, 2026). This is compounded by the growing weight of valid identities and remote services, especially in the cloud, and by exfiltration becoming consolidated as a precursor to ransomware, reinforcing double extortion.

In summary, the semester points to a more mature adversary, whose priority is **to preserve access, evade detection, and monetize impact**, rather than display novel techniques.

Top MITRE ATT&CK techniques observed in H1 2026

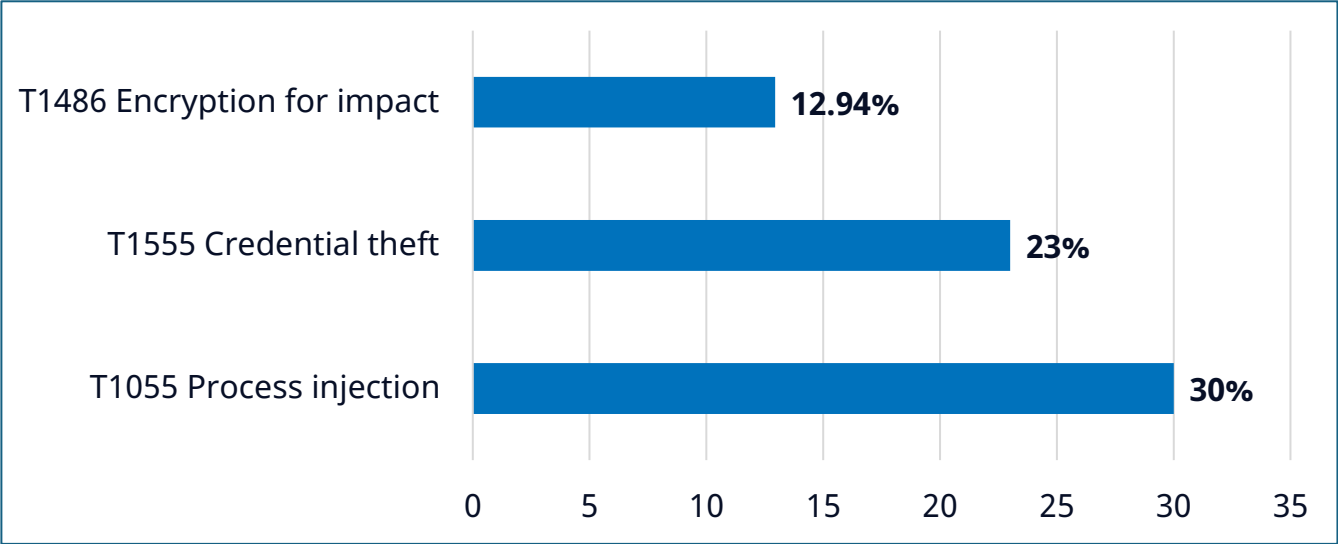


Figure 15 | Most prevalent MITRE ATT&CK techniques observed in the first half of 2026.

Tactic	MITRE ATT&CK ID	Description
Execution (TA0002)	T1059 – Command and Scripting Interpreter	PowerShell, scripts, and native binaries used to execute in memory and minimize the disk footprint; second most observed technique during the semester.
	T1059.001 – PowerShell	Preferred resource in hands-on-keyboard operations and Living-off-the-Land approaches.
	T1047 – Windows Management Instrumentation (WMI)	Remote execution and persistence supported by a legitimate Windows management service.
Persistence (TA0003)	T1098 – Account Manipulation	Modification of existing accounts, whether local, service, or cloud accounts, to perpetuate access without raising suspicion.
	T1098.004 – Additional Cloud Keys	Creation of keys, tokens, or credentials in cloud platforms to sustain access; on the rise in SaaS and hybrid intrusions.
	T1136.001 – Create Account: Local Account	Creation of backup local accounts to ensure persistence after initial access.
	T1547.001 – Startup Execution: Registry Run Keys / Startup Folder	Anchoring in Windows automatic startup to survive reboots.
	T1133 – External Remote Services	Use of exposed services such as RDP, VPN, or web applications as an entry point and discreet persistence mechanism.
Privilege Escalation (TA0004)	T1134 – Access Token Manipulation	Appropriation and impersonation of tokens to operate with higher privileges.
	T1548 – Abuse of Privilege Escalation Mechanisms	Exploitation of loose configurations or deficient controls to escalate privileges.
Defense Evasion (TA0005)	T1055 – Process Injection	Code injection into trusted processes to bypass EDR; most prevalent technique of the semester (30%) .
	T1497 – Virtualization / Sandbox Evasion	Detection of analysis environments to abort detonation; enters among the leading techniques.
	T1036 – Masquerading	Disguising processes and files as legitimate; debut in the high-prevalence range.
	T1562.001 – Disable or Modify Security Tools	Neutralization of antivirus and EDR tools through EDR killers and abuse of vulnerable drivers, BYOVD.
	T1562.004 – Modify or Disable System Firewall	Rewriting firewall rules to enable attacker communications.
	T1070.001 – Indicator Removal: Clear Windows Event Logs	Deletion of logs, sometimes with periodic purging, to blur the trace of the intrusion.
	T1564.008 – Hide Artifacts: Email Hiding Rules	Mailbox rules used to hide communications or exfiltration, including BEC and SaaS abuse.

Table 5 | Main TTPs in the first half of 2026 - 1.

Tactic	MITRE ATT&CK ID	Description
Credential Access (TA0006)	T1555 – Credentials from Password Stores	Extraction from browsers and password managers; present in ~1 in 4 samples and elevated to an objective in itself.
	T1003 – OS Credential Dumping	Dumping credentials from memory or system files, such as SAM/NTDS.
	T1552 – Unsecured Credentials	Collection of secrets stored in cleartext in scripts or configurations, for example in TruffleHog .
	T1528 – Steal Application Access Token	Capture of valid tokens to access applications and services, especially cloud environments.
Discovery (TA0007)	T1046 – Network Service Discovery	Scanning of services and ports to identify new targets.
	T1082 – System Information Discovery	Collection of operating system and hardware information.
	T1016 – System Network Configuration Discovery	Reconstruction of topology and connections using native commands.
	T1057 – Process Discovery	Inventory of active processes to detect security tools or assets of interest.
	T1087.001 – Account Discovery: Local Account	Enumeration of local users to prepare subsequent movement.
Lateral Movement (TA0008)	T1021 – Remote Services	Movement through RDP, SMB, or other services using valid credentials; Akira has been observed initiating it in as little as six minutes.
	T1570 – Lateral Tool Transfer	Distribution of the attacker’s tooling across the compromised network.
Command and Control (TA0011)	T1071 – Application Layer Protocol	C2 over web protocols and legitimate services, including third-party cloud infrastructure, such as AI APIs and cloud providers.
	T1219 – Remote Access Software	Abuse of legitimate RMM solutions, such as ScreenConnect and similar tools, as a command channel; new entry among the top techniques.
Exfiltration (TA0010)	T1041 – Exfiltration Over C2 Channel	Extraction of data through the already established C2 channel.
	T1567.002 – Exfiltration to Cloud Storage	Mass data theft through legitimate APIs and cloud services, as a precursor to extortion.
Impact (TA0040)	T1486 – Data Encrypted for Impact	Encryption of systems in ransomware campaigns; still relevant, but clearly declining from 21% to 12.94%, reflecting the shift toward extortion without encryption.
	T1490 – Inhibit System Recovery	Deletion or deactivation of backups and snapshots to prevent restoration.

