TrendAI™ Research

2026 H1 APT REPORT:

How APTs Are Weaponizing Trust in the Age of AI

State-aligned threat actors are folding AI into every stage of the attack chain while hiding their infrastructure inside the services defenders already trust. This report unpacks the geopolitics driving the activity and what defenders should prioritize next.

TrendAI™ Research

Executive summary

This report provides an analysis of advanced persistent threat (APT) activity aligned to four major geopolitical regions from January to June 2026. Five points stand out:

- **AI is being used across more of the attacks observed.** In the first half of 2026, AI was observed in more stages of the intrusion; China-aligned groups used generative AI to sharpen exploits and to build malware through iterative "vibe coding." In one case an AI agent ran its own reconnaissance and lateral movement. Meanwhile, Russia-aligned and Democratic People's Republic of Korea (DPRK)-aligned actors have been observed to use commercial AI as well.
- **Known and zero-day flaws were weaponized quickly, and the supply chain was a favored entry point.** Russia-aligned Pawn Storm opened the first half of 2026 with an Office zero-day exploit. Earth Dahu, meanwhile, kept exploiting an unpatched WinRAR flaw for months because the tool does not update itself. Iran-aligned Earth Vetala scanned for a fresh Ivanti flaw within days of disclosure, while DPRK-aligned actors poisoned a widely used software package to reach downstream developers.
- **Critical infrastructure and physical-world targets came back into focus.** Iran-aligned actors turned to hands-on attacks on internet-exposed operational technology, tampering with fuel-tank gauges at U.S. sites. Meanwhile, Russia-aligned campaigns pressed against Ukraine and its partners across government, defense, and wartime aid. Operators posing as advertising buyers were also observed to use advertising intelligence (ADINT), harvesting location and device data from online ad auctions to track individuals through the apps they use.
- **Control and tooling increasingly ride on trusted and shared infrastructure.** Threat actors were observed to keep command and control (C&C) on services that enterprises already trust, such as major cloud platforms, developer tunnels, public blockchains, and paste sites. They favor these services so the traffic blends into normal activity and resists takedown. Many actors now rent malware as a service (MaaS) or share tooling, which obscures who is behind an intrusion.
- **The political picture behind these campaigns is durable.** The war in Ukraine has settled into a long fight while Russia tightens information control ahead of its September legislative elections. Meanwhile, the DPRK appears to be entrenching itself as a permanent nuclear-armed state funded by cyber theft. China manages its U.S. rivalry while pushing chip and AI self-reliance, and Iran-aligned operations escalate with regional tension. These trends are expected to continue to shape the threat picture at year end.

The analysis in this report is drawn from a broader, ongoing body of work: the APT Research Report, published bimonthly and available in TrendAI Vision One™ Threat Intelligence Hub. Readers will find the complete research, including indicators and technical details, in that ongoing series.

Table of Contents

People's Republic of China

People's Republic of China (PRC)-aligned intrusion sets were observed continuing to pursue cyberespionage. The political backdrop frames the targeting and tradecraft seen across the cyber activity we monitored in the first half of 2026.

Political trends

- **AI is a national priority, backed by energy abundance but constrained on chips.** China has positioned AI as a core engine of economic growth at the highest level of national planning. China's 15th Five-Year Plan (15-5), which aims to set the country's economic and developmental roadmap, named AI a central priority, supported by state investment in energy and domestic chip development. The country installed power-generation capacity that reached 4 terawatts (TW)[1] by the end of May 2026, a substantial base to draw on for compute-intensive AI. Cheap green electricity[2] in the western regions can reportedly enable rapid expansion of domestic computing capacity. Meanwhile, Chinese firms continue to develop new technologies[3] in response to sanctions affecting the production of cutting-edge chips.

- **Beijing has become a hub for high-level diplomacy.** In January, China hosted South Korean President Lee Jae-myung, Canadian Prime Minister Mark Carney, and UK Prime Minister Keir Starmer. This was followed by U.S. President Donald Trump's visit to Beijing, during which China and the U.S. agreed to set up committees to advance tariff cuts on select nonsensitive goods.[4] Discussions also touched on the possibility of increased Chinese purchases of U.S. agricultural products, Boeing aircraft, and energy. While issues such as China's near-monopoly on rare earth elements (REEs) and technological controls saw little progress, a framework for further talks was established. Shortly after, PRC President Xi Jinping and Russian President Vladimir Putin met in Beijing and signed roughly 40 cooperation agreements.[5] The pairing of the two summits underscored China's dual-track positioning: managing the U.S. trade relationship while deepening the Russia partnership.

- **Amid a Chinese military purge, U.S.-China military and trade tensions escalate.** In May, former defense ministers and onetime Central Military Commission members Wei Fenghe and Li Shangfu both received suspended death sentences for bribery.[6] The two generals are the most senior officers publicly sentenced so far in a campaign that China has pursued since 2022 against corruption and disloyalty within the military. Tensions also spilled into trade. The Pentagon expanded its list of Chinese "military companies"[7] to include Alibaba, Baidu, and BYD. Beijing retaliated by placing 10 U.S. firms on its export control list,[8] including rare earth producers MP Materials and USA Rare Earth. The PRC also barred nearly 50 U.S. defense contractors from Chinese government procurement.

Cyber campaigns

AI-assisted development and agentic lateral movement

- **AI-enhanced exploit development by Earth Krahang.** Earth Krahang is a China-aligned group that targets global government and defense sectors, often using compromised infrastructure to launch attacks. It used generative AI to enhance a publicly available proof-of-concept exploit for CVE-2026-0740,[9] a vulnerability in the Ninja Forms – File Uploads plugin for WordPress. The enhanced exploit could conduct large-scale automated scans to identify vulnerable public-facing servers. The group also installed Trae, an integrated development environment (IDE) AI coding tool developed by ByteDance, on its C&C server. AI-generated code comments written in Simplified Chinese suggested the operator's origin.

- **Vibe coding for malware development by Earth Naga.** Earth Naga (associated with Flax Typhoon) is a China-aligned group that heavily targets critical infrastructure, government, and technology sectors by employing highly adaptive, "living-off-the-land" (LotL) techniques to evade detection. It has been observed to use an iterative AI prompting workflow ("vibe coding") to develop a malicious PowerShell script. The script compiles and executes C# code at runtime to perform process hollowing and reflective loading of backdoor payloads. Multiple evolving versions of the script were found on the hosting server, with the AI's responses to prompts left inside the code as comments; these comments inadvertently revealed the development methodology.

- **The use of an autonomous AI agent for lateral movement by an unknown actor (possibly Earth Lamia).** The group deployed the Claude Code command-line interface (CLI) as an autonomous AI agent against an organization in Thailand. The actor jailbroke the AI model by falsely claiming the operation was a legitimate penetration test. The AI agent then autonomously conducted internal network scanning, exploitation attempts (EternalBlue, SMBGhost, PrintNightmare, SMB relay), credential harvesting (via secretsdump, LaZagne, and Impacket), and password spraying.

