TrendAI™ Research

Nation-Aligned APTs in 2025

AI-Fueled Threats and the Shifting Global Cyber Balance

Ted Lee
Senior Engineer-Threat Research,APT Ops

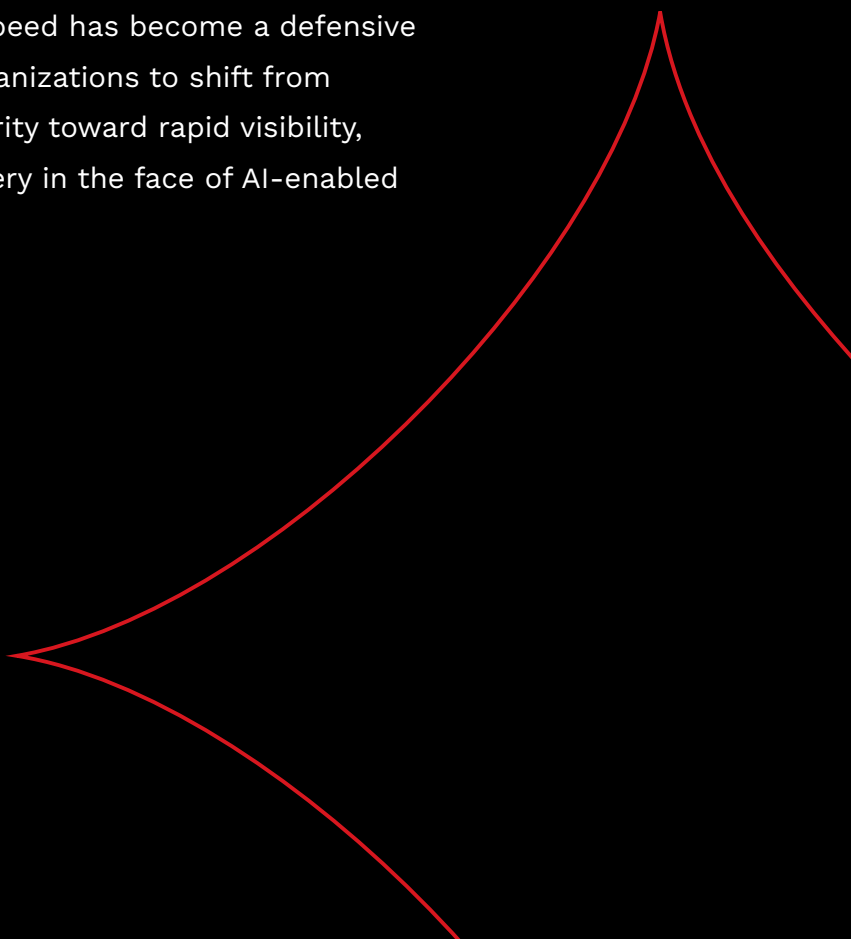
Kakara Hiroyuki
Senior Threat Researcher, Forward-Looking Threat Research Team AI and Data

Feike Hacquebord
Principal Threat Researcher, Forward-Looking Threat Research Team

Table of Contents

Key Takeaways

- Cyber operations are now tightly coupled with geopolitical objectives, with APT activity increasingly aligned to geopolitical events and military operations.
- Collaboration among APT groups is increasing attack speed and complexity, as access-sharing models such as “Premier Pass-as-a-Service” allow secondary actors to bypass initial compromise stages and complicate attribution.
- AI is now embedded directly in APT operations, with some nation-state-aligned actors deploying AI-assisted and semi-autonomous attack components that accelerate campaigns and sharply reduce defender response windows.
- Resilience at machine speed has become a defensive requirement, forcing organizations to shift from prevention-centric security toward rapid visibility, containment, and recovery in the face of AI-enabled threats.



1

Introduction

The TrendAI™ 2025-APT Annual Report offers a strategic overview of advanced persistent threat (APT) campaigns in 2025 and the first quarter of 2026, providing valuable insights for decision makers and senior defenders. It examines a pivotal year where cyberwarfare transcended traditional espionage to become a core pillar of national survival and regional dominance. A defining characteristic of 2025 was what major think tanks sometimes describe as the "Digital Autocracy" bloc; an informal axis of upheaval between China, Russia, North Korea (DPRK) and Iran.[1]

This report describes the 2025 campaigns and activities of APT actors aligned with Russia, China, and North Korea and how they try to leverage artificial intelligence (AI)[2] in an effort to neutralize Western sanctions and project power at "machine speed."

1.1. 2025 Annual Highlights

- **AI-Integrated kill chains:** 2025 marked the first practical deployment of large language models (LLMs) in active malware (e.g., Russia aligned LAMEHUG)[3] and AI-driven reconnaissance. Attackers have transitioned from using AI as a helper tool to deploying autonomous "AI agents" capable of real-time adaptation.
- **The "Premier Pass-as-a-Service" model:** China-aligned groups (Earth Estries and Earth Naga)[4] significantly transformed initial access by sharing compromised environments as a "priority pass" for other specialized units. This collaboration has made attribution more complex and has significantly increased the speed of secondary exploitation.
- **Cyber operations coinciding with broader geopolitical interests:** An example of this is North Korea's drone reconnaissance activities in Ukraine occurring alongside cyber campaigns.

- **Supply chain and edge dominance:** The exploitation of edge infrastructure (e.g., Ivanti) and developer ecosystems (e.g., Void Dokkaebi's fake job lures) has become the preferred route for high-stealth, long-term persistence.
- To effectively defend against both current and emerging APT campaigns, it is important for governments and large enterprises to understand the significance of the four previously-mentioned developments: AI-powered campaigns, the Premier Pass model, increased geopolitical alignment, and the focus on edge devices and supply chains. The use of AI solutions for defense is essential for scaling up and staying ahead of APT actors.

1.2. Strategic Outlook (2026–2027)

There are significant differences in the AI technology investments and development plans between the US and other countries.[5] **While China can compete with and even potentially exceed the advancements and innovations resulting from AI investments in the West, both North Korea and Russia face challenges in keeping pace**. This technological gap means that DPRK- and Russia-aligned APT actors will likely rely on niche attack methodologies and third party AI platform for their campaigns. Meanwhile, we can expect advanced attacks in the near future from China-aligned threat actors who will prove to be adept at using domestic AI tools and platforms.

The next 24 months will be a race for "resilience at machine speed." As APT actors move towards fully autonomous kill chains, the window for human intervention is closing. Successful defensive measures will depend on the deployment of "defensive AI" that can anticipate and neutralize agentic threats before they can perform lateral movement. In essence, no nation can afford to let their rivals get too far ahead in AI technologies.

2

Geopolitical Threat Landscape

In 2026, the global landscape is being dominated by a "Digital Autocracy" axis. China, Russia, Iran and North Korea have formed an informal strategic bloc aimed at achieving "digital sovereignty" using AI as a force multiplier to bypass Western sanctions and modernize their military and cyber capabilities.

For the rest of this report, our focus will be on China, Russia, and North Korea.

Feature	China (CN)	North Korea (DPRK)	Russia (RU)
Primary Goal	Global hegemony and self reliance	Regime survival and sabotaging others	National sovereignty
AI infrastructure	Sovereign stack (Huawei/SMIC)	Illicit/Russia-aided	Grey market/nuclear-backed
APT Style	Industrialized espionage	Financial and military asymmetry	Financial and military asymmetry Strategic sabotage

Table 1. AI strategies of China, Russia and North Korea

- **China: the "Full-Stack Anchor."** Through its "AI Plus" initiative,[6] Beijing has achieved an end-to-end domestic ecosystem. By mastering algorithmic efficiency (exemplified by DeepSeek-V3) and leveraging its unmatched ultra-high voltage (UHV) power grid, China remains the only country capable of sustaining a large-scale AI arms race against the US, even under intensified sanctions.
- **North Korea: the "Asymmetric Saboteur."** North Korea has transitioned from a recipient of technology to a specialized "digital guerrilla." A 2025 landmark defense pact with Russia[7] paved the way for the regime to gain access to high-end computing resources needed to fuel AI-driven cybercrime, generating funds through automated crypto-theft and deepfake-based social engineering to sustain its missile program.
- **Russia: the "Sovereign Fortress."** Operating under a war economy, Russia has pivoted to "automated battlefields." Despite hardware shortages, it uses its energy surplus, including nuclear-powered data centers, to fuel AI for electronic warfare and domestic surveillance, while increasingly relying on Chinese hardware and a "Russia-first" alliance with Pyongyang.