Table 6 | Main TTPs in the first half of 2026 - 2.

8.2 Most common entry vectors

Entry vectors in 2026 have maintained continuity with the previous period, but with a qualitative shift: alongside the consolidation of identity abuse, **vulnerability exploitation has regained prominence as an initial access route**. For the first time in nineteen years, it has surpassed credential theft as the most common access mechanism in analyzed breaches (Verizon, 2026) in the cloud, third-party software exploitation rises from 2.9% to **44.5%**, overtaking credential abuse (Google Cloud, 2026). High and critical security vulnerabilities exploited doubled year on year (+105%) (Rapid7, 2026).

This rebound does not contradict the underlying trend, but nuances it: the value of these vectors does not lie in their technical novelty, but in their **establishment as silent, persistent accesses with low visibility and in their industrialization**. Increasingly, initial access is packaged by Initial Access Brokers (IABs), who sell RDP, VPN, and RDWeb access as **Access-as-a-Service**, and assemble inventories of devices and compromised credentials before the final operation. As a result, the adversary combines exploitation of exposed services with valid identities and credentials, blurring the distinction between legitimate and malicious activity from the earliest stages.

Abuse of valid identities	Vulnerability exploitation and perimeter devices	Identity-oriented social engineering
Legitimate identities are consolidating as one of the main entry points. Using stolen credentials, session cookies, and tokens, the attacker operates without malware, reducing visibility and making detection more difficult. Accounts without MFA or with poorly configured MFA remain the most common access points during the period.	Reactivation of vulnerability exploitation, concentrated on perimeter and publicly exposed applications such as FortiGate, Cisco FMC, SharePoint, F5, and ShareFile. The disclosure-to-exploitation window narrows to zero-day levels and connects directly with ransomware chains.	Maneuvers to obtain credentials or user consent: vishing, help desk impersonation, CEO fraud/BEC, and abuse of authentication flows. Vishing rises to the second access vector, present in 11% of investigations (Mandiant, 2026).
Advanced infostealers	Abuse of legitimate remote services	Cloud environments and APIs
Infostealers are consolidating as the phase prior to ransomware and fraud. Automated capture of credentials, cookies, and browser data feeds IABs and is highly cost-effective: half of ransomware victims with leaked credentials were attacked in under 95 days.	RDP, VPN, and RDWeb with valid credentials as initial access, with growing IAB interest in RDWeb. By relying on legitimate services, the adversary reduces its technical footprint and makes early detection harder.	Access through configuration errors in the cloud, excessive permissions, exposed API keys, and abuse of trust relationships between services. This becomes more acute in hybrid and multicloud environments with lower visibility: third-party software exploitation is already the leading vector in cloud environments (Google Cloud, 2026; ReliaQuest, 2026).

Table 7 | Most common entry vectors used during the first half of 2026.

Ultimately, initial access in 2026 rests on **two mutually reinforcing pillars**: exploitation of exposed infrastructure accelerated by **rapid weaponization** and **pre-positioned access**, and the abuse of identities, trust, and legitimate use of services. Both converge in the IAB market, which turns entry into a commodity. The result: harder detection and greater potential impact, as these forms of access do not trigger immediate alerts or clearly anomalous behavior. Addressing this requires integrating vulnerability management and agile patching with identity governance, cloud visibility, and monitoring of human processes: the ground for the innovation addressed below.



8.3 Innovation in attacks: new techniques and tactics

Innovation in 2026 does not come from techniques that are new to MITRE ATT&CK, but from **a transformation in the adversary's operating logic**. The model that is taking hold combines persistence, automation, compression of the attack cycle, and methodical exploitation of trust; its goal is not only to compromise systems, but to blend into the organization's ordinary operations and trigger impact as soon as it becomes profitable. The change is less visible in how attackers get in and more in **how they act once inside**: time management, signal reduction, and the way damage is materialized.

From noisy operations to stealthy, automated, compressed-cycle intrusions

The first evolutionary line combines a deliberate reduction in technical noise with **a drastic acceleration of the attack cycle**. The adversary prioritizes manual work, or hands-on-keyboard activity, native tools, or Living-off-the-Land, and

assisted execution over persistent malware, to the point that a growing share of interactive intrusions takes place without traditional malware. This convergence blurs the boundaries between actors: nation-state groups and ransomware gangs such as **Volt Typhoon, APT28, Black Basta, and FIN7** use an almost identical native toolkit: PowerShell, WMI, RDP, ntdsutil, and netsh ([SentinelOne, 2026](#)).

At the same time, time has become a weapon. The median interval between initial access and handoff to an operator has fallen to **22 seconds**, compared with more than eight hours in 2022; **Akira** initiates lateral movement in **6 minutes**, and the fastest campaigns move from access to exfiltration in around **72 minutes** ([Mandiant, 2026](#); [ReliaQuest, 2026](#); [Unit 42, 2026](#)). This high-speed, low-profile approach is made possible by **pre-positioned access**: attackers no longer need to exploit in real time; they only need to activate pre-existing inventories, which also spreads defensive signals across several domains — identity, endpoint, and cloud — making correlation more difficult.

Industrialization of ransomware and consolidation of multiple extortion

The ecosystem is undergoing **reconsolidation**: the top 10 groups accounted for 71% of victims published on data leak sites, and just four operators — **Qilin, Akira, The Gentlemen, and LockBit** — account for 41%, while the number of active groups has fallen from 85 to 71 in just a few quarters: “fewer adversaries, but more capable ones” ([Check Point Research, 2026](#)).