Abuse of legitimate services as C&C channels

- **C&C communication via Microsoft 365 email drafts by Earth Baxia.** Earth Baxia is a highly active China-aligned group targeting government entities across Southeast Asia and the Indo-Pacific. It is distinguished by its investment in custom tooling and commitment to maintaining a completely silent footprint. Its custom Rust backdoor called CRAITHNEX has been observed to communicate entirely through unsent draft emails via the Microsoft Graph API. It uses the API to read instructions from draft subject lines and write results back into draft replies while offloading file transfers to OneDrive. Because no emails are ever sent, the traffic blends seamlessly into normal Microsoft 365 business operations. Detecting or blocking it is therefore exceptionally difficult without disrupting enterprise workflows.

- **Cloud service and blockchain transaction platform abuse by SHADOW-EARTH-067.** SHADOW-EARTH-067 is a China-aligned group targeting Taiwan, Thailand, and Malaysia, distinguished by its layered evasion and long-term persistence capabilities. Its WHISPERNOTE backdoor has been observed to abuse Microsoft DevTunnel, OneNote, and OneDrive for C&C communication. If those channels are disrupted, it falls back to parsing network configuration hidden in Stellar blockchain transaction memos. For lateral movement, the group builds a peer-to-peer mesh across infected hosts using KCP over User Datagram Protocol (UDP), with a Server Message Block (SMB) named-pipe fallback for restricted environments.

Multistage phishing with decoy documents and social engineering lures

- **The use of geopolitical lures and decoy PDFs for social engineering by Earth Baxia.** As an active group primarily targeting government entities in the Indo-Pacific, Earth Baxia crafts highly tailored spear-phishing emails centered on regional territorial disputes and policy forecasts. When a victim opens the attached malicious script (HTA or WSF), the malware displays a legitimate-looking decoy PDF to distract the user while silently executing the CRAITHNEX backdoor in the background.

- **The use of parallel vectors and trojanized software by APT24.** Known for broad cyberespionage campaigns across East Asia, APT24 uses multiple initial access pipelines simultaneously, hiding malicious shortcuts (LNK files) within Google Drive links. Most notably, the group has been observed to deploy SUESTAG, a malicious utility masquerading as a legitimate Taiwanese input method editor ("Going IME") updater. It displays a realistic update dialog to capture user credentials and drop the NOMASTEAL information stealer.

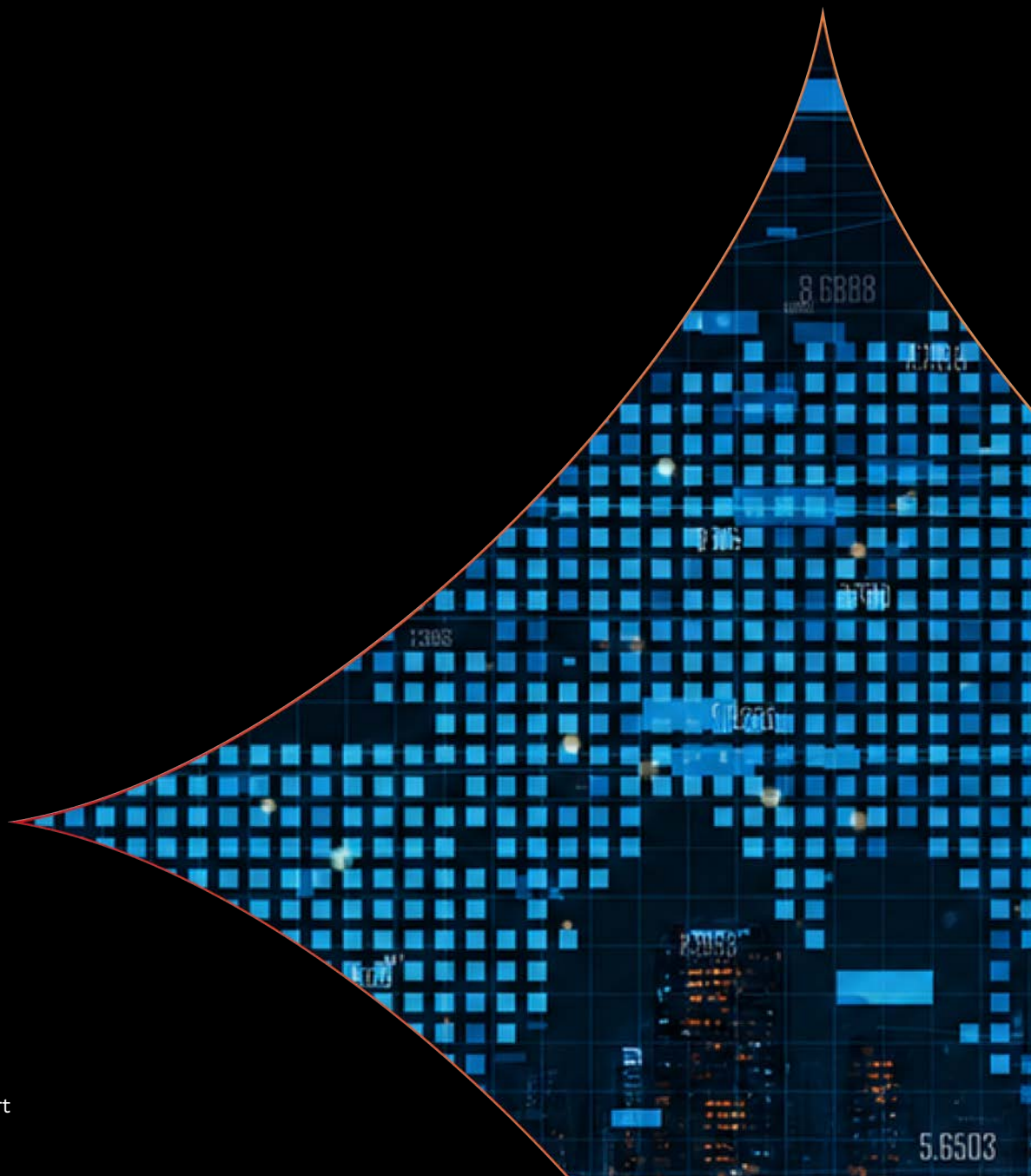
- **The use of multiturn trust-building and watering-hole traps by SHADOW-EARTH-068.** Focusing heavily on the maritime, semiconductor, and logistics sectors, SHADOW-EARTH-068 takes a high-patience approach by engaging in multiweek email conversations under corporate personas to build rapport before sending malware-laced payloads. The group has also been observed to execute watering-hole attacks by hijacking trusted websites and injecting scripts that display fake browser certificate errors in multiple languages (Traditional Chinese, English, German, and Indonesian). The scripts trick victims into downloading a malicious "CertFixer" utility. The campaign has targeted organizations across the Philippines, Taiwan, Indonesia, Peru, Czechia, Germany, and the U.S. Confirmed victims span government agencies, shipbuilding companies, semiconductor foundries, logistics firms, nongovernmental organizations (NGOs), and research institutions.