2.1. People's Republic of China

2.1.1. Political Trends

- **Strategic diplomacy and resource security:** Facing intensified US restrictions after major tech firms like Tencent and Contemporary Amperex Technology Co. Limited (CATL) were designated as Chinese military companies, China countered by deepening its ties with Russia and the Global South. A key highlight was their aggressive resource strategy, specifically securing mining rights in South America's "Lithium Triangle" to maintain a competitive edge in the global energy transition.[8]
- **Economic resilience amid structural challenges:** Despite a prolonged real estate slump and demographic headwinds, China managed to achieve its 5.0% GDP growth target, largely driven by a pivot toward high-tech investments (AI and new materials) and expanding exports to emerging markets. This shift helped offset the impact of the trade war with the US.
- **Military modernization and assertive posture:** With a 7.2% increase in its defense budget, China accelerated the deployment of stealth fighters and missiles. 2025 was marked by high-frequency exercises around Taiwan and long-range drills in distant waters — a clear intent to project power and maintain effective control over regional waters.

2.1.2. APT Activities Overview

In 2025, China-aligned APT groups expanded and further advanced their global cyberattacks. Several China-aligned groups deployed advanced malware and new methods to continue their cyberespionage activities.

- **Earth Kasha (associated with APT10):** Earth Kasha continued its spear-phishing attacks against government and research institutions in Taiwan and Japan.[9] The initial email attacks targeting Japanese think tank personnel were observed in 2024, with the group expanding its targets to Taiwanese government agencies in March 2025 via a new infection campaign using the ANEL malware. This campaign used content disguised as legitimate business emails to lure targets into downloading malicious ZIP files on OneDrive, eventually leading to a backdoor via Excel documents with macros (named ROAMINGMOUSE). The attack methodology in these attacks were similar to the 2024 Japan attacks, evading detection by using cleverly disguised legitimate cloud services to deliver malware.

- **Earth Preta (associated with Mustang Panda):** The primary targets of Earth Preta are government and public institutions in Southeast Asia and Europe. Our 2025 investigations confirmed the group's use of a technique that cleverly combines legitimate executables with malicious components for detection evasion.[10] Specifically, they employ DLL sideloading by exploiting trusted programs like VLC Media Player to execute malware such as PubLoad or MQsSrv in-memory. Through this "hiding in legitimate files" tactic, Earth Preta can disable security monitoring by security technologies and services such as Endpoint Detection and Response (EDR) while continuing the persistent infiltration and theft of confidential information within target organizations via spear phishing.

- **Earth Estries and Earth Naga (Premier Pass-as-a-Service):** These are recent China-aligned APTs that target a wide range of industries and regions. Earth Estries primarily focuses on telecommunications and government agencies and has significantly expanded its scope from the Asia-Pacific to South America and Africa over the past two years. Meanwhile, since 2021, Earth Naga has systematically concentrated on "strategically valuable" organizations in Taiwan, including government, telecom, media, academia, defense, and high-tech companies. As of 2025, it has expanded its intelligence targets to North America, the Middle East, and Africa, aligning its movements with global information-gathering needs.

A new trend that has emerged with these group's activities is an advanced collaboration model we call "Premier Pass-as-a-Service."[11] This model refers to an arrangement where a specific threat group infiltrates deep within a target organization, then provides or shares the maintained access as a "priority pass" service to another specific group. Similar to a priority pass at a theme park, this mechanism allows the second group to skip the initial intrusion process and gain direct backdoor access to sensitive assets. There have been incidents where Earth Preta and Earth Naga were active within the same session, corroborating the reality of this model. This collaboration, which we have classified into a four-tier framework from A to D, is a complicating element that not only enables prolonged underground activities, but also makes intrusion detection and attribution significantly more difficult for organizations.

- **Other cases:** China-aligned APT activities also saw new developments, such as supply chain infiltrations and the utilization of overseas bases. In April 2025, an incident occurred where China-aligned attackers attempted to use a Taiwanese software company's server as a malware distribution point. Fortunately, the company responded early, preventing large-scale damage.

However, since this organization provides services to numerous Taiwanese manufacturers, the intent to target the supply chain of high-tech manufacturing companies was clear. Attackers used several sophisticated evasion techniques and a long-term infiltration strategy, persistently targeting the electronics industry supply chain in Taiwan. Additionally, arrests related to the theft of vaccine data from US companies[12] and the exposure of over 4 billion leaked personal data records within the country occurred in succession.[13]

2.1.3. Impact

The impact of China-aligned APT activities is multifaceted. Intellectual property and confidential information stolen through cyberespionage can contribute to the strengthening of defense capabilities and high-tech industries.

For instance, espionage against government and research institutions in Taiwan and Japan targets information that directly affects regional security and foreign policy (such as diplomatic negotiation strategies and advanced technology trends), posing a serious threat to the targeted nations. Furthermore, as evidenced by the attack targeting a Taiwanese supply chain server, these groups seek to enter major corporate networks through indirect routes, spreading the risk across broad industries. Even for companies outside traditional high-risk sectors, there is a risk that their business partners or service providers could be used as a stepping stone, necessitating increased vigilance across the entire supply chain.

It is also noteworthy that cyberattacks are occurring in connection with domestic situations. The 2025 arrests regarding vaccine data theft confirmed that espionage activities continue to target medical and academic institutions. Furthermore, Western nations have strengthened moves to exclude communications equipment from certain providers due to security concerns, with the US and Europe implementing phase-out policies in 2025.[14] These measures reflect a growing international distrust of these cyber activities and exerts both diplomatic and economic pressure on the government.

The “Premier Pass-as-a-Service” trend is particularly troublesome for defenders. **By sharing access rights behind the scenes, it becomes difficult to track attacks based on the traces of a single group**, potentially delaying the blocking of intrusion routes and the identification of the scope of damage. Consequently, early discovery and containment have become more difficult, increasing the risk of long-term exploitation of confidential information. In fact, the apparent inactivity of some China-aligned APTs in recent years may be due to their shift toward this collaborative model.

As described, the China-aligned APT threat is backed by advanced technical capabilities and national strategy, making it a risk that cannot be ignored by government agencies or general corporations. Because the targeted domains range from diplomatic and security information to advanced technology, economic data, and personal records, senior management, including CISOs, must understand the latest intelligence tactics and continuously review their own defense postures. Cross-domain defense (supply chain risk management, detection of unusual remote management tools, etc.) and the strengthening of information-sharing systems with government agencies are required.

2.2. Democratic People's Republic of Korea (DPRK)

2.2.1. Political Trends

- **Deepening "Russia-First" diplomacy:** North Korea solidified its strategic alliance with Russia, moving beyond rhetoric to "unconditional support" for the invasion of Ukraine. This relationship was bolstered by high-level military visits and a new cooperation agreement with Belarus, effectively creating a trilateral axis to counter Western pressure while maintaining a pragmatic, albeit cooler, distance from China.
- **Advancement in missile technology and combat integration:** North Korea achieved significant hardware milestones in 2025, including the unveiling of the Hwasong-20 Intercontinental Ballistic Missile (ICBM) and successful hypersonic missile tests. Notably, the military shifted toward active engagement by providing drone reconnaissance and personnel to the Ukrainian front, likely in exchange for Russian technical expertise in satellites and submarines.
- **Survival tactics amidst internal hardship:** While the regime tightened domestic social control and rejected all dialogue with South Korea, it attempted to bypass sanctions through "tourism diplomacy," opening the Wonsan-Kalma area specifically to Russian visitors. However, despite these efforts to secure foreign currency, the broader population continues to face severe food and energy shortages.

2.2.2. APT Activities Overview

The activities of DPRK-aligned cyber units remained aggressive and diverse in 2025. To potentially support the state's fiscal and military objectives, these groups continued the theft of funds from financial institutions and cryptocurrency businesses, the collection of confidential information, and offensive cyber operations against various countries.

Notably, DPRK-aligned APT groups employ sophisticated methods to target developer communities and software supply chains, characterized by a wide range of attacks beyond the traditional government and defense sectors.

- **Void Dokkaebi (associated with Famous Chollima):** Void Dokkaebi is either a faction of the Lazarus Group, or a closely-related attack group, known for a series of campaigns targeting software developers and IT companies. From late 2024 through the first half of 2025, the group frequently used methods to lure targets with fake job offers or freelance contracts, sending project files or NPM packages containing malware. For instance, in an operation reported under the name "Contagious Interview",[15] they distributed packages with embedded malware to Web3/blockchain developer communities, turning many developer terminals into backdoors. These activities are grouped as Void Dokkaebi using our classification.[16]

  The group continuously updates its tools, including introducing an improved version of the new Python-based RAT GolangGhost,[17] forming a sophisticated threat that blends advanced malware capabilities with social engineering techniques that skillfully trap developers.