The novelty has not been encryption, but the comprehensive orchestration of the campaign. **The Gentlemen** exemplifies the industrialization of access: it launched its operation with around 14,700 compromised FortiGate devices and 969 VPN credentials obtained through brute force (CVE-2024-55591), accumulated before making its demand. At the same time, the shift from encryption to data theft and extortion without encryption has become entrenched: the 38% decline in the encryption technique ([Picus Security, 2026](#)), the widespread use of EDR killers, encryptionless extortion, and cases such as **ShinyHunters** have generated disproportionate damage through identity-first intrusions and native SaaS data theft, without a

single encryptor. This reflects the maturity of double and triple extortion ([ReliaQuest, 2026](#)).

Artificial intelligence as a tactical accelerator, not a substitute

During the first half of 2026, **artificial intelligence has consolidated as a tactical accelerator within the attack chain**. Its impact is not reflected so much in the emergence of completely new techniques within MITRE ATT&CK, but in the reduction of the time needed to prepare, adapt, and execute already known phases of the offensive cycle. Google Threat Intelligence Group observes a transition from early uses of AI toward a more industrialized application of generative models in adversarial workflows, including vulnerability research, exploit development, malware, reconnaissance, social engineering, and influence operations ([Google Threat Intelligence Group, 2026](#)).

The most relevant uses have focused on support tasks: generating more credible phishing lures, linguistic and cultural adaptation of messages, reconnaissance automation, classification of large volumes of stolen data, scripting assistance, tool modification, and synthetic content creation. Sophos also identifies AI as an increasingly present topic in underground communities, where actors discuss its potential, claim to use it for malware or tool development, and, at the same time, express doubts about the veracity, usefulness, and operational security of some offerings ([Sophos, 2026](#)).

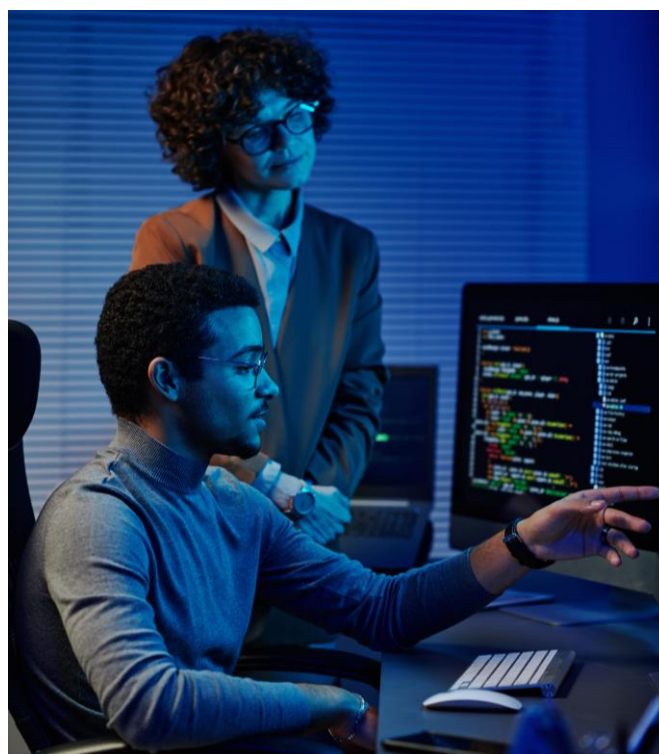
This nuance is key: AI does not eliminate the need for human oversight. Actors still depend on operators to select targets, validate access, decide lateral movements, interpret the victim's context, and monetize the compromise. However, it reduces the cognitive load of repetitive tasks and allows less sophisticated profiles to access capabilities that previously required greater technical expertise. In this sense, AI acts more as a criminal productivity multiplier than as an autonomous substitute for the attacker.

In social engineering campaigns, the impact is especially relevant. Verizon notes that different attack techniques are being reinforced by generative AI and that actors use it to accelerate

phases ranging from breach identification to malware writing ([Verizon, 2026](#)). This facilitates lure personalization, multilingual content production, the use of synthetic identities, and the execution of phishing, smishing, vishing, or BEC campaigns at lower operational cost.

More technical uses have also begun to be observed. Google Threat Intelligence Group stated in May 2026 that it had identified, for the first time, a criminal actor that allegedly used AI to develop a zero-day exploit intended for a mass exploitation operation. The same report describes cases of AI-assisted malware development, evasion logic, use of AI for autonomous commands, and attacks against AI software environments and dependencies as an initial access vector ([Google Threat Intelligence Group, 2026](#)).

Overall, AI should be understood as a cross-cutting accelerator of already known TTPs. It does not replace the attacker, but it enables campaigns to be prepared faster, messages to be adapted to more victims, repetitive phases to be automated, and entry barriers to be reduced. For defense, this means that looking for "AI attacks" is not enough; it is necessary to reinforce controls over identity, email, anomalous behavior, abuse of legitimate tools, data exposure, and response speed.



9. Vulnerabilities



During the first half of 2026, vulnerability exploitation consolidated its role as a priority initial access vector, driven by the rapid operationalization of critical flaws in exposed services, perimeter appliances, management platforms, security solutions, and widely deployed components. The cases observed show a transition toward more automated campaigns oriented toward post-exploitation, where the value of a CVE does not depend only on its severity, but on its real exposure, active exploitation, and ability to facilitate persistence, privilege escalation, credential theft, or operational impact.

• January:

The beginning of the semester was marked by the exploitation of vulnerabilities in networking technologies and centralized management. **CVE-2026-24858**, associated with **Fortinet** ([Fortinet Security Advisory, 2026](#)), represents a particularly relevant pattern: **the abuse of trust relationships and federated authentication in perimeter ecosystems**. Its exploitation allowed initial access actors to operate on registered devices, automate firewall changes, create users, enable VPN access, and extract configurations. From a CTI perspective, the case reflects how attackers no longer seek only to compromise an exposed device, but to turn that access into immediate operational control over network infrastructure.

In parallel, active exploitation of **CVE-2024-37079** in **VMware vCenter Server** ([Broadcom/VMware Security Bulletin, 2026](#)) illustrates the strategic value of virtualization platforms as a corporate control plane. vCenter exploitation should not be analyzed only as remote code execution, but as a potential path toward the administration of virtualized workloads, system inventory, elevated privileges, and lateral movement across critical infrastructures. This case confirms that **centralized management systems have become high-value targets** for campaigns focused on persistence and expansion.

A consolidation of post-exploitation automation is observed. Threat actors are no longer limited to obtaining initial access through vulnerabilities in exposed services; they also integrate **automated workflows for configuring malicious infrastructure** immediately after compromise.