BYOVD for EDR and anti-malware evasion

- **Blinding endpoint detection and response (EDR) and anti-malware tools through BYOVD by SHADOW-EARTH-067.** In the first half of 2026, China-aligned groups increasingly used Bring Your Own Vulnerable Driver (BYOVD) techniques to blind security defenses. Rather than evading protections at the user level, these actors deploy rootkits that load trusted, signed third-party drivers with known vulnerabilities. This gives them kernel-level access, letting them disable EDR agents at the source. SHADOW-EARTH-067 has been observed to use this technique to permanently disable the victim's security monitoring, giving it undetected, full-system persistence during its operation. The group uses its custom DELEVATE loader to deploy the VIRIFUSE rootkit. It then weaponizes a vulnerable driver (ICRTouchIO.sys) to reach into the kernel and manipulate memory, unhook process-monitoring routines, and blind Event Tracing for Windows Threat Intelligence (ETW-TI) telemetry. An external configuration file supplies the per-version offsets that drive the entire chain. This lets the group run the same attack reliably across a wide range of Windows versions.

Democratic People's Republic of Korea (DPRK)

Democratic People's Republic of Korea (DPRK)-aligned cyber campaigns in the first half of 2026 remained dominated by financially motivated operations with espionage as an opportunistic byproduct. The main attack methods include supply chain poisoning, cryptocurrency theft, and IT worker infiltration. Separate cells appear to run these campaigns independently, each forced to fund their own operations.

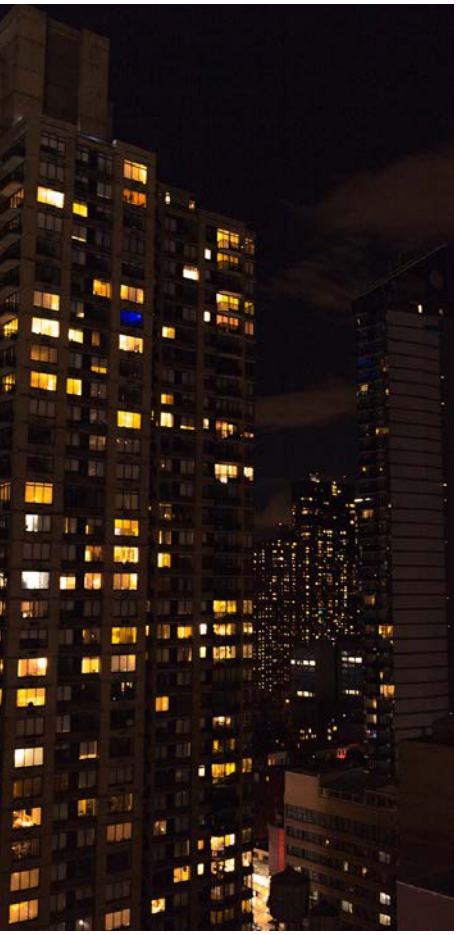


Political trends

- **Sanctions and power grid issues keep the DPRK from developing powerful AI models domestically.** International sanctions have left North Korea short of advanced chips, and the outdated electrical power grid might not reliably deliver the sustained load that large-scale AI requires. However, DPRK Supreme Leader Kim Jong Un's February 2026 address to the Ninth Congress of the Workers' Party of Korea put forward AI as an immediate priority.[10] The most concrete passage referred to "various AI unmanned attack complexes." Combined with the confirmed AI-guided missile tests in May 2026[11] and the drone training delegation to Russia's Far East, this suggests the military AI track is already in execution. To realize the DPRK's AI ambitions in the short term, it will have to continue with asymmetric methods. These include running computer servers outside the country, abusing Western-based AI models, using Chinese AI models, and receiving AI training in Russia.

- **The DPRK continues to establish itself as a permanent nuclear-armed state.** The cost of this nuclear ambition appears to remain a key driver of DPRK-aligned offensive cyber campaigns. In March 2026, a new solid-fuel rocket engine was reported to have been tested,[12] intended for intercontinental ballistic missiles (ICBMs). In March 2026, the DPRK amended its constitution to remove all references to "national unification," formally recasting South Korea as a separate hostile state. The change also explicitly grants Kim or a designated delegate command over the regime's nuclear forces.[13] In June 2026, the DPRK unveiled a new uranium enrichment site.[14] Within the same month, it commissioned its first 5,000-metric-ton multipurpose destroyer,[15] which may be able to launch nuclear-capable land-attack cruise missiles, though this has not been confirmed.

- **The relationship between North Korea and the United States remains frozen, with the former feeling little pressure to compromise.** Kim insists that the U.S. must abandon its denuclearization framework and accept North Korea as a permanent nuclear weapons state.



- **The Russia-DPRK relationship deepened further in the first half of 2026.** North Korea has sustained its support for Russia's war against Ukraine. In return, it receives food, cash, military technology, and innovative battlefield knowledge. Pyongyang now openly frames casualties as acts of great sacrifice for the homeland.[16] A DPRK delegation visited Russia's drone training center in Amur Oblast,[17] and multiple senior Russian officials visited Pyongyang. Russia issued more than 36,000 visas to DPRK nationals in 2025,[18] officially for what it labeled as educational purposes. This is approximately four times the 2024 figure, and the influx is likely intended to offset Russia's labor shortage.

- **After a period of apparent distance, China reengaged significantly with the DPRK.** Chinese Foreign Minister Wang Yi visited Pyongyang in April 2026, holding talks with both Foreign Minister Choe Son Hui and Kim himself. Beijing appears to seek to retain influence over the DPRK, likely as a card against the U.S., while preventing it from moving too closely toward Russia.

- **The DPRK economy is growing for the elite, and not for everyone.** It grew by an estimated 3.1% and 3.7%[19] in 2023 and 2024, respectively, suggesting recovery from the post-Covid contraction. However, this growth appears largely state-fueled, driven by military spending and by selling weapons and sending troops to Russia. Rice prices hit a sharp peak by October 2025,[20] roughly quadrupling in local currency. In U.S. dollar terms they remained stable, because the won collapsed against the dollar over the same period. It is effectively a wealth transfer from the population to the foreign-currency-holding elite and state apparatus.

- **DPRK cyber campaigns use Chinese and Russian internet infrastructure.** To be able to launch cyberattacks, the DPRK heavily relies on China and Russia for internet connectivity. Since the Russia-Ukraine war, North Korea has been using more static IP ranges in Russia.[21] The DPRK also deploys hundreds of virtual private servers (VPS) around the world. These servers are managed over virtual private network (VPN) services, proxies, and sometimes directly from IP addresses assigned to the DPRK, Russia, and other countries. These VPS instances are used for experimenting with AI, developing websites, hosting cryptocurrency scam sites, and hosting C&C servers. They also serve as egress points to access services such as LinkedIn, Upwork, GitHub, and Dropbox.