- **Earth Kumiho (associated with Kimsuky):** Earth Kumiho, which was previously sanctioned by Japan, the US, South Korea, and Australia in November 2023,[18] primarily targets government officials, diplomatic and security think tanks, experts on DPRK issues in South Korea, the US, and Japan in general. The group uses a notable attack methodology: in 2025, Earth Kumiho sent ZIP files containing shortcut (LNK) files to targets which, when executed, deployed attacks via PowerShell scripts. After the LNK execution, numerous scripts are downloaded from cloud services like Dropbox to collect and exfiltrate information or launch backdoors. When a target opens the LNK, a first-stage script starts via PowerShell, uploading survey results such as the machine's boot time, OS information, and process list to Dropbox. Subsequently, additional scripts obtained from private repositories on GitHub are used for continuous data theft and backdoor execution, eventually deploying remote control tools such as KimJongRAT or HttpTroy in memory.[19] A characteristic feature of Earth Kumiho is its abuse of trusted services like Dropbox and GitHub, with short-term deactivation of shared links to hide traces.

- **Earth Imp (associated with KONNI Group):** Earth Imp primarily targets South Korea and Russia and is thought to be a sub-organization of Kimsuky.[20] The group is known for conducting espionage via the KONNI malware (a remote access Trojan), targeting the personal and financial information of victims in South Korea, along with governmental and diplomatic information of victims in Russia.[21]

In 2025, Earth Imp's activities saw changes. After previously using LNK files with Korean-language filenames disguised as tax or financial documents to steal data in South Korea, the group launched espionage attacks against the Russian Ministry of Foreign Affairs via LNK files with Russian filenames that translate to "invitation." Although the latter showed some differing behaviors from the tactics used in the South Korean campaign, there were commonalities in the command-and-control (C&C) domains and types of information collected, leading us to believe that they were carried out by the same group.

The fact that this DPRK-aligned actor includes the government agencies of its nominal ally, Russia, as targets is noteworthy, showing that it is willing to steal information from anywhere regardless of geopolitical alliances, possibly to gain a better position in upcoming negotiations or collaborations.

- **Earth Manticore (associated with APT37):** Earth Manticore's primary targets are South Korean government and military organizations, and defector communities. Its activities were confirmed again in 2025; with a July RokRAT campaign using a malicious Hangul document (.HWP) being reported to be circulating in South Korea.[22] The group used the typical tactic of getting targets to open a specially crafted fake document before planting a backdoor in their system. Earth Manticore is also said to use browser exploits and mobile malware for broad espionage within South Korea.

2.2.3 Impact

DPRK-aligned APT activities are positioned as an essential "side business," potentially for maintaining the regime and achieving strategic goals, with impacts spreading across both international security and cyberspace. With regards to financial impact, North Korea obtains vast funds through cyberattacks even under sanctions. In fact, the amount of stolen cryptocurrency accumulates year by year, with UN reports suggesting that a significant portion of the funds for nuclear and missile development could be covered by cybercrime proceeds.[23] A massive theft of assets from a South Korean cryptocurrency exchange in 2025 highlights how these motivated cyberattacks represent a major management risk for the financial sector. Across the broader enterprise landscape, the targeting of software development and IT service providers has expanded to organizations beyond just the crypto and fintech fields. Attacks originating from trusted products and services, such as malware in NPM packages, or advanced social hacking using fake job openings risk spreading cascading damage.

In terms of information security, country secrets are threatened by these cyberespionage activities. **Military secrets, sensitive diplomatic information, and personal information of individuals such as activists critical of North Korea are**

among the primary targets of these attacks, with the impact of leakage leading directly to human damage and security risks. For instance, Earth Kumiho targets geopolitical information and diplomatic secrets from think tanks, which can be used to gain an advantage in diplomatic strategy or negotiations with the US. Furthermore, DPRK-aligned cyber units often operate with a high degree of autonomy while leveraging internet infrastructure located in Russia or China, alongside DPRK-linked reconnaissance activities related to the war in Ukraine. This indicates that North Korea is stepping into a new stage where it involves itself in foreign conflicts by combining cyber capabilities with traditional military operations.

The international community is strengthening its response to these developments through law enforcement and sanctions. The US Treasury specifically designated Kimsuky for sanctions in November 2023, freezing the assets of related organizations and individuals. Furthermore, the US Department of Justice and South Korean authorities have taken concrete actions, such as indicting agents involved in cryptocurrency hacking and seizing virtual currency wallets used in crimes. In 2025, the United States sanctioned dozens of individuals and entities involved in DPRK-aligned illicit IT worker schemes, while intensifying efforts to disrupt related money-laundering networks, which include the use of cryptocurrency services and facilitators. While these international measures are expected to place pressure on illicit funding channels, the DPRK-aligned threat actors will likely pursue new methods to sustain their operations.

For organizations, it is important to note that these APTs do not necessarily target only state secrets but also intrude into private companies for profit. Companies handling crypto assets and blockchain technology, as well as groups of engineers with deep overseas connections, are prime targets for these groups. Moreover, these APT actors possess high stealth capabilities; once they gain entry into the system, they are able to hide for long periods, making it difficult to assess damage and impact. CISOs and senior managers should keep in mind that their own companies or related industries could be targets and strengthen defensive measures by gathering threat intelligence, actively monitoring indicators of compromise (IoCs), and regularly conducting incident response drills.

2.3. Russian Federation

2.3.1. Political Trends

- **Wartime attrition and stalled diplomacy:** Russia focused its military strategy on exhausting Ukraine by targeting critical energy infrastructure while maintaining large-scale ground offensives. Despite mediation efforts by the Trump administration

throughout 2025, peace negotiations remained deadlocked into early 2026, with the Kremlin demanding territorial concessions that Ukraine and the West continue to reject.

- **Total mobilization of economy and control:** To sustain a war budget that consists of 30% of national spending, the government implemented aggressive measures like VAT hikes and the issuance of Yuan-denominated bonds. Domestically, the regime tightened its grip by expanding the internet surveillance powers of the Federal Security Service of the Russian Federation (FSB) and criminalizing the viewing of "extremist" content to suppress anti-war sentiment.
- **Shift to "dual diplomacy" and new vulnerabilities:** Facing isolation from the West, Russia deepened its "honeymoon" with North Korea and strategic (though cautious) ties with China. However, 2025 also exposed emerging cracks in Russia's strategic position: influence faded in the former Soviet sphere (e.g., Armenia), while the Russian mainland faced increasing domestic disruption from drone strikes and cyberattacks on national infrastructure like Aeroflot.

2.3.2. APT Activities Overview

Russia-aligned intrusion sets synchronized with the invasion of Ukraine and deployed aggressive cyber operations in 2025. While continuing sabotage and espionage against Ukraine and its supporters, they also diverted their advanced cyber technology to espionage activities worldwide.

- **Pawn Storm (associated with APT28):** Pawn Storm remained active against Ukraine and Western nations in 2025. In April, the French government issues a public attribution linking a series of cyberattacks against its institutions to this group, alongside the publication of details.[24] Meanwhile, in May, the US Department of Defense issued a warning regarding attacks on Western logistics and technology companies,[25] underscoring that pressure is being applied not only in the military sphere but also on the economic infrastructure of hostile countries.

  In the context of the war, the group is believed to be actively conducting espionage against Ukraine and supporting nations. Notably, the LAMEHUG malware, reported by the Computer Emergency Response Team of Ukraine (CERT-UA)[26] as being used in attacks against Ukraine in 2025, has a feature that dynamically generates commands required for operation using large language models (LLMs), suggesting the practical use of LLMs in the field. Pawn Storm also demonstrated additional concealment techniques, including the use of a backdoor that communicated via Outlook macros for C&C. and malware hidden as steganography within PNG images.

- **Earth Dahu (associated with Gamaredon):** Earth Dahu is known for its persistent attacks against Ukrainian defense and government agencies. The group's tactics usually involve conducting spear-phishing using HTA files for initial instrusion. This is typically followed by the deployment of modules that self-spread via USB or a PowerShell version of the GammaSteel information theft tool in an attempt to invade the entire local network. Earth Dahu has actively used RAR files in its attack chain; in 2025, the group launched a campaign in which malicious RAR attachments were emailed to targets. When opened using a vulnerable version of WinRAR, the files exploited the path traversal vulnerability (CVE-2025-8088)[27] to deploy a malicious HTA file in the startup folder for infection.