• February:

During February, a significant diversification of attack vectors was observed, combining mass exploitation of exposed systems with more targeted campaigns against critical network infrastructure and enterprise applications. The SQL injection flaw in the FortiClient EMS GUI component, identified as **CVE-2026-21643** ([Fortinet, 2026](#)), represents the pattern of **rapid weaponization of Internet-facing services**: mass scanning, use of public PoCs, and exploitation by multiple attacking IP addresses. Its relevance lies not only in command execution, but also in the fact that it affects a platform used for corporate endpoint management, amplifying the impact in enterprise environments.

On the other hand, the authentication bypass vulnerability tracked as **CVE-2026-20127** in **Cisco Catalyst SD-WAN** ([Cisco Security Advisory, 2026](#)) reflects another relevant pattern: **the abuse of internal trust between infrastructure components**. Activity associated with **UAT-8616**, including version downgrade, exploitation of a previous vulnerability (**CVE-2022-20775**), and subsequent software restoration, demonstrates a more sophisticated and stealthy approach. This behavior points to actors seeking to maintain privileged access while reducing the visibility of the intrusion.

Finally, **CVE-2026-21513**, associated with **Microsoft MSHTML** ([Microsoft, 2026](#)) and the **Operation Neusplit** campaign attributed to **APT28 (Fancy Bear / Forest Blizzard)**, reinforces **the convergence between technical exploitation and social engineering**.

This **zero-day exploitation campaign** based on the use of *spear phishing* with LNK files and malicious RTF documents — which installed advanced in-memory malware such as **NotDoor, MiniDoor, and CovenantGrunt** to exfiltrate confidential information — confirms that vulnerabilities in widely used components remain an effective resource for cyber-espionage operations against government, diplomacy, and foreign policy targets. The observed pattern combines client-side exploitation, evasion of security controls, and abuse of legitimate services for C2 and exfiltration.

A greater orientation toward the **compromise of critical business applications is observed**. Threat actors leveraged authentication and remote code execution vulnerabilities to **access platforms that store sensitive corporate information and essential operational processes**.

• March:

March introduced a turning point with the **Zero-click Copilot Theft campaign**, associated with **CVE-2026-26144** in **Excel** ([Microsoft Security Response Center, 2026](#)). The case is relevant because it shifts the focus from classic exploitation of office applications toward the abuse of artificial intelligence agents integrated into productivity workflows. Exploitation made it possible to exfiltrate corporate information without direct user interaction, leveraging agent-mode capabilities and unauthorized outbound connections.

From a CTI perspective, this case represents the emergence of a new pattern: **“AI-Agent Hijacking.”** The attack surface is no longer limited to the document, macro, or endpoint; it extends to agents that process, interpret, and connect internal data. The trend points to attacks targeting the core of corporate productivity, where sensitive information can be extracted through channels that appear legitimate and are difficult to distinguish from normal activity.

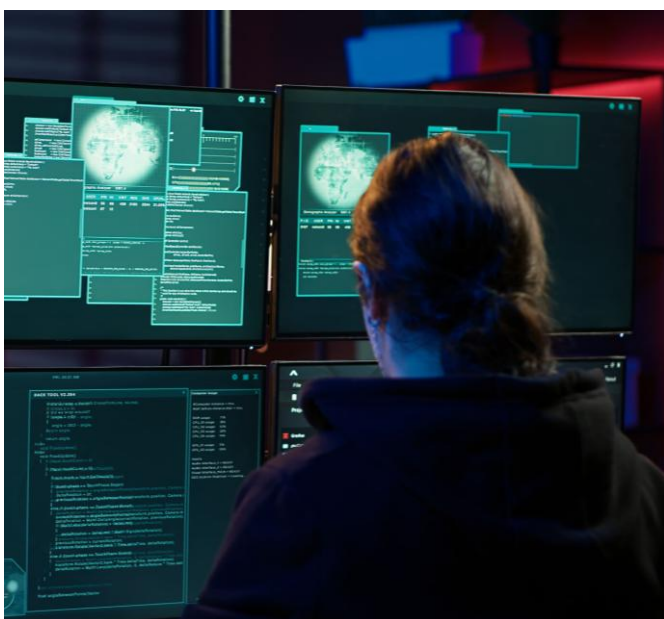
March marks a significant turning point in the threat landscape by introducing **“AI-Agent Hijacking”** attacks. The ability to silently exfiltrate data through internal agents indicates an evolution toward attacks targeting the core of organizational productivity and confidential data.



• April:

April was marked by *ransomware* campaigns that leveraged remote administration tools and internal management platforms to maximize their impact. Particularly notable were the vulnerabilities identified as **CVE-2024-1708** and **CVE-2024-1709** in **ConnectWise ScreenConnect** — now **ConnectWise Access** — ([NIST, 2026](#)) which represent a recurring pattern: attackers prioritize RMM tools because they provide administrative access, persistence, and internal movement capability **without the need to deploy complex malware**. Their exploitation by groups such as **Black Basta**, **Bl00dy**, and **LockBit**, linked to North Korea and China, confirms that remote support platforms remain a high-value entry point for extortion operations.

Likewise, **CVE-2023-27350** and **CVE-2023-27351** in **PaperCut NG/MF** (PaperCut Security Bulletin, 2026) reinforce a second reading: **the persistent exploitation of N-day vulnerabilities** in internal services that remain exposed or unpatched. Although these are not new vulnerabilities, their use by groups such as **Cl0p**, **Bl00dy**, **Mint Sandstorm**, **Mango Sandstorm**, and **Lace Tempest** shows that the risk cycle of a CVE does not end with publication of the patch. Actors continue to exploit old flaws when they provide rapid administrative access, sensitive information, or pivoting capability toward other corporate systems.



Ransomware groups are prioritizing the compromise of these platforms because they provide almost immediate administrative-level access, **eliminating the need to develop custom malicious tools for persistence**.

• May:

May reflected a marked transition toward post-exploitation techniques focused on privilege escalation, defense evasion, and access consolidation. The vulnerability chain **CVE-2026-31431 (Cozy Fail)**, **CVE-2026-43500**, **CVE-2026-43284 (Dirty Frag)**, and **CVE-2026-46300 (Fragnesia)** in the **Linux Kernel** represents the use of LPE vulnerabilities as a post-initial compromise phase. Their operational value lies in enabling privilege escalation to root, reinforcing persistence, and hindering detection by operating in memory instead of modifying obvious artifacts on disk ([INCIBE-CERT, 2026b](#)).