Cyber campaigns

Supply chain attacks target trusted developer infrastructure

- **BlueNoroff compromised the npm account of Axios's lead maintainer and published poisoned versions of the popular JavaScript HTTP client library[22] on March 31, 2026.** The victim is known to have over 100 million downloads per week. BlueNoroff, also known as APT38 and Sapphire Sleet, is a financially motivated Lazarus subgroup known for targeting cryptocurrency platforms and financial institutions. The group injected a phantom dependency called plain-crypto-js that was never used in Axios's code. It existed solely to trigger npm's postinstall hook, which deployed a cross-platform remote access trojan (RAT) targeting macOS, Windows, and Linux. TrendAI™ telemetry confirmed over 100 detections across 21 countries affecting organizations in government, finance, technology, healthcare, and other sectors.

- **Void Dokkaebi launched a wormlike campaign that lured software developers into cloning malicious code repositories disguised as job interview coding tests,[23] then turned their infected machines into propagation nodes.** The campaign used two infection vectors. The first is malicious VS Code .vscode/tasks.json files that auto-execute when a workspace is opened. The second is active commit tampering that injects obfuscated JavaScript into victims' repositories while rewriting git history. The delivered payload (a DEV#POPPER RAT variant) uses blockchain infrastructure for payload staging to resist takedowns and persists by hijacking developer applications such as VS Code, Cursor, and Discord. In March 2026, TrendAI™ identified over 750 infected repositories, over 500 malicious VS Code task configurations, and 101 instances of the commit-tampering tool. Repositories belonging to organizations such as DataStax and Neutralinojs carried infection markers. The group is also known as Famous Chollima and is best known for its BeaverTail and InvisibleFerret malware delivered through fake job interviews. It was also observed to combine social engineering with a propagation model that creates a supply chain risk.

Cryptocurrency theft remains a primary revenue channel

- **In April 2026, there were two large cryptocurrency theft incidents that were publicly associated with DPRK-aligned actor groups.** On April 1, 2026, US$285 million was stolen from the Solana-based decentralized exchange (DEX) Drift in an operation known as the Drift Protocol hack, likely carried out by one such group.[24] The theft followed months of social engineering against Drift's Security Council signers. The attackers exploited Solana's durable nonce feature to preauthorize withdrawals that executed in roughly 12 minutes.

On April 18, 2026, an unattributed DPRK-aligned actor group extracted about US$292 million from KelpDAO's cross-chain bridge. It compromised internal remote procedure call (RPC) nodes and launched a distributed denial-of-service (DDoS) attack,[25] forcing the bridge's single verifier to rely on poisoned data and approve a fraudulent cross-chain message.

Apart from the large heists, DPRK-aligned actor groups are likely to run smaller cryptocurrency scam websites targeting unsuspecting investors. Multiple DPRK-aligned actor groups such as Void Dokkaebi also steal from individuals' crypto wallets in their campaigns.

DPRK-aligned campaigns appear to be operated by self-financed cells

Attributing cyber campaigns to specific DPRK-aligned intrusion sets is often challenging because of overlaps in tactics, techniques, and procedures (TTPs) and infrastructure. Distinct subsets can also be identified within a single intrusion set. An explanation for this could be that different DPRK-aligned cells work independently with the same malware kit and have to self-finance their operations.

IT workers still infiltrate organizations worldwide

The IT worker scheme continues to feature prominently in DPRK-aligned cyber campaigns in 2026. According to TrendAI™ email scanning telemetry, several job openings attracted multiple applications from DPRK-aligned IT workers who progressed at least to online interview rounds. These IT workers are known to use face-swapping tools, deepfakes, ChatGPT, and similar tools for enhancing their resumes and for answering interview questions on the fly.

Multiple clusters of IT worker activity can be distinguished, based on technical indicators. This indicates that there are multiple cells that run the IT worker scheme, possibly from different locations in the world. In one observed case, a cluster of IT workers was linked to an apparent attempt to circumvent sanctions forbidding the export of computer numerical control (CNC) machinery into the DPRK.

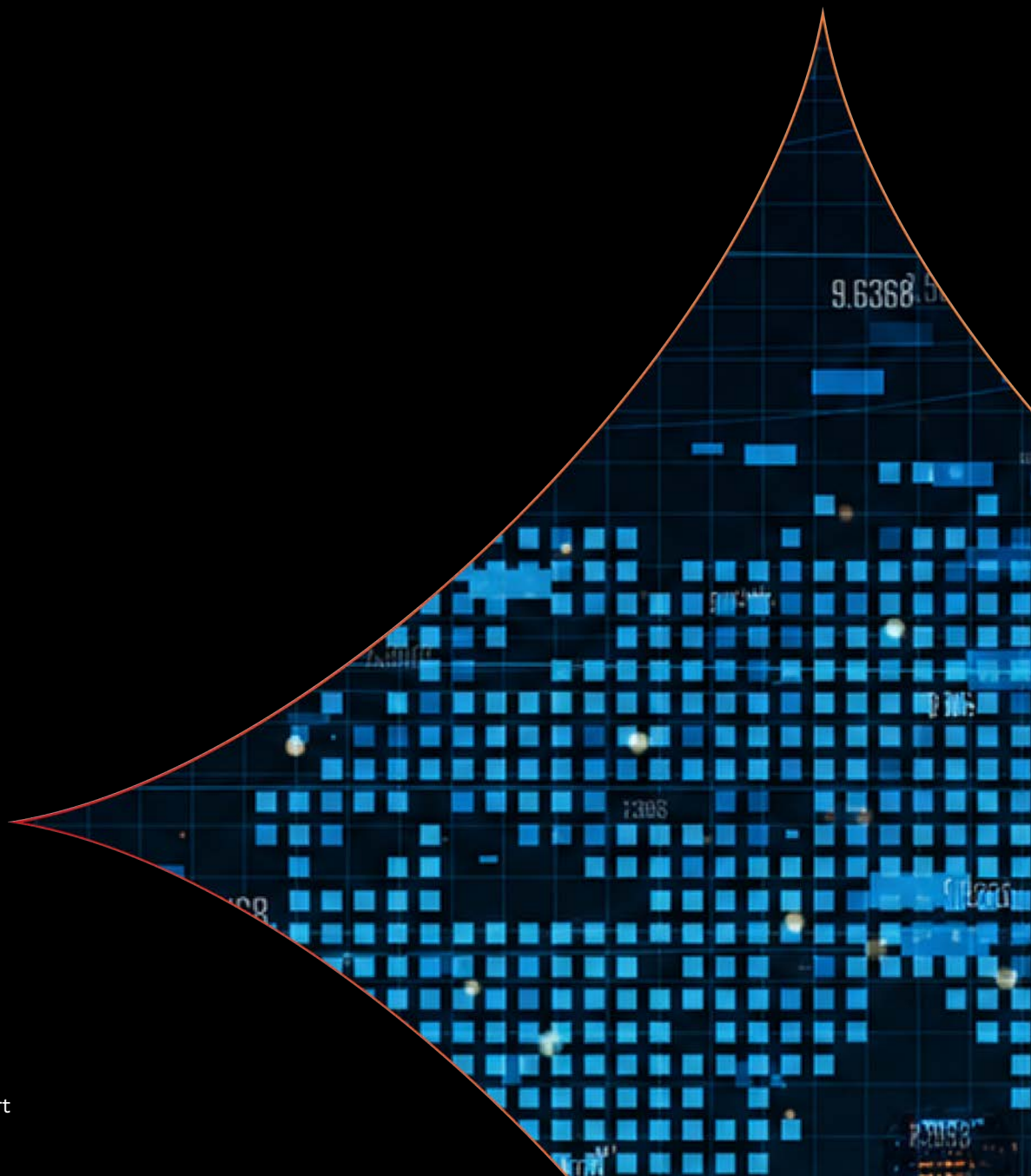
The IT worker scheme heavily depends on facilitators in targeted countries; these facilitators helped launder money and evade sanctions for the operation. The U.S. sanctioned facilitators in several countries, including Laos and Vietnam,[26] and sentenced a Ukrainian citizen[27] and four U.S. citizens in April[28] and May 2026.[29]