- **Sandworm:** Known as an APT actor specializing in sabotage, Sandworm carried out destructive malware attacks on Ukraine in 2022 (such as Industroyer2 and CaddyWiper), with continued activity being observed in 2025. CERT-UA reported a series of cyberattacks by a group believed to be related to Sandworm that targeted several companies, including critical infrastructure operators for energy, water, and heating.[28] Confirmed activity included initial intrusions via LNK files disguised as PDFs, long-term information theft using rsync, and the use of malware such as SECONDBEST and CROOKBAG.

  In early 2025, Sandworm targeted dozens of companies, including ICS solution suppliers supporting Ukraine's critical infrastructure. The group has also intermittently launched attacks using the malware KALAMBUR disguised as legitimate security products or messaging modules. From June 2025 onward, the threat actor has demonstrated enhanced stealth methods, such as attempting privilege escalation via DLL sideloading using an on-screen keyboard process in campaigns targeting military-related organizations. Furthermore, the wiper malware PathWiper[29] was used in multi-stage attacks that aimed to cause substantial damage to internal systems. Attackers hijacked the administrative privileges of a legitimate endpoint management product to distribute and execute the wiper on many terminals simultaneously. PathWiper overwrites critical data such as the MBR and $MFT on connected storage, making the system unrecoverable. Destructive APTs like Sandworm possibly function as tools for direct military operations in cyberspace, posing a threat not only within Ukraine but also to the energy and logistics foundations of other European countries.

- **Earth Koshchei (associated with APT29):** In 2025, this group deployed several campaigns using advanced phishing and cloud platform abuse. In a May incident, multiple European diplomats, specifically Ministry of Foreign Affairs personnel, were targeted with emails disguised as wine tasting invitations containing links that led

to malware.[30] New malware types GRAPELOADER and WINELOADER were reportedly deployed to gather information from European diplomatic networks.

Furthermore, in the summer of 2025, the group conducted a large-scale watering hole attack exploiting Microsoft's device code authentication.[31] In this watering hole attack, a fake page disguised as a Cloudflare security challenge was displayed to users, prompting them to enter email addresses and other details to steal authentication information. The Amazon Web Services (AWS) security team discovered and blocked this attack infrastructure in August 2025, taking measures to close malicious domains and isolate hijacked cloud instances in cooperation with Cloudflare and Microsoft. However, the attackers immediately responded by registering new domains and moving their infrastructure.

- **Ghost Blizzard:** On December 29, 2025, a series of destructive attacks targeted approximately 30 wind and solar farms, a private company, and a combined heat-and-power facility in Poland.[32] Fortunately, the campaign did not disrupt electricity generation or compromise stability of the Polish electrical grid. Operations of the combined heat-and-power system, which serves half a million people in Poland, were also unaffected. After gaining initial access and elevated privileges, the threat actors deployed two wipers called DynoWiper[33] and LazyWiper, which are designed to overwrite system data and corrupt the Master Boot Record (MBR). This marks a clear escalation for Russia-aligned actors who are now willing to attack not only Ukraine's power grid, but also those in allied countries.

2.3.3 Impact

Russia-aligned APT activities strongly exhibit the characteristics of cyber warfare supporting the actual war in Ukraine, with their impact potentially reaching both the battlefield and the international community. The spearhead of these attacks are also directed not only at countries supporting Ukraine, but also towards neutral countries, creating global security risks. Groups like Pawn Storm and Earth Koshchei carried out espionage and sabotage against organizations in Western countries (government agencies, energy companies, logistics companies, international organizations, etc.) supporting the war. For example, hacking attacks launched against the French government and US companies were publicly condemned and became a diplomatic issue, intensifying state-to-state confrontation in cyberspace. Consequently, Western nations imposed cyber sanctions and issued public denunciations against Russia-aligned actors. In 2025, countries like France and the UK cited the involvement of military intelligence in official statements. This is an unusually strong measure, and international pressure is rising even in cyber domains.

Companies should note that these Russia-aligned APT attacks are not limited to government targets. Western defense-related and energy companies, as well as media and communications companies, have become targets for threat actors who aim to sever the flow of strategically important goods and information. Furthermore, credential theft campaigns that target a wide range of users indiscriminately (such as those conducted by Earth Koshchei) can affect general companies and individuals with no direct relation to military or diplomacy. This suggests that the attackers are casting a wide net for intelligence collection to acquire access rights in various fields for future operations.

In response, Western nations have been strengthening cooperation to counter these APTs. NATO is strengthening information sharing among member states through its Cyber Defense Centre, while the European Union (EU) has implemented asset freezes on individuals and organizations under its cyber sanctions regime. Japan also issued a statement for the first time in 2025, publicly naming and condemning specific threat groups, while the joint G7 statement called for coordinated action against malicious cyber activities. Although such measures impose a certain diplomatic cost, their ability to immediately halt ongoing attacks is limited. Therefore, companies and organizations must continue to prioritize independent defensive measures.

For CISOs and senior security executives, the Russia-aligned APTs cannot be ignored as a geopolitical risk. **Companies involved in businesses supporting Ukraine or the energy, transportation, and communications sectors (fields of high interest to the government) could become direct targets.** Even those that are not may suffer indirect damage if suppliers or partners are attacked. Organizations should integrate state-level attack scenarios into their incident response plans and strengthen preparedness through threat hunting and red team exercises. We also recommend that companies in critical infrastructure industries deepen cooperation with government authorities and actively participate in sharing early warning information and joint cyberdefense exercises.

Overall, **Russia-aligned APT activities in 2025 demonstrated a growing global reach while remaining closely tied with the war in Ukraine, reinforcing the view that cyberspace has become one of the main battlefields of state-to-state confrontation.** We expect this trend to persist, making it essential for corporate leadership to view cybersecurity from the perspective of geopolitical risk management and deal with it strategically. Cooperation between governments and the private sector to improve defense technology and establish deterrents will be the key to long-term cyberthreat mitigation.

3

Industry Victimology and Vertical Analysis

3.1. Global Targeting Statistics

Victimology Data

This section provides a statistical presentation of industries affected by APTs and the data-driven rationale for identifying four primary target sectors: Government & Defense,Energy & Logistics, Technology & Manufacturing, and Financial Services.

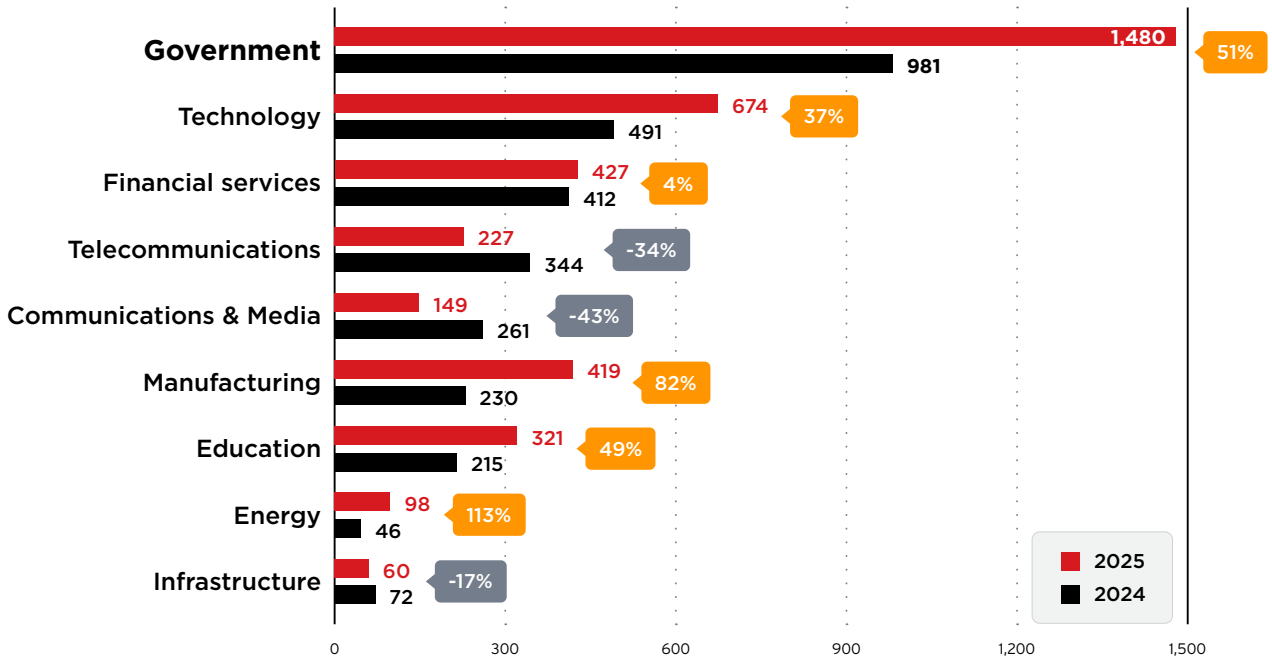


Figure 1. The top targeted industries by frequency of APT attacks

Government and technology sectors faced the highest volume of APT attacks in 2025. Although their year-over-year growth was marginal, these sectors have consistently remained among the primary targets over a long period. This reflects their core strategic value in intelligence collection, supply chain influence, and broader geopolitical and economic competition.