In parallel, **CVE-2026-41091** and **CVE-2026-45498** in **Microsoft Defender** ([Microsoft Security Response Center, 2026](#)) showed a complementary pattern: attacking security controls themselves. Their exploitation to escalate privileges to SYSTEM or disrupt the antimalware platform confirms that **defensive solutions are also part of the attack surface**. This trend requires treating security engines, EDR, and active antimalware components as critical assets that must be updated and monitored with the same rigor as exposed services.

The strategic shift from mass intrusion techniques to “below-the-radar” operations seeks to consolidate full control of critical assets without leaving persistent evidence on disk, posing a **direct challenge to traditional detection systems** and highlighting the critical need to implement **behavior-based security** — EDR/XDR.

• June:

To close the semester, June confirmed the pressure on widely deployed enterprise platforms and Internet-facing services. First, exploitation of the authentication-bypass vulnerabilities **CVE-2026-50751** and **CVE-2026-50752** in **Check Point VPN** (CheckPoint, 2026), shows sustained interest in VPN and remote access solutions. Their exploitation, partially linked to a Qilin affiliate, allowed connections to be established without valid credentials, aligning with one of the most relevant trends of the semester: the remote access perimeter remains a priority entry point for ransomware, initial access brokers, and espionage-oriented actors.

Second, **CVE-2026-28318** in **SolarWinds Serv-U** (SolarWinds, 2026) represents a different pattern focused on availability. As a denial-of-service (DoS) vulnerability, its impact should primarily be linked to the disruption or degradation of exposed file transfer services, rather than to initial access, persistence, or lateral movement, unless an additional exploitation chain has been documented. Its relevance lies in the fact that corporate information-exchange services can become operational pressure points, especially when they support critical processes or sensitive business workflows.

Attackers are exploiting the security vulnerability without requiring privileges, **through low-complexity attacks that do not require user interaction.** Its exploitation can have a high impact on the confidentiality, integrity, and availability of the affected system.

Exploitation trends for these vulnerabilities

Overall, the first half of 2026 confirmed four main patterns.

- Attackers have prioritized **vulnerabilities in widely deployed enterprise technologies that concentrate privileges, connectivity, or centralized administration:** Internet-facing services such as firewalls and VPNs, management platforms, remote access, virtualization and printing, office tools, and security solutions.

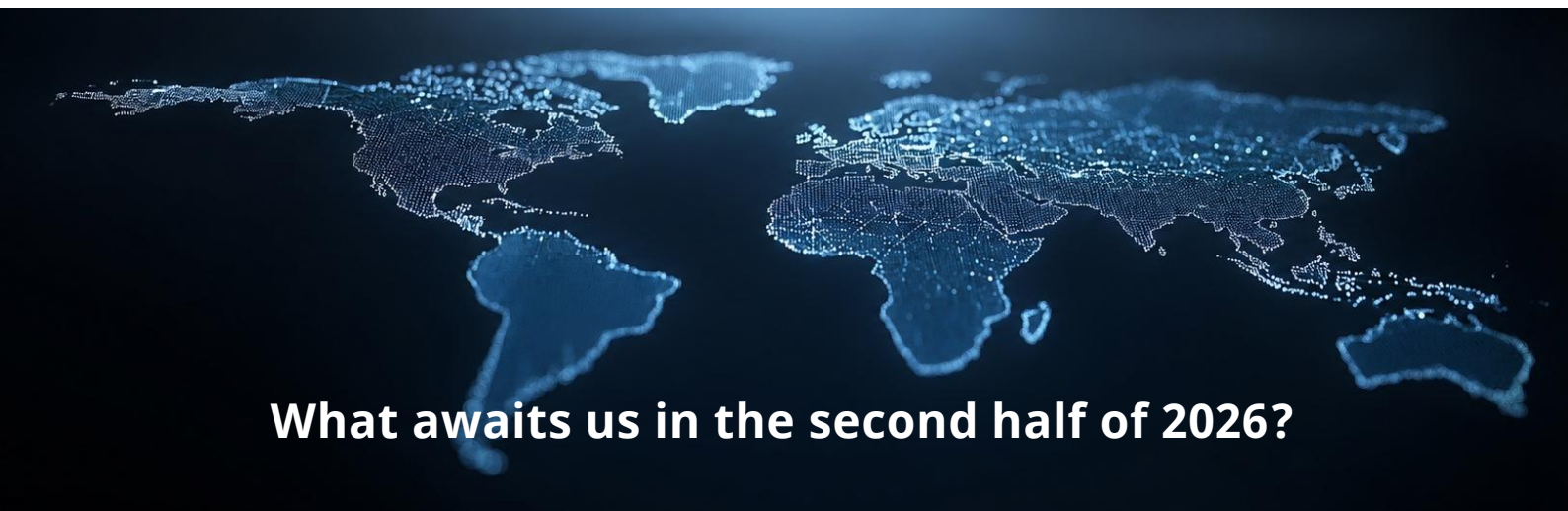
- **Post-exploitation automation has consolidated.** Actors no longer limit themselves to exploiting a flaw and waiting for a second manual phase; instead, they integrate workflows to create users, enable VPN access, modify configurations, extract credentials, or prepare lateral movement almost immediately after compromise.
- A growing **convergence between technical exploitation, identity, and social engineering** has been observed. Campaigns no longer depend on a single vector: they combine malicious documents, spear phishing, ClickFix techniques, abuse of legitimate services, valid credentials, AI agents, and exploitation of exposed services.
- The risk of a CVE depends increasingly less on its theoretical severity and more on its real exposure, active exploitation, the criticality of the affected asset, and its **ability to be integrated into ransomware, espionage, or disruption campaigns.** These are the factors on which defensive prioritization should be based.

Thus, the semester shows that the most relevant vulnerabilities are not necessarily the newest, but those that allow attackers to gain rapid access, operate with low noise, consolidate privileges, and turn initial compromise into real impact on the organization.



A man with short dark hair and a light beard is sitting in a server room, looking at a laptop. He is wearing a blue jacket over a white t-shirt and a blue lanyard with a white ID card. The room is filled with server racks, and the lighting is dim with a blue tint. The text "10. Future outlook" is overlaid on the left side of the image.

10. Future outlook



What awaits us in the second half of 2026?

Looking ahead to the second half of 2026, the cyber threat landscape points to **a consolidation of the dynamics observed during the first half of the year**. No radical break in the attack model is expected, but rather an evolution toward faster, quieter operations supported by automation, abuse of legitimate identities, exploitation of exposed services, and the use of artificial intelligence as an operational accelerator.