Espionage campaigns appear opportunistic

These campaigns tend to be opportunistic, arising as byproducts of other intrusions. Examples include Void Dokkaebi operations against high-profile targets and IT workers who secured positions in sectors such as defense. SHADOW-EARTH-062, a temporary designation for the Operation Dream Job-related intrusion set, is using BLINDINGCAN malware in highly targeted campaigns. In at least one case, TrendAI™ detected an attempted compromise in the supply chain for the defense sector.

The Russian Federation

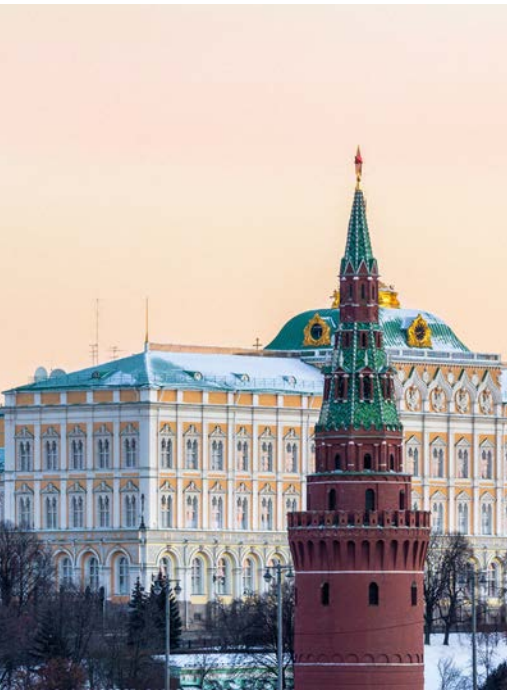
Through the first half of 2026, Russia-aligned cyberthreat efforts unfolded against three developments: a war settling into attrition, a state tightening its grip at home before September's Russian legislative elections, and a hard push into sovereign AI. Against that backdrop, its intrusion sets kept hunting the systems and supply lines that sustain Ukraine and its partners. Their tools ranged from a fresh Office zero-day exploit to a decade-old implant reworked into a botnet.



Political trends

- **A state-run push for sovereign AI is held back by a hardware ceiling.** Russia spent the first half of 2026 turning AI into a state project. In February, President Vladimir Putin created a Presidential Commission on AI,[30] with the Federal Security Service of the Russian Federation (FSB), the defense ministry, and Sberbank (Sber) represented. This signals that the Kremlin treats AI as a security and control tool, not just an industry. A draft federal law on sovereign, national, and trusted AI followed in March, which was also when Sber launched GigaChat Ultra. The hard limit the state faces now is computing capacity. Sanctions keep high-end GPUs scarce, forcing Russia to buy them through third countries at steep markups. Publicly available evidence does not show that Russian frontier models match leading Western ones. Russia's efforts in AI adoption are also moving into drones, with reported autonomous-targeting tests on Geran-2 airframes.

- **Russia is settling in to fight a frozen war for the long haul.** By the first half of 2026, Russia's invasion of Ukraine was in its fifth year.[31] The front line barely moved, even as casualties kept climbing and both sides traded limited gains to use as bargaining chips. Talks on territory were unproductive, and Ukraine kept up the pressure with intensified drone strikes on Russian oil refineries.[32] These attacks are intended to cut into Russia's refining output, pushing Moscow into fuel export curbs and regional rationing by mid-2026. After Ukraine and SpaceX moved to cut off unofficial Russian use of Starlink,[33] the vulnerability of Russia's battlefield communications became more visible. In parallel, Moscow continued developing its own satellite internet alternative through Bureau 1440,[34] which is reportedly aimed for commercial service by 2027. The drone war also matured on both sides, keeping weather data, logistics, and supply lines as valuable targets.



- **Information control is being locked in ahead of the September Duma election, the first since the invasion began.** The clearest domestic trend across the first half of the year is the state tightening its grip on the information space and doing it on a schedule. Mobile internet shutdowns went from border regions to nationwide[35] by late 2025, and by March 2026 even central Moscow lost stable service for more than 2 weeks. A new law now forces telecommunications providers to comply with FSB shutdown orders. Russia now also pushes a safelist of approved domestic services, including the homegrown Max messenger, while restricting Telegram, WhatsApp, YouTube, and Roblox. A Levada poll in February 2026 put support for peace talks at 67%,[36] a record. The fiscal picture is the other slow-moving risk. Oil and gas fell to about 23% of the federal budget,[37] the lowest in 5 years. A Middle East price spike briefly eased the decline, and value-added tax (VAT) was raised to fund the war.

Cyber campaigns

Exploiting document and file vulnerabilities for initial access

- **Pawn Storm opened the half with an Office zero-day exploit, weaponizing it ahead of public disclosure.** The group, also tracked as APT28 or Fancy Bear, has run Russia-aligned espionage against governments, militaries, and defense industries for years. It weaponized a previously unknown flaw in Microsoft Office[38] (a zero-day vulnerability tracked as CVE-2026-21509[39]) that let a prepared document quietly fetch and run the attacker's code with almost no user interaction. Rather than a memory-corruption bug, it turned on a logical gap in how Office decides which embedded objects are safe to load, easy to miss and hard to spot in transit. The attack infrastructure was registered about 2 weeks before disclosure, showing the group held it in reserve.
- **Earth Dahu leaned on a known WinRAR flaw that most of its targets did not patch.** Widely known as Gamaredon, it is a Russia-aligned group that runs high-tempo espionage against Ukrainian government and military targets. The prepared archive silently plants a file that runs the next time the machine starts[40] (CVE-2025-8088[41]). Because WinRAR does not update itself, many never fixed it, so the flaw stayed useful for months, and other groups exploited it in the same period. Both Russian cases reached targets through emailed files. One used a fresh zero-day vulnerability, while the other used an unpatched known bug. A single tool that never updates can keep an old flaw alive long after a fix exists.