3.2. Threats Against Government and Defense

Government institutions remain top APT targets due to their control over policy, diplomacy, and defense. Observed campaigns primarily emphasize long-term infiltration, internal network reconnaissance, and intelligence collection.

- **APAC regional targeting:** China-aligned APT groups have demonstrated a persistent operational tempo across the APAC region, executing targeted campaigns against regional neighbors. Earth Preta focused on government agencies in the APAC, leveraging spear-phishing and strategies involving removable media. Meanwhile. Earth Baxia established long-term persistence within Taiwanese government infrastructure through sophisticated backdoors. Finally, Earth Kurma targeted government and telecommunications sectors across Southeast Asia, employing advanced custom malware, kernel-level rootkits, and cloud storage services for data exfiltration.
- **Eastern European Conflict Zone:** Russian-aligned actors continued high-intensity operations. Earth Dahu (Gamaredon) sustained a high volume of HTML Application (HTA)-based attacks against Ukrainian central and local government bodies. Pawn Storm (APT28) targeted government entities, frequently exploiting compromised legitimate accounts to evade detection. Earth Koshchei (APT29) orchestrated credential phishing campaigns against the government and education sectors in the US and Europe, abusing trusted cloud services to facilitate access.
- **American Region:** China-aligned APT groups (Earth Estries, Earth Naga, and Earth Alux) targeted the Americas, with a primary focus on government-related sectors. Earth Estries broadened its operational scope beyond APAC to target government entities in the United States and South America, employing a "Premier Pass-as-a-Service" collaboration model with Earth Naga to facilitate access and resource sharing. Concurrently, Earth Alux established a significant foothold in Latin America starting in mid-2024, using advanced tools like the VARGEIT backdoor to conduct long-term cyberespionage against regional government infrastructure. This convergence of APT actors suggests a strategic, geopolitically driven effort to compromise public sectors across both North and South America.

3.3. Threats Against Critical Infrastructure (Energy, Transport, Logistics)

APT activity targeting critical infrastructure has also increased significantly, reflecting its central role in national security and economic stability. APT campaigns predominantly focused on intelligence collection related to power grids and oil and gas infrastructure. These operations typically prioritize reconnaissance, credential harvesting, and prepositioning rather than immediate disruption, aligning with preparedness and deterrence strategies under geopolitical confrontation.

- **Sabotage and disruption:** Sandworm targeted Ukrainian logistics networks, grain equipment manufacturers, and railway operators. The group deployed destructive malware to disrupt operations, directly impacting Ukraine's economic stability and logistical support for the war effort.
- **Covert espionage and persistent access:** Earth Vetala (MuddyWater) targeted telecommunications providers and critical infrastructure organizations, including government-linked and energy-adjacent entities. The group leveraged social engineering and abused legitimate remote management tools to establish long-term footholds, continuously enhancing its stealth and persistent access capabilities to support sustained intelligence collection.
- **Transportation intelligence:** Earth Baxia expanded its targeting scope to include the transportation sector in Taiwan, likely to fulfill strategic intelligence gathering requirements regarding critical logistics infrastructure.

3.4. Threats Against Technology and Manufacturing

Technology and manufacturing sectors are highly targeted because of their critical roles in innovation and global supply chains. APT actors seek not only intellectual property and advanced research outcomes but also leverage these industries as entry points for lateral movement into government networks or critical infrastructure.

- **Developer ecosystem targeting:** DPRK-aligned threat actor Void Dokkaebi aggressively targeted software developers, with a specific focus on the Web3 and blockchain verticals. The group employed social engineering tactics, including fake job interviews, to distribute malware families such as BeaverTail and InvisibleFerret via malicious npm packages and compromised VSCode extensions.
- **Advanced industrial espionage:** Earth Baku targeted Taiwan's technology sector, employing advanced evasion techniques such as the abuse of Microsoft Dev Tunnel and Google Calendar for stealthy C&C communications.
- **Supply Chain and edge infrastructure:** APT actors increasingly exploited edge infrastructure vulnerabilities. For instance, UNC5221 and other groups targeted Ivanti Connect Secure appliances globally, deploying sophisticated implants like the SPAWN family to maintain persistent, stealthy access to corporate networks.

3.5. Threats Against Financial Services

While espionage remains the dominant motivator in other sectors, the financial sector continues to be a primary target for DPRK-aligned actors focused on illicit revenue generation.

- **Cryptocurrency theft:** Void Dokkaebi and Citrine Sleet continued to prioritize cryptocurrency assets as high value targets. Citrine Sleet (associated with the the AppleJeus cluster) focused on cryptocurrency organizations using macOS-specific malware such as INLETDRIFT.
- **Financial services targeting:** Earth Imp (KONNI) targeted financial services institutions in South Korea, utilizing tax and finance-themed decoys to distribute malware and compromise financial data.

4

Strategic Forecast: A Two-Year Horizon

The next two years will be a race to see what cybersecurity strategies and solutions can achieve "resilience at machine speed." Organizations need to be able to quickly adapt and recover from disruptions or cyberthreats with the speed and efficiency of automated machine-driven processes. In the context of cybersecurity, it emphasizes the importance of leveraging technology and automation to enhance resilience, enabling defenses to respond and adapt to threats as rapidly as they occur, minimizing downtime and maintaining operational continuity.

Countries around the world are accelerating efforts to reduce dependence on foreign AI platforms, cloud services, and digital connectivity. In an increasingly competitive environment, states can ill afford to let their rivals get too far ahead in AI technology. As a result, worldwide investments in sovereign AI tools, LLMs, and AI platforms have become priorities. AI development is more than a defensive requirement against criminal and APT-driven cyberattacks; states are also increasingly motivated to integrate AI into large-scale offensive operations.

4.1. Emerging Technologies and Threat Vectors

Private companies and governments are investing unprecedented sums in AI. According to estimates published by Reuters,[34] global investment in AI reached approximately 1.6 trillion dollars from 2013 to 2024, surpassing the cost of landmark historic initiatives like the Manhattan project and NASA's Apollo program.

While debate continues whether the massive investments into AI will pay off, a global race is underway to achieve leadership in AI-related technologies. In the West, the main driver is largely commercial, while, in contrast, some countries such as China have their AI technology development directed by the state. China has the ambition to be the world leader in AI technologies by 2030, focusing on autonomous driving, robotics, facial recognition, and the military use of AI (such as drones), and is widely

regarded as the only nation that can seriously compete with the US. Other states, such as North Korea and Russia, suffer from imposed sanctions that restrict their ability to compete at the same level. Recognizing these limitations, Russia has increasingly focused on AI sovereignty instead.

Regardless of AI's ultimate commercial success, it will fundamentally reshape how APT actors will conduct cyberattack campaigns in the next few years. We anticipate several significant changes fueled by AI:

- We will see an acceleration in attack campaigns, eventually leading to autonomous kill chains.
- Complex multistage attacks will become easier to launch, as AI simplifies reconnaissance, targeting, privilege escalation, and lateral movement.
- Malware will be replaced by AI agents that perform offensive tasks and can adapt to their targets' defensive schemes.[35]
- New commercial AI products and platforms will be abused by APT actors for the exfiltration of sensitive data and detection evasion, a trend we expect to be more pronounced among DPRK- and Russia-aligned APT actors.
- AI-powered, highly personalized spear phishing will become the norm, with attackers generating context-aware lures at scale.
- AI will accelerate the discovery of software vulnerabilities, logical errors, and misconfigurations across IT, cloud, and network environments. While this can support ethical hackers in finding bugs, leading to more robust systems, it also potentially enables malicious actors to find, identify, and exploit these flaws for cyberattacks.

4.2. Evolution of APT Tactics

This section summarizes our predictions regarding the automation of attacks, advanced evasion techniques, and the shift towards stealthier operations.