Cybercrime will continue to move toward more specialized and distributed models. Law-enforcement pressure on forums, markets, and criminal infrastructure does not eliminate demand for credentials, initial access, infostealer logs, or criminal services, but it does push activity toward private communities, closed channels, and more fragmented markets. Trust between actors, reputation, and the ability to migrate quickly will remain key elements of the underground ecosystem.

Artificial intelligence will continue to gain relevance as a support tool in repetitive and scalable phases: phishing lure generation, linguistic and cultural adaptation, reconnaissance automation, scripting assistance, classification of stolen data, and creation of synthetic content.

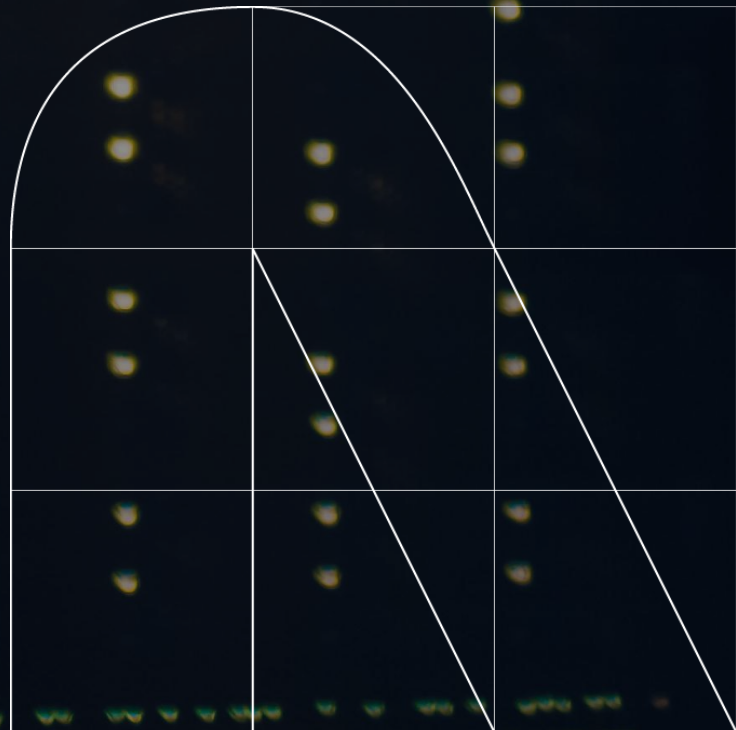
Its impact will not lie so much in replacing the attacker as in reducing time, increasing scale, and enabling more credible and personalized campaigns.

Identity will remain one of the main battlegrounds. Abuse of valid credentials, tokens, sessions, SaaS applications, remote services, and excessive permissions will continue to hinder early detection, especially in intrusions that simulate legitimate activity during their early stages. In parallel, ransomware and extortion will remain relevant, with greater weight given to data theft, reputational pressure, and flexible monetization of access.

At the geopolitical level, cyberspace will continue to function as an environment of strategic pressure. **Tensions between blocs, active conflicts, technological competition, and the protection of critical supply chains will continue to drive espionage, influence, limited sabotage, and hacktivism operations aligned with state narratives.** Sectors such as defense, energy, telecommunications, transport, financial services, technology, and strategic suppliers will continue to concentrate a significant share of the risk.

Overall, the second half of 2026 is shaping up to be a period in which defensive advantage will depend on the ability to anticipate, correlate, and respond quickly. Rather than preparing for completely new threats, organizations will need to prepare for faster, more adaptive, and better-coordinated adversaries.

11. References



- Australian Department of Home Affairs. (2026). Cyber security act. <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-security-act>
- Australian Department of Home Affairs. (2026). Security standards for smart devices. <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/security-standards-for-smart-devices>
- Council of the European Union. (2026). Council implementing regulation (EU) 2026/589 implementing regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the union or its member states. https://eur-lex.europa.eu/eli/reg_impl/2026/589/oj/eng
- Council of the European Union. (2026). Council implementing regulation (EU) 2026/1078 implementing regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the union or its member states. https://eur-lex.europa.eu/eli/reg_impl/2026/1078/oj/eng
- European Commission. (2026). Commission delegated regulation (EU) 2026/881 supplementing regulation (EU) 2024/2847. https://eur-lex.europa.eu/eli/reg_del/2026/881/oj/eng
- Government of Canada. (2026). Government of Canada strengthens cyber security and critical infrastructure with royal assent of bill C-8. <https://www.canada.ca/en/public-safety-canada/news/2026/06/government-of-canada-strengthens-cyber-security-and-critical-infrastructure-with-royal-assent-of-bill-c8.html>
- Indian Computer Emergency Response Team. (2026). CERT-In security guidelines CISG-2026-01: cyber security framework and guidelines for space including satellite communication. <https://www.cert-in.org.in/s2cmainservlet?pageid=guidInview02&refcode=cisg-2026-01>
- Indian Computer Emergency Response Team. (2026). CERT-In security guidelines CISG-2026-02: blueprint for reducing exposure and defending against ai-assisted vulnerabilities exploitation in digital infrastructure. <https://www.cert-in.org.in/s2cmainservlet?pageid=guidInview02&refcode=cisg-2026-02>
- Indian Computer Emergency Response Team. (2026). CERT-In security guidelines. <https://www.cert-in.org.in/s2cmainservlet?pageid=guidInview01>
- Library of Congress. (8 January 2026). China: amended cybersecurity law takes effect. <https://www.loc.gov/item/global-legal-monitor/2026-01-08/china-amended-cybersecurity-law-takes-effect/>
- National Institute of Standards and Technology. (2026). SP 800-172 rev. 3: enhanced security requirements for protecting controlled unclassified information. <https://csrc.nist.gov/pubs/sp/800/172/r3/final>
- National Institute of Standards and Technology. (2026). SP 800-172A rev. 3: assessing enhanced security requirements for protecting controlled unclassified information. <https://csrc.nist.gov/pubs/sp/800/172/a/r3/final>
- U.S. Department of Defense Chief Information Officer. (2026). Cybersecurity maturity model certification. <https://dodcio.defense.gov/cmmc/>
- Boletín Oficial de la República Argentina. (2026). Decreto 941/2025. <https://www.boletinoficial.gob.ar/detalleaviso/primera/337032/20260102>
- Boletín Oficial de la República Argentina. (2026). Disposición 1/2026 del Centro Nacional de Ciberseguridad. <https://www.boletinoficial.gob.ar/detalleaviso/primera/341893/20260513>
- Europol. (2026). 29 arrested: law enforcement strikes criminal networks behind illegal streaming. <https://www.europol.europa.eu/media-press/newsroom/news/29-arrested-law-enforcement-strikes-criminal-networks-behind-illegal-streaming>
- Europol. (2026). Cybercriminal VPN used by ransomware actors dismantled in global crackdown. <https://www.europol.europa.eu/media-press/newsroom/news/cybercriminal-vpn-used-ransomware-actors-dismantled-in-global-crackdown>