Hiding the malware: obfuscation, steganography, and trusted runtimes

- **Pawn Storm hides its PRISMEX toolkit inside trusted processes and images to stay unseen.** It sets up persistence by hijacking a trusted Windows process, so the malware runs under a name the system already trusts. It then hides its next stage inside an ordinary-looking image using steganography,[42] spreading the hidden data across the whole image so it is hard to detect. The final stage runs entirely in memory and leaves little on disk. The toolkit extends a set of infection chains the group had run before, now fitted to exploit newly disclosed vulnerabilities quickly. This lets the same operator slot a fresh, high-value exploit into machinery it already trusts.

- **Laundry Bear (Void Blizzard) runs its code on a genuine, signed runtime, so the download looks legitimate.** Laundry Bear is a more recently identified Russia-aligned group focused on espionage against Ukraine and its supporters. Victims were approached over Signal-style messengers and steered to spoofed charity websites, where the malware arrived in several distinct loader variants. Those loaders pulled a genuine, signed programming runtime straight from the official source, then ran the attacker's own code on top of it. Because the download itself is legitimate, the activity is hard to flag. Its PLUGGYAPE backdoor[43] gained heavier obfuscation across successive versions, and there were signs the group was extending it to macOS.

- **Earth Dahu reshapes its loader every few weeks to stay ahead of detection.** Across the first half of 2026, the group's loader was observed to have changed format on a near-monthly cadence, moving from one scripting format to another and then to an encoded variant. Each shift lined up with defenders getting better at spotting the last one. By mid-year it also fell back on a 1990s archive format[44] that many email filters barely inspect, disguised with more familiar file extensions. The changes read as deliberate reactions to defenders catching up rather than routine rotation. Much of the phishing came from real but compromised government and municipal mailboxes, with the same account reused in several cases, which makes the mail look authentic to the recipient.

- **SHADOW-EARTH-065 leans on packing and disguise to keep its tools from being recognized.** SHADOW-EARTH-065 is the temporary designation of TrendAI™ for a Russia-aligned cluster that overlaps with UAC-0099 and has reportedly handed access to the destructive group Sandworm.[45] It packed its BadPaw[46] tool with a commercial protector, concealed the payload inside an image, and disguised the file as a harmless document type.

C&C built to blend in and resist takedown

- **Turla (Secret Blizzard) reworked Kazuar into a quiet botnet that is hard to find and hard to take down.** Turla is one of the oldest Russia-aligned espionage groups, known for stealthy, long-term intrusions into government and defense networks. It has run the Kazuar toolset since at least 2017, and from early 2024, TrendAI™ has observed it being used against government targets in Cyprus and Ukraine. Microsoft published an analysis showing Kazuar reworked into a botnet,[47] where only one elected node in each network reaches out on behalf of the rest. This sharply reduces the outbound traffic defenders can notice. It communicates mainly over ordinary web traffic, with other channels held in reserve. It collects its instructions from dead drops planted on compromised legitimate websites, so there is no fixed attacker server to block, and each victim group can be kept separate. TrendAI™ has tracked this three-module version of Kazuar since 2024.

- **Other groups keep their C&C on trusted services so it cannot simply be blocked.**
  - Pawn Storm routes PRISMEX through a legitimate encrypted cloud-storage service, so its C&C blends into routine encrypted web use.
  - Laundry Bear keeps its address on public paste sites such as Pastebin, rentry.co, and Ghostbin. The operators can change where the malware reports in by editing a web page rather than touching the malware.
  - Earth Dahu fronts its C&C with Cloudflare Workers and TryCloudflare tunnels, rotating the infrastructure quickly and tagging each build so the operators can tell which target set it belongs to.
  - SHADOW-EARTH-065 hides its traffic inside otherwise normal-looking web responses.

The shared goal is to make the connection back to the operator the least visible, most disposable part of the intrusion—the very part defenders have relied on to catch it.

Targeting entities connected to the war, with hacktivist pressure alongside

- **Pawn Storm reached across a wide set of war-related bodies rather than one sector.** It targeted a defense ministry, border police, a parliament, a defense university, and the national weather service, not only in Ukraine but among allies in the region.[48] The interest in a weather service is notable, since weather data feeds drone and artillery planning, and observed message content also pointed at Ukrainian military drone units.

- **Laundry Bear impersonated wartime charities to reach the same supply chain.** The group posed as charities offering generators and winter heating and timed its activity for the cold months. Its lures referenced drone positions and warehouse stocks in Ukraine and neighboring countries. A victim would see a genuine-looking document open as expected while the malicious code ran in the background. Taken with the interest in supply locations, the campaign reads as groundwork for physical strikes as much as intelligence gathering. Its reach was not limited to Ukraine; aid-linked organizations elsewhere were caught up in the same campaign. In late 2025, a Russian national was detained abroad at U.S. request over alleged involvement with the group.

- **SHADOW-EARTH-065 went after Ukrainian government and defense staff.** It posed as a border-guard unit, then deployed its BadPaw and MeowMeow tools. It has also been observed to have ties to a destructive group as mentioned in an earlier section.

- **NoName057(16) kept up volunteer-driven DDoS that tracks the politics of the war.** NoName057(16) is a pro-Russian hacktivist collective that runs DDoS attacks in support of Moscow's political aims. It hits government, transport, finance, and energy targets across dozens of countries, reaching beyond NATO, especially after a government announces support for Ukraine or sanctions on Russia. It runs on a custom tool handed to volunteers who are paid in cryptocurrency by how much they contribute. This lets a small core sustain the tempo on a Moscow working-hours rhythm. A European law-enforcement action in mid-2025 seized infrastructure and led to arrests, yet the group was back within days. That is the pattern to expect from a volunteer-fueled movement rather than a fixed organization. It is lower severity than the espionage campaigns, but it is the conflict's constant background noise.