4.2.1. Automation of Attacks Using AI: Stealthier Operations

APT actors are increasingly using AI platforms to automate attack workflows and enhance evasion capabilities. Soon, attackers will use AI-driven reconnaissance to map corporate and government network infrastructures and quickly identify vulnerabilities.

The use of agentic AI composed of relatively small, seemingly fragmented tasks will avoid triggering safety filters, enabling attackers to automate multiple steps in the kill chain with minimal need for human intervention. An attack resembling this was reported in November 2025, illustrating an early step towards autonomous attack operations.[36]

In this campaign, human intervention remained critical, but it reflects a trajectory towards autonomous kill chains that are fully automated, AI-enabled attacks. We expect APT actors to outpace typical cybercriminal groups by leveraging state-level resources, which include tools developed by military and defense contractors. This trend is further evidenced by the early use of AI in disinformation campaigns. The FBI reported that Russian-aligned actors began to develop an AI-powered system called Meliorator as early as 2022, intended to support foreign malign influence and disinformation operations.[37]

Several APT actors were reported to have used publicly available AI platforms, like OpenAI[38] and Gemini,[39] to conduct reconnaissance, collect information, and research vulnerabilities. These groups also use generative AI to produce deepfake videos and craft highly convincing messages for spear-phishing campaigns. Looking ahead, we expect that the more brazen APT groups such as Pawn Storm will continue to leverage publicly available AI platforms and tools for evasion and rapid deployment.

However, at the same time, more stealthy APT actors will transition away from using Western-based AI platforms and start to use homegrown AI tools, language models, and sovereign AI platforms, leading to reduced visibility on how these groups are using AI in their attacks. We also expect that both APT actors and regular cybercriminals will continue to exploit vulnerable corporate MCP servers for data exfiltration.[40]

4.2.2. Prepositioning in Critical Infrastructure and Residential IoT Devices

APT actors will persist in their efforts to preposition within critical infrastructures such as telecommunications networks and power grids. Simultaneously, state-sponsored entities are increasingly exploiting millions of compromised residential IoT devices that are part of proxy networks and botnets. Some of these botnets are specifically created by APT actors themselves.[41]

Large residential proxy networks are being established by companies with formal legal structures and physical offices. Although these networks have been set up primarily for cybercriminal activities, they represent significant national assets for the countries where the companies managing them are headquartered. Following this reasoning,

these large residential proxy networks can also be viewed as prepositioning by nation state actors.

In times of heightened geopolitical tensions, these networks can be used for espionage, DDoS attacks, large-scale password spray attacks, as well as a launching point for attacks against devices on the local network that are not directly exposed to the internet but can be accessed through end nodes of residential proxy networks. Despite efforts to dismantle some of the networks,[42] massive botnets of IoT devices continue to operate.

4.2.3 Collaboration Among APT Groups

APT groups are increasingly sharing access and infrastructure to enhance their technical capabilities. These partnerships produce more sophisticated, stealthy operations[43, 44] that make attribution more difficult. The December 2025 attack against the Polish electrical grid was attributed by security vendor ESET to the Russian-aligned group Sandworm,[45] while CERT Polska attributed the campaign to Ghost Blizzard.[46] This example illustrates how attribution has become murky, with different organizations openly disagreeing on the source of the attack.

4.2.4 Cybermercenaries, Private Companies, and Criminal Groups

In recent years, specialized and previously unknown APT groups have begun supplanting some of the special tasks and operations associated with long-established threat actors. A clear example is the Russian-aligned actor group Void Blizzard (Laundry Bear)[47] that successfully breached the Dutch National Police in 2024.[48] According to Dutch intelligence services, Void Blizzard conducts its cyber operations at a rapid pace, with relatively simple methods that are difficult to detect. CERT-UA attributed campaigns against Ukrainian organizations in late 2025 to Void Blizzard, even while the TTPs appear different.[49] In 2025, an alleged member of Void Blizzard was arrested in Thailand,[50] with unconfirmed online reporting suggesting that this Russian individual had a past as a cybercriminal.

Criminal groups, such as Void Rabisu[51] and the cybermercenary group Void Balaur,[52] have shifted from purely financial motives to geopolitical-motivated campaigns, possibly acting on behalf of existing intelligence services. Given the volatile geopolitical climate, we expect cybermercenaries and private companies to play a bigger role in APT campaigns.

5

Risk Mitigation and Defensive Strategies

The 2025 landscape requires a fundamental shift from preventing intrusions to limiting damage from inevitable compromises. Nation-state-aligned actors will gain access to target environments; the question is how quickly organizations will be able to detect them and how much damage they can do before discovery. For companies whose operational profile or internal risk assessments place them at high interest to a foreign state, the following strategic defense considerations are recommended. Effectively implementing these defenses will require a modern, full-stack platform designed to cover all elements of the organization. Fragmented reliance on multiple point solutions leaves visibility and security gaps, which nation-state-aligned groups particularly excel at exploiting.

5.1 Operating Under the "Assumed Breach" Mindset

Adopting an "assume breach" mindset reflects the reality that nation-state–aligned threat actors will eventually penetrate even well-defended environments. Rather than focusing exclusively on perimeter prevention, this approach prioritizes early detection, damage containment, and operational resilience. By accepting that compromise is possible, organizations can develop strategies that reduce impact.

Limiting the blast radius

- **Micro-segmenting critical assets:** Organizations should isolate R&D, financial systems, and executive endpoints from general networks.
- **Eliminating standing privileges:** Businesses should require just-in-time admin access with approval and automatic expiration.
- **Classifying and isolating data:** Defenders should avoid clearly labeling high-value assets, increasing the time and effort attackers must spend identifying critical data.

Detecting lateral movement

- **Performing behavioral analytics:** Organizations should focus on detecting credential theft, privilege escalation, and data staging, not just specific malware.
- **Monitoring critical chokepoints:** Critical chokepoints should be continuously monitored, including domain controllers, VPN gateways, backup servers, and developer workstations.
- **Creating alerts for anomalies**: Organizations should be on the lookout for anomalous behavior such as impossible travel events, off-hours privilege use, and unusual process execution.

Planning for long-term compromise

- **Building immutable offline backups:** IT and security teams should create immutable offline backups that are tested quarterly and stored in air-gapped environments.
- **Pre-contracting IR Firms:** Organizations should establish retainer agreements in advance of an incident to avoid delays during initial response.
- **Running tabletop exercises for 6- to 12-month dwell times:** Defenders should run tabletop exercises beyond ransomware scenarios that account for longer dwell times.

5.2. Implementing Practical, Not Aspirational AI Defenses

As AI becomes embedded in both offensive and defensive cyber operations, effective defense requires a measured, pragmatic approach rather than reliance on speculative "AI versus AI" narratives. While automation and machine learning offer meaningful advantages, they do not replace human judgment, particularly in high-impact decisions involving containment, recovery, or business continuity. This involves focusing on slowing attackers and augmenting human analysts.

Slowing automated reconnaissance

- **Deploying honeypots and decoy credentials:** Organizations should deploy honeypots and decoy credentials to waste the attacker's time.
- **Rate-limiting and monitoring AI platform usage:** IT and security personnel should rate-limit and monitor unusual API calls to commercial AI platforms.

- **Sandboxing internal AI agents:** Enterprises should sandbox internal AI agents with read-only access and strict logging.

Implementing human-AI collaboration

- **Using security orchestration, automation, and response (SOAR) for tier-1 triage:** Organizations should consider employing SOAR for tier-1 triage (log aggregation, IOC enrichment) to reduce defender workload.
- **Requiring human validation for containment actions:** While machine learning and AI can detect anomalies, organizations should still require human validation for containment actions.
- **Retaining human authority over critical actions:** Businesses should never outsource critical decisions (data deletion, system shutdowns) to automation.

5.3. Accepting the Limits of Edge Devices and Supply Chains

Edge infrastructure and software supply chains have become favored entry points for threat actors, reflecting their central role in enterprise connectivity. VPN gateways, firewalls, IoT devices, and third-party dependencies are frequently targeted to establish initial access or persistence, often outside the visibility of security controls. Effective defense in these areas requires accepting that not all compromises can be prevented and focusing instead on isolation, rapid containment, and impact reduction.

Protecting edge devices

- **Treating exposed edge infrastructure as compromised:** Organizations should treat all VPN gateways, firewalls, IoT as compromised, and isolate them from internal networks.
- **Patching or isolating vulnerable devices rapidly:** Organizations should reduce exposure by patching critical CVEs as quickly as possible or by taking devices offline.
- **Eliminating non-essential IoT:** Enterprises should remove non-essential IoT devices (smart TVs, cameras) or place them on guest networks.