- Eurojust. (2026). Eurojust coordinated investigation shuts down criminal VPN network. <https://www.eurojust.europa.eu/news/eurojust-coordinated-investigation-shuts-down-criminal-vpn-network>
- Fiscal Information and Investigation Service. (2026). FIOD houdt twee verdachten aan wegens overtreding sanctiewetgeving. <https://www.fiod.nl/fiod-houdt-twee-verdachten-aan-wegens-overtreding-sanctiewetgeving/>
- Interpol. (2026). 201 arrests in first-of-its-kind cybercrime operation in MENA region. <https://www.interpol.int/news-and-events/news/2026/201-arrests-in-first-of-its-kind-cybercrime-operation-in-mena-region>
- Ministerio del Interior. (2026). Desarticulada una organización criminal que creaba herramientas informáticas para cometer ciberestafas bancarias. <https://www.interior.gob.es/opencms/es/detalle/articulo/desarticulada-una-organizacion-criminal-que-creaba-herramientas-informaticas-para-cometer-ciberestafas-bancarias/>
- National Cyber Security Centre. (2026). Joint operation by police and NCSC takes down major botnet. <https://www.ncsc.nl/en/news/joint-operation-by-police-and-ncsc-takes-down-major-botnet>
- Politie. (2026). International law enforcement initiate hunt on malware group SocGolish. <https://www.politie.nl/en/news/2026/juni/18/11-international-law-enforcement-initiate-hunt-on-malware-group-socgholish.html>
- U.S. Department of Justice. (2026). Canadian man arrested by international authorities and charged with administrating kimwolf DDoS botnet. <https://www.justice.gov/usao-ak/pr/canadian-man-arrested-international-authorities-charged-administrating-kimwolf-ddos>
- Escudo digital. (2026). Desmantelan una red que había infectado 15.000 páginas webs hechas con wordpress. <https://www.escudodigital.com/ciberseguridad/desmantelan-red-operacion-endgame-webs-infectadas.html>
- Operation Endgame. (2026). Operation Endgame. <https://www.operation-endgame.com/>
- Breachsense. (2026). Top 7 dark web markets in 2026: what gets sold and how to monitor them. <https://www.breachsense.com/blog/dark-web-markets/>
- Cloudsek. (2026). Dark web forums and deep web communities. <https://www.cloudsek.com/knowledge-base/dark-web-forums-and-deep-web-communities>
- Deepstrike. (2026). Top dark web marketplaces. <https://deepstrike.io/blog/top-dark-web-marketplaces>
- Rapid7. (2025). Inside russian market: uncovering the botnet empire. <https://www.rapid7.com/blog/post/tr-inside-russian-market-uncovering-the-botnet-empire/>
- SOCRadar. (2026a). Top 10 deep web and dark web forums in 2026. <https://socradar.io/blog/top-10-deep-web-and-dark-web-forums/>
- SOCRadar. (2026b). Top 10 dark web markets in 2026: list & threat analysis. <https://socradar.io/blog/top-10-dark-web-markets/>
- SOCRadar. (2026c). Iran-Israel Cyber Conflict Dashboard. <https://socradar.io/iran-israel-cyber-conflict-dashboard/>
- Sophos. (2026). AI in the underground: curiosity, claims, and concerns. <https://www.sophos.com/en-us/blog/ai-in-the-underground-curiosity-claims-and-concerns>
- U.S. Department of Justice. (4 March 2026). United States leads dismantlement of one of the world's largest hacker forums. <https://www.justice.gov/opa/pr/united-states-leads-dismantlement-one-worlds-largest-hacker-forums>

- CrowdStrike. (2026). 2026 global threat report. <https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-global-threat-report-findings/>
- Google Cloud. (2026). Cybersecurity forecast 2026. <https://cloud.google.com/security/resources/cybersecurity-forecast>
- Google Threat Intelligence Group. (2026). ai-assisted vulnerability exploitation and initial access. <https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access/>
- Mandiant. (2026). M-Trends 2026. <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026/>
- Microsoft. (2025). Microsoft Digital Defense Report 2025. <https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/>
- World Economic Forum. (2026). Global Cybersecurity Outlook 2026. <https://www.weforum.org/publications/global-cybersecurity-outlook-2026/digest/>
- Biblioteca del Congreso Nacional de Chile. (2024). Ley 21.663: Ley marco de ciberseguridad. <https://www.bcn.cl/leychile/navegar?i=1202434>
- Gabinete de Segurança Institucional. (2026). Plano Nacional de Cibersegurança. <https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/plano-nacional-de-ciberseguranca-p-ciber>
- Presidencia de Colombia. (2026). Ley 2573 de 2026. <https://dapre.presidencia.gov.co/normativa/normativa/ley%20no.%202573%20del%2019%20de%20mayo%20de%202026.pdf>
- Aftra. (2026). The growing economic impact of cybercrime threats. <https://aftra.io/blog/economic-impact-of-increasing-cybercrime>
- Axonius. (2026). Verizon DBIR 2026: back to the fundamentals. <https://www.axonius.com/blog/verizon-dbir-2026-fundamentals-beyond-cves>
- Center for Strategic and International Studies. (2026). Significant cyber incidents. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
- CERT-EU. (2026). European commission cloud breach: A supply-chain compromise. <https://cert.europa.eu/blog/european-commission-cloud-breach-trivy-supply-chain>
- Check Point Research. (16 February 2026). 16th February threat intelligence report. <https://research.checkpoint.com/2026/16th-february-threat-intelligence-report/>
- Check Point Research. (16 March 2026). 16th March threat intelligence report. <https://research.checkpoint.com/2026/16th-march-threat-intelligence-report/>
- Check Point Research. (13 April 2026). 13th April threat intelligence report. <https://research.checkpoint.com/2026/13th-april-threat-intelligence-report/>
- Check Point Research. (18 May 2026). 18th May threat intelligence report. <https://research.checkpoint.com/2026/18th-may-threat-intelligence-report/>
- Check Point Research. (8 June 2026). 8th June threat intelligence report. <https://research.checkpoint.com/2026/8th-june-threat-intelligence-report/>
- Check Point Research. (2026). The state of ransomware Q1 2026. <https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/>