Other regions

Outside what has been discussed so far, the most notable activity in the first half of 2026 was Iran-aligned. It ran along three lines that a defender should read together:

- Hands-on attacks on internet-exposed operational technology
- A shift toward renting criminal tooling and abusing trusted software rather than building in-house
- Tracking at scale in the surveillance ecosystem, with no malware required

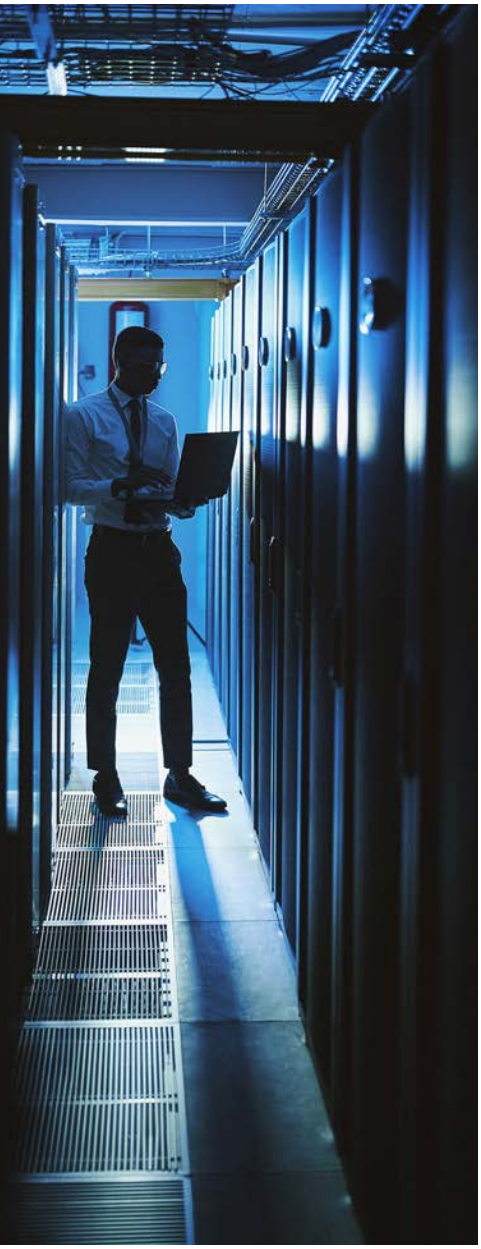
The through-line is that capability once limited to top-tier states is now bought off the shelf, which blurs who is behind an intrusion.

Cyber campaigns

Attacks on internet-exposed operational technology

- **Internet-exposed fuel-tank gauges became a live target in the first half of 2026.**[49] These gauges, at gas stations and storage sites, were designed to answer commands over the network without checking who is asking. Many reach the internet through aging adapters, so an attacker can read or alter tank data with simple commands. TrendAI™ first documented the exposure in 2015 with honeypot research, when attackers were already scanning for these systems, issuing valid gauge commands, and, in one case, changing a tank's name to a defacement message. That message was believed to be left by Iranian Dark Coders Team (IDC-TEAM), a pro-Iran hacktivist group known for defacements and low-level tampering. What began as opportunistic tampering has since escalated to attacks on real fuel infrastructure, and the same shape of problem applies wherever industrial readouts are placed online for convenience.

- **The U.S. joint advisory ties CyberAv3ngers to the IOCONTROL malware.**[50] It is an Iran-aligned group focused on attacks against critical infrastructure and operational technology. IOCONTROL can run on many kinds of Linux-based operational and connected devices, from cameras and routers to controllers and fuel-management systems. This makes it a reusable platform rather than a single-purpose tool. Around the same time, and attributed only to suspected Iran-linked actors, a nationwide wave of attacks breached U.S. fuel gauges,[51] including confirmed attacks in Tennessee.[52] There, one convenience store chain had 15 of its tanks affected and, in a few cases, tank and sensor data deleted. Exposure numbers reveal that the count of internet-facing gauges barely moved for years despite repeated warnings, then fell sharply only after these confirmed attacks and the coverage that followed. Beyond the network exposure, top-severity command-injection flaws in widely used gauges, such as CVE-2024-45066[53] in Dover units and CVE-2025-58428[54] in Veeder-Root's TLS4B, keep the software risk high.



Renting attack tools and abusing trusted software

Earth Vetala (MuddyWater) mixed its own tools with rented and trusted-software capability, and DinDoor is assessed as one of its backdoors. This Iran-aligned espionage group has been active across the Middle East for years. In the first half of 2026, it leaned on capability rented from criminal platforms, lowering cost and making attribution harder. Analysis of dump data from an internet-exposed server highly likely operated by the group showed this clearly. Alongside its own tooling, written in Persian, sat a rented backdoor called ChainShell,[55] bought as a service from a Russian-speaking criminal platform.

It was also quick to weaponize newly disclosed flaws, scanning for a fresh Ivanti vulnerability (CVE-2026-1281[56]) within days of its disclosure and exploiting a FortiOS flaw (CVE-2024-55591[57]) against targets. This shows how little breathing room a slow patch cycle now leaves.

A separate backdoor, DinDoor, shows the trusted-software angle: It runs the attacker's code on top of Deno, a legitimate and signed programming runtime. This reduces suspicion because defenses do not expect a trusted developer tool to be hostile. DinDoor points to a shared service used by more than one customer, and other researchers tied the same infrastructure to a ransomware operation.[58] It is assessed at medium confidence as a tool of Earth Vetala, based on shared code-signing certificates and Middle East victimology,[59] with the caveat that certificates can be stolen or reused. When the same tooling serves both espionage and a ransomware crew, the malware alone no longer tells a defender which one they are facing.

Hiding C&C on a blockchain

Earth Vetala resolves its C&C through a public blockchain, which makes it hard to block or take down. Its rented ChainShell backdoor carries no fixed address and instead works out where to report in by reading one from a public blockchain.[60] The lookups blend in with ordinary blockchain activity, so they are awkward to block. The address is also harder to remove once published than a conventional hard-coded domain or IP address, and the operator can change it without rebuilding the malware.

The malware also checks the system locale and avoids running on machines set to several post-Soviet Commonwealth of Independent States (CIS) languages,[61] a pattern common in Russian-speaking criminal tooling. Because this resilient technique now ships in tooling that several actors can buy, its presence says little about who is behind an intrusion. This pushes detection back toward endpoint behavior rather than the network destination.

ADINT: Surveillance at scale without malware

In another unattributed campaign, advertising intelligence (ADINT) tracks and deanonymizes targets by abusing the online ad ecosystem, largely without malware. Every time a phone shows an ad, details about the device and its location are broadcast to the companies bidding for that slot.[62] A party that registers as a bidder can collect this information without ever buying an ad and without touching the target device or network. Malware delivery through advertising does occur on a highly targeted basis, but it is secondary. The surveillance value comes from the bidstream data itself, and standard security tools cannot flag what is technically a legitimate advertising transaction.

A months-long investigation by TrendAI™ found two operators doing this. One was a U.S. company running an advertising business and a location-intelligence business side by side. The other, linked to the commercial spyware world, tracked over 184,000 people across more than 155 countries for over a year. Its focus shifted within hours of a regional election in Spain and the Strait of Hormuz crisis, which reads as intelligence collection rather than advertising. The risk is not hypothetical: In May 2026, U.S. Central Command reported that adversaries had used commercially available location data to target U.S. personnel in theater,[63] including in the Strait of Hormuz area. Because this happens inside the legitimate advertising system, there is no malware to detect, and the exposure comes from the data that leaks out of ordinary apps. The practical defense sits in governance and in limiting what device and location identifiers are allowed to leave staff phones in the first place.

Conclusion

These campaigns concentrate in a few places that defenders already know matter: trusted services, the software supply chain, and unpatched internet-facing software, with AI now added to the mix. The point is not to chase a single new tool, but to keep pushing detection and control toward those places. In rough priority:

Shift detection toward identity, cloud, and endpoint behavior.
Because C&C often hides in major cloud platforms, developer tunnels, blockchains, and paste sites, blocking known bad servers is not enough on its own. Watch for anomalous cloud and identity activity, enforce phishing-resistant multifactor authentication, and hunt on what a process does on the host, not only where it connects. Owner: Security Operations and Identity teams.

Treat the software supply chain and the developer as part of the attack surface.
A single poisoned dependency or maintainer account can reach many victims at once, as the npm package compromise showed. Pin and verify dependencies, turn alerts on for install-time scripts, and give maintainer and developer accounts the same protection as production systems. Owner: Governance and Security Operations.

Shrink the patch and exposure window on edge and unmanaged software.
Actors weaponized both zero-day vulnerabilities and long-known flaws, and tools that do not auto-update kept old bugs alive. Prioritize internet-facing systems, track software that patches slowly such as archive utilities and management appliances, and assume a capable actor may hold an exploit before a fix ships. Owner: Risk Management.

Take operational technology and critical-infrastructure devices off the public internet.
Fuel-tank gauges and serial-to-IP converters left exposed online were attacked directly this half. Remove these devices from public reach, segment and monitor control networks, and patch the highest-severity fuel-system flaws. The exposure count only fell after confirmed attacks and press coverage, which is not a model to rely on. Owner: Risk Management and Security Operations.

Plan for AI-accelerated adversaries, including AI already on the host.
Expect faster exploit and lure generation and early use of AI agents. Watch, too, for actors turning AI tools that already sit inside the environment, such as coding assistants and agent frameworks, into a way to act on the host. Expect the same tooling to serve both espionage and crime, so weigh behavior and intent over any single indicator when judging who is behind an intrusion. Owner: Security Operations and Governance.

References

1 National Energy Administration of China. (June 25, 2026). *National Energy Administration (*国家能源局*).* "National Energy Administration Releases National Electricity Statistics for January–May 2026." Accessed July 16, 2026, at: Link.

2 National Energy Administration of China. (June 30, 2026). *National Energy Administration (*国家能源局*).* "National Energy Administration Releases May 2026 Data on National Renewable Energy Green Power Certificate Issuance and Trading." Accessed July 16, 2026, at: Link.

3 Che Pan, Eduardo Baptista, and Casey Hall. (May 25, 2026). *Reuters.* "Huawei Proposes New Path for Chip Development Amid US Sanctions." Accessed July 16, 2026, at: Link.

4 Chang Siying. (May 16, 2026). *BBC News* 中文 *(BBC Chinese).* "Trump's Visit to China Concludes: The US and China Each Got What They Wanted, But Where Are Unresolved Issues Like Taiwan and Tariffs Headed?" Accessed July 16, 2026, at: Link.

5 Ministry of Foreign Affairs of the People's Republic of China. (May 21, 2026). *Ministry of Foreign Affairs of the People's Republic of China (*中华人民共和国外交部*).* "Joint Statement Between the People's Republic of China and the Russian Federation on Further Strengthening Comprehensive Strategic Coordination and Deepening Good-Neighborliness and Friendly Cooperation." Accessed July 16, 2026, at: Link.

6 Steven Jiang. (May 7, 2026). *CNN.* "China Gives Suspended Death Sentences to Two Former Defense Ministers." Accessed July 16, 2026, at: Link.

7 U.S. Department of Defense. (June 8, 2026). *U.S. Department of Defense.* "Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H." Accessed July 16, 2026, at: Link.

8 Ministry of Commerce of the People's Republic of China. (June 22, 2026). *Ministry of Commerce of the People's Republic of China (*中华人民共和国商务部*).* "MOFCOM Announcement No. 23 of 2026: Decision on Adding 10 US Entities to the Export Control List." Accessed July 16, 2026, at: Link.

9 Wordfence. (April 7, 2026). *National Vulnerability Database (NVD), NIST.* "CVE-2026-0740 Detail." Accessed July 16, 2026, at: Link.

10 Korean Central News Agency (KCNA). (Feb. 26, 2026). *KCNA Watch.* "Let Us Make Great Victory and Glory Gained Through Indomitable Pioneering Struggle Lead onto Steady Prosperity and Leaps Forward in New Struggle: Report on Ninth Congress of Workers' Party of Korea." Accessed July 16, 2026, at: Link.

11 Jack Kim and Joyce Lee. (May 27, 2026). *Reuters.* "North Korea Tests Mix of Enhanced Ballistic, Cruise Missiles and Artillery Rockets, KCNA Says." Accessed July 16, 2026, at: Link.

12 Vann H. Van Diepen. (April 2, 2026). *38 North.* "A New Rocket Motor Further Muddles North Korea's Solid-Propellant ICBM Outlook." Accessed July 16, 2026, at: Link.

13 Chung Yeong-gyo and Michael Lee. (May 6, 2026). *Korea JoongAng Daily.* "North Korea Scraps References to Unification, Limits to Kim's Powers in Amended Constitution." Accessed July 16, 2026, at: Link.

14 The Associated Press. (June 4, 2026). *NPR.* "North Korea Unveils a New Plant to Produce Fuel for Nuclear Weapons." Accessed July 16, 2026, at: Link.

15 Kim Tong-Hyung. (June 24, 2026). *Military.com.* "North Korea's Kim Claims Progress on Nuclear-Armed Navy as New Warship Is Placed into Service." Accessed July 16, 2026, at: Link.

16 Park Hee-soo. (June 26, 2026). *Daily NK.* "North Korea Marks Russia Treaty Anniversary with Lectures Glorifying Troops Killed in Ukraine." Accessed July 16, 2026, at: Link.

17 NK News. (May 19, 2026). *The Korea Times.* "North Korean Officials Tour Drone Operator Training Facility in Russian Far East." Accessed July 16, 2026, at: Link.

18 NK News. (April 8, 2026). *The Korea Times.* "Russia Issued Over 36,000 Visas to North Koreans in 2025, Almost All for Education." Accessed July 16, 2026, at: Link.

19 Bank of Korea. (Aug. 29, 2025). *Bank of Korea.* "Gross Domestic Product Estimates for North Korea in 2024." Accessed July 16, 2026, at: Link.

20 Kim Young-Hoon. (June 19, 2026). *Korea Development Institute (KDI).* "Chapter 5. Food and Agriculture in North Korea