Defending the supply chain

- **Focusing on software composition analysis (SCA):** Defenders cannot vet every dependency, and should instead focus on SCA for known vulnerabilities.

- **Isolating development environments:** Organizations can limit supply-chain compromise impact through stricter npm/PyPI controls and code review.
- **Segmenting third-party access:** Companies should accept that third-party compromises will happen, and thus segment networks so vendor portals are unable to grant full access to attackers.

5.4. Understanding That Collective Defense Is the Only Sustainable Solution

Nation–state–aligned threat actors cannot be countered effectively in isolation. Their scale, resources, and persistence exceed what any single organization can sustain over time. As a result, long-term resilience depends on collective defense, combining intelligence sharing, coordination, and joint response efforts to increase attacker cost and reduce operational freedom.

- **Joining information sharing and analysis centers (ISACs):** Organizations should be willing and able to share anonymized indicators of compromise (IOCs) and tools, tactics, and procedures (TTPs) with industry peers.
- **Partnering with national CERTs:** Businesses should establish relationships with national security entities prior to incidents. This provides them access to classified briefings and intelligence access.
- **Coordinating disclosure:** For organizations, sharing threat data forces attackers to rebuild infrastructure and disrupt their campaigns.
- **Raising attacker costs:** Organizations should force threat actors to expend additional time and resources through rapid patching, widespread use of deception techniques, and legal or regulatory action where feasible.

5.5. Improving Visibility and Awareness

5.5.1. The Importance of Comprehensive Visibility

Attackers tend to dwell and expand within the gaps: unmanaged endpoints, shadow IT, forgotten cloud assets, and network segments outside your security perimeter. Addressing these gaps requires achieving unified visibility across the enterprise environment, which can be enabled through integrated security platforms such as Trend Vision One™,[53] alongside other complementary security technologies.

- **Consolidating to a platform approach:** Organizations should deploy a unified security platform with centralized visibility across the entire attack surface (endpoints, cloud assets, network infrastructure, email, identity systems, data repositories). Fragmented point solutions create seams that attackers can traverse undetected.
- **Proactively eliminating blind spots:** Organizations should continuously discover and inventory all assets, including unmanaged devices, rogue cloud instances, and third-party integrations.
- **Using AI-driven risk assessment:** Firms should consider using modern platforms that analyze network configurations, asset relationships, and security posture to calculate risk scores and visualize potential attack paths before adversaries discover them.
- **Correlating across telemetry sources:** Extended Detection and Response (XDR) ingests and correlates signals across endpoints, cloud, network, and email to detect sophisticated attacks that evade siloed tools.

5.5.2. Knowledge Is Power: Actionable Threat Intelligence

Understanding which threat actors are targeting comparable organizations or their supply chains, the techniques they employ, and the indicators that signal their presence transforms visibility into actionable defense.

- **Consuming curated threat intelligence:** The TrendAI Vision One™ Threat Intelligence Hub[54] delivers emerging threat intelligence, which includes IoCs and contextual analysis as new threats are discovered. Defenders should proactively hunt for threats rather than merely waiting for alerts.
- **Understand attacker TTPs:** Strategic threat research covering both APT groups and cybercriminal operations provides insight into attacker methodologies, tooling, and the geopolitical motivations driving campaign. Organizations should anticipate

targeting and prioritize defenses accordingly.

- **Leveraging detailed threat coverage:** The individual threats discussed throughout this report have been covered in greater depth through the TrendAI Vision One™ Threat Intelligence Hub as they emerged. Here, businesses can find more detailed technical analysis, IoCs, and tactical guidance on the specific campaigns referenced in this report.

5.5.3. Shift to Proactive Defense

Combining comprehensive environment visibility with operationalized threat intelligence enables organizations to:

- Identify and remediate exposure before exploitation.
- Hunt for attacker presence using current intelligence.
- Prioritize patching and hardening based on active threat campaigns.
- Brief leadership on relevant risks with geopolitical context.

6

Conclusion: Resilience, Not Perfection

Organizations cannot indefinitely prevent nation-state-aligned actors from gaining initial access. Across the campaigns examined in this report, well-resourced threat actors consistently demonstrated the ability to bypass perimeter defenses, exploit trust relationships, and sustain covert access over extended periods. For governments and enterprises alike, the strategic objective is therefore not absolute prevention, but the ability to withstand intrusion, limit damage, and recover faster than adversaries can achieve their objectives.

This shift reflects the reality of the modern threat environment. APT campaigns have become an integral part of the geopolitical competition for many states, increasingly augmented by automation and AI. As attack speed accelerates and dwell times shorten, traditional security models that are built around episodic detection and manual response are proving insufficient. Resilience must now operate at machine speed, combining human decision-making with automation, visibility, and pre-planned response.

For organizations, the goal is to:

1. Detect intrusions faster, reducing dwell time from months to weeks.
2. Limit access and lateral movement through network segmentation and isolation of high-value assets.
3. Recover quickly by maintaining offline backups and regularly tested incident response plans.

Organizations that demonstrate sustained resilience share several common characteristics. They accept the likelihood of compromise and design environments accordingly, collaborate with peers rather than operate in isolation, prioritize protection of critical assets, and invest in people and processes ahead of costly standalone tools.

The threat landscape is permanent. Resilience is not a one-time initiative but an enduring operational posture, required for as long as geopolitical competition continues to shape the cyberspace.

References

1 Angela Stent. (October 2025). *Atlantic Council*. “The CRINK: Inside the New Bloc Supporting Russia’s War Against Ukraine.” Accessed on April 7, 2026, at: Link.

2 TrendAI™. (Aug. 20, 2024). *TrendAI™*. “What Is Artificial Intelligence (AI)?” Accessed on April 8, 2026, at: Link.

3 CERT-UA. (July 17, 2025). *CERT-UA*. “Кібератаки UAC-0001 на сектор безпеки та оборони із застосуванням програмного засобу LAMEHUG (CERT-UA#16039).” Accessed on April 7, 2026, at: Link.

4 Daniel Lunghi and Leon M Chang. (Oct. 22, 2025). *TrendAI™*. “Premier Pass-as-a-Service.” Accessed on April 7, 2026, at: Link.

5 Reuters. (2025). *Reuters*. “AI Investment: The Future of the US Economy.” Accessed on April 7, 2026, at: Link.

6 The State Council of the People’s Republic of China. (August 27, 2025). *Gov.cn*. “Latest Policies and Releases.” Accessed on April 7, 2026, at: Link.

7 Reuters. (December 4, 2024). *Reuters*. “North Korea-Russia Treaty Comes Into Force, KCNA Says.” Accessed on April 7, 2026, at: Link.

8 Francesco Torri and Manuel Núñez Fernández. (March 11, 2025). *Undisciplined Environments*. “China’s Expanding Footprint in South America’s Lithium Triangle.” Accessed on April 7, 2026, at: Link.

9 Hara Hiroaki. (April 30, 2025). *TrendAI™*. “Earth Kasha Updates TTPs in Latest Campaign Targeting Taiwan and Japan.” Accessed on April 7, 2026, at: Link.

10 Nathaniel Morales and Nick Dai. (Feb. 18, 2025). *TrendAI™*. “Earth Preta Mixes Legitimate and Malicious Components to Sidestep Detection.” Accessed on Apr. 7, 2026, at: Link.

11 Daniel Lunghi and Leon M Chang. (Oct. 22, 2025). *TrendAI™*. “The Rise of Collaborative Tactics Among China-aligned Cyber Espionage Campaigns.” Accessed on Apr. 7, 2026, at: Link.

12 United States Department of Justice. (July 8, 2025). *Office of Public Affairs*. “Justice Department Announces Arrest of Prolific Chinese State-Sponsored Contract Hacker.” Accessed on Apr. 7, 2026, at: Link.

13 Vilius Petkauskas. (June 10, 2025). *Cybernews*. “Largest Ever Data Leak Exposes Over 4 Billion User Records.” Accessed on Apr. 7, 2026, at: Link.

14 Reuters. (July 30, 2025). *Reuters*. “Telefonica Ditches Huawei’s 5G Gear in Spain and Germany; Keeps it in Brazil.” Accessed on Apr. 7, 2026, at: Link.

15 Unit 42. (Nov. 21, 2023). *Unit 42*. “Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors.” Accessed on Apr. 7, 2026, at: Link.