- Check Point. (2026). Security Advisory – Action Required – Active Exploitation of Check Point VPN Authentication Bypass (CVE-2026-50751). <https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/>
- Check Point Software Technologies. (2026). 2026 cyber security report. Stocktitan. <https://www.stocktitan.net/news/chkp/check-point-software-s-2026-cyber-security-report-shows-global-0aw8dddde6fjb.html>
- Cyber Insurance News. (2026). Verizon 2026 DBIR: vulnerability exploitation now the #1 breach vector. <https://cyberinsurancenews.org/verizon-2026-dbir-data-breach-report/>
- Cyber Security Agency Of Singapore. (February 2026). Largest multi-agency cyber operation mounted to counter threat. <https://www.csa.gov.sg/news-events/press-releases/largest-multi-agency-cyber-operation-mounted-to-counter-threat>
- Cybersecurity Dive. (16 March 2026). Telus digital confirms hack as shinyhunters claims credit for massive data theft. <https://www.cybersecuritydive.com/news/telus-digital-cyberattack-shinyhunters/814817/>
- Deepstrike. (14 June 2026). Infostealers stole 1.8B credentials. Shattered.io. <https://shattered.io/infostealer-malware-1-8b-credentials/>
- Federal Student Aid. (12 May 2026). Technology security announcement. <https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2026-05-12/technology-security-announcement>
- Group-IB. (13 March 2026). Six supply chain attack groups to watch out for in 2026. <https://www.group-ib.com/blog/supply-chain-attack-groups-2026/>
- INCIBE. (13 January 2026). Endesa notifica a sus clientes una filtración de datos personales. <https://www.incibe.es/ciudadania/avisos/endesa-notifica-sus-clientes-una-filtracion-de-datos-personales>
- INCIBE-CERT. (5 May 2026a). Detección de un acceso no autorizado a datos de usuarios de Booking. <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/deteccion-de-un-acceso-no-autorizado-datos-de-usuarios-de-booking>
- INCIBE-CERT. (11 May 2026b). Escalada local de privilegios en el kernel de Linux, Dirty Frag. <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/escalada-local-de-privilegios-en-el-kernel-de-linux-dirty-frag>
- INCIBE-CERT. (21 May 2026c). Incidente de seguridad en Inditex vinculado a infraestructura externa de un proveedor. <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/incidente-de-seguridad-en-inditex-vinculado-infraestructura-externa-de>
- Industrial Cyber. (24 March 2026). M-Trends 2026 reveals threat landscape shaped by faster, coordinated and industrialized cyberattacks. <https://industrialcyber.co/reports/m-trends-2026-reveals-threat-landscape-shaped-by-faster-coordinated-and-industrialized-cyberattacks/>
- Le Monde. (18 February 2026). Hacker accessed data from 1.2 million bank accounts. https://www.lemonde.fr/en/economy/article/2026/02/18/hacker-accessed-data-from-1-2-million-bank-accounts-french-economy-ministry-says_6750628_19.html
- Medtronic. (24 April 2026). Medtronic statement on unauthorized system access. <https://news.medtronic.com/medtronic-statement-on-unauthorized-system-access>

- Radware. (19 February 2026). 2026 global threat report shows DDoS attacks jump 168% as cyber threats escalate across networks and applications. GlobeNewswire.
<https://www.globenewswire.com/news-release/2026/02/19/3240861/0/en/radware-2026-global-threat-report-shows-ddos-attacks-jump-168-as-cyber-threats-escalate-across-networks-and-applications.html>
- SecurityToday. (6 April 2026). Ransomware 2026: pay or not pay.
<https://www.securitytoday.de/en/2026/04/06/ransomware-2026-companies-pay-ransom-payment/>
- Securityweek. (19 May 2026). Verizon DBIR 2026: vulnerability exploitation overtakes credential theft as top breach vector.
<https://www.securityweek.com/verizon-dbir-2026-vulnerability-exploitation-overtakes-credential-theft-as-top-breach-vector/>
- SentinelOne. (7 May 2026). 55 estadísticas más recientes de malware para 2026.
<https://www.sentinelone.com/cybersecurity-101/cybersecurity/malware-statistics/>
- SOSransomware. (28 February 2026). Ransomware in 2026: fewer victims paying but higher ransoms.
<https://sosransomware.com/en/ransomware-en/ransomware-payments-in-2025-fewer-victims-paying-but-higher-ransoms/>
- StationX. (June 2026). Cyber security breach statistics 2026: key facts & data.
<https://app.stationx.net/articles/cyber-security-breach-statistics>
- Stryker. (April 2026). Customer updates: stryker networks disruption.
<https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html>
- TechRepublic. (3 April 2026). FBI declares surveillance system breach a 'major incident'.
<https://www.techrepublic.com/article/news-china-linked-fbi-surveillance-breach-major-incident/>
- TechRepublic. (20 April 2026). 2026's breach list so far.
<https://www.techrepublic.com/article/news-top-cyberattacks-2026-so-far/>
- The Cyber Express. (12 March 2026). Cyber Warfare 2026: Nation-state attacks.
<https://thecyberexpress.com/cyber-warfare-2026-nation-state-attacks/>
- The Hacker News. (17 January 2026). Experts detect Pakistan-linked cyber campaigns aimed at Indian Government Entities.
<https://thehackernews.com/2026/01/experts-detect-pakistan-linked-cyber.html>
- The Hacker News. (2 May 2026). Trellix confirms source code breach with unauthorized repository access.
<https://thehackernews.com/2026/05/trellix-confirms-source-code-breach.html>
- Verizon. (2026). 2026 Data Breach Investigations Report.
<https://www.verizon.com/business/resources/reports/dbir/>
- World Economic Forum. (12 January 2026). Cyber Risk in 2026: what execs need to know as global cyber risk.
<https://www.weforum.org/stories/2026/01/geopolitics-ai-fraud-global-cyber-cybersecurity-2026/>
- Zscaler. (2 February 2026). APT28 leverages CVE-2026-21509 in operation neusplit.
<https://www.zscaler.com/blogs/security-research/apt28-leverages-cve-2026-21509-operation-neusplit>
- ESET. (2026). APT Activity Report.
<https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2025-q1-2026.pdf>