16 Feike Hacquebord and Stephen Hilt. (Apr. 23, 2025). *TrendAI™*. “Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations.” Accessed on Apr. 7, 2026, at: Link.

17 Vanja Svajcer. (June 18, 2025). *Talos Intelligence*. “Famous Chollima Deploying Python Version of GolangGhost RAT.” Accessed on Apr. 7, 2026, at: Link.

18 United States Department of the Treasury. (Nov. 30, 2023). *Treasury News*. “Treasury Targets DPRK’s International Agents and Illicit Cyber Intrusion Group.” Accessed on Apr. 7, 2026, at: Link.

19 Dominik Reichel. (June 17, 2025). *Unit 42*. “Exploring a New KimJongRAT Stealer Variant and Its PowerShell Implementation.” Accessed on Apr. 7, 2026, at: Link.

20 ESTsecurity. (June 20, 2019). *ESTsecurity*. “[스페셜 리포트] APT 캠페인 ‘Konni’ & ‘Kimsuky’ 조직의 공통점 발견.” Accessed on Apr. 7, 2026, at: Link.

21 FSEC. (Mar. 13, 2025). *FSEC*. “금융보안원, 국가배후 해킹조직의 금융권 대상 위협 경고.” Accessed on Apr. 7, 2026, at: Link.

22 ASEC. (July 21, 2025). *ASEC*. “악성 한글(.HWP) 문서를 이용한 RokRAT 악성코드 유포 주의.” Accessed on Apr. 7, 2026, at: Link.

23 MSMT. (Oct. 22, 2025). *MSMT*. “The DPRK’s Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities.” Accessed on Apr. 7, 2026, at: Link.

24 National Cybersecurity Agency of France. (Apr. 29, 2025). *CERT-FR*. “Targeting and Compromise of French Entities Using the APT28 Intrusion Set.” Accessed on Apr. 7, 2026, at: Link.

25 NSA, FBI, CISA, et al. (May, 2025). *NSA*. “Russian GRU Targeting Western Logistics Entities and Technology Companies.” Accessed on Apr. 7, 2026, at: Link.

26 Computer Emergency Response Team of Ukraine. (July 17, 2025). *CERT-UA*. “Кібератаки UAC-0001 на сектор безпеки та оборони із застосуванням програмного засобу LAMEHUG (CERT-UA#16039).” Accessed on Apr. 7, 2026, at: Link.

27 Google Threat Intelligence Group. (Jan. 28, 2026). *Google Cloud*. “Diverse Threat Actors Exploiting Critical WinRAR Vulnerability CVE-2025-8088.” Accessed on Apr. 7, 2026, at: Link.

28 Computer Emergency Response Team of Ukraine. (Feb. 23, 2025). *CERT-UA*. “Цільова активність UAC-0212 у відношенні розробників та постачальників рішень АСУТП (CERT-UA#13702).” Accessed on Apr. 7, 2026, at: Link.

29 Jacob Finn, Dmytro Korzhevin, Asheer Malhotra (June 5, 2025). *Talos Intelligence*. “Newly Identified Wiper Malware ‘PathWiper’ Targets Critical Infrastructure in Ukraine.” Accessed on Apr. 7, 2026, at: Link.

30 Check Point. (Apr. 15, 2025). *Check Point*. “Renewed APT29 Phishing Campaign Against European Diplomats.” Accessed on Apr. 7, 2026, at: Link.

31 CJ Moses. (Aug. 29, 2025). *Amazon*. “Amazon Disrupts Watering Hole Campaign by Russia’s APT29.” Accessed on Apr. 7, 2026, at: Link.

32 CERT Polska. (2025). *CERT.pl*. “Energy Sector Incident Report – 29 December.” Accessed on Apr. 7, 2026, at: Link.

33 Stephen Hilt and Robert McArdle. (Dec. 9, 2025). *TrendAI™*. “VibeCrime: Preparing Your Organization for the Next Generation of Agentic AI Cybercrime.” Accessed on Apr. 7, 2026, at: Link.

34 Reuters. (2025). *Reuters*. “AI Investment: The Future of the US Economy.” Accessed on April 7, 2026, at: Link.

35 Stephen Hilt and Robert McArdle. (Dec. 9, 2025). *TrendAI™*. “VibeCrime: Preparing Your Organization for the Next Generation of Agentic AI Cybercrime.” Accessed on Apr. 7, 2026, at: Link.

36 Anthropic. (Nov. 13, 2025). *Anthropic*. “Disrupting the first reported AI-orchestrated cyber espionage campaign.” Accessed on Apr. 7, 2026, at: Link.

37 Internet Crime Complain Center (IC3). (July 9, 2024). *IC3*. “State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity.” Accessed on Apr. 7, 2026, at: Link.

38 OpenAI LLC. (Feb. 14, 2024). *OpenAI*. “Disrupting Malicious Uses of AI by State-Affiliated Threat Actors.” Accessed on Apr. 7, 2026, at: Link.

39 Google Threat Intelligence Group. (Jan. 30, 2025). *Google Cloud*. “Adversarial Misuse of Generative AI.” Accessed on Apr. 7, 2026, at: Link.

40 Alfredo Oliveira and David Fiser. (July 17, 2025). *TrendAI™*. “MCP Security Network: Exposed Servers are Backdoors to Your Private Data.” Accessed on Apr. 7, 2026, at: Link.

41 Feike Hacquebord, Stephen Hilt, and Fernando Merces. (Mar. 17, 2022). *TrendAI™*. “Cyclops Blink Sets Sights on ASUS Routers.” Accessed on Apr. 8, 2026, at: Link.

42 Google Threat Intelligence Group. (Jan. 29, 2026). *Google Cloud*. “No Place Like Home Network: Disrupting the World’s Largest Residential Proxy Network.” Accessed on Apr. 8, 2026, at: Link.

43 Daniel Lunghi and Leon M Chang. (Oct. 22, 2025). *TrendAI™*. “Premier Pass-as-a-Service.” Accessed on April 7, 2026, at: Link.

44 ESET Research. (Sept. 19, 2025). *ESET*. “Gamaredon and Turla Target High-Profile Ukrainian Entities.” Accessed on Apr. 7, 2026, at: Link.

45 ESET Research. (Jan. 30, 2026). *WeLiveSecurity*. “DynoWiper update: Technical Analysis and Attribution.” Accessed on Apr. 8, 2026, at: Link.

46 Microsoft Threat Intelligence. (May 27, 2025). *Microsoft*. “New Russia-Affiliated Actor Void Blizzard Targets Critical Sectors for Espionage.” Accessed on Apr. 7, 2026, at: Link.

47 Microsoft Threat Intelligence. (May 27, 2025). *Microsoft*. “New Russia-Affiliated Actor Void Blizzard Targets Critical Sectors for Espionage.” Accessed on Apr. 7, 2026, at: Link.

48 General Intelligence and Security Service. (May 27, 2025). *AIVD.nl*. “AIVD and MIVD identify new Russian cyber threat actor.” Accessed on Apr. 7, 2026, at: Link.

49 Computer Emergency Response Team of Ukraine. (Jan. 20, 2026). *CERT-UA*. ““Untrustworthy Fund”: UAC-0190 Targeted Cyber Attacks on SOUs Using PLUGGYAPE (CERT-UA#19092).” Accessed on Apr. 7, 2026, at: Link.

50 Laura Sharman, Helen Regan, and Sean Lyngaas. (Nov. 15, 2025). *CNN*. “Russian alleged cyber-hacker faces extradition to US after arrest in Thailand.” Accessed on Apr. 7, 2026, at: Link.

51 Feike Hacquebord, Stephen Hilt, Fernando Merces, and Lord Alfred Remorin. (May 30, 2023). *TrendAI™*. “Void Rabisu’s Use of RomCom Backdoor Shows a Growing Shift in Threat Actor’s Goals.” Accessed on Apr. 7, 2026, at: Link.

52 Feike Hacquebord. (Nov. 10, 2021). *TrendAI™*. “Tracking Void Balaur’s Activities: A Cybermercenary’s Journey.” Accessed on Apr. 7, 2026, at: Link.

53 TrendAI™. (2025). *TrendAI™*. “TrendAI Vision One™.” Accessed on Apr. 7, 2026, at: Link.

54 TrendAI™. (2025). *TrendAI™*. “TrendAI Vision One™ Threat Intelligence.” Accessed on Apr. 7, 2026, at: Link.

Want more insights like this?

trendmicro.com/apt

TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk.

Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data.

AI Fearlessly.

Learn more: **trendaisecurity.com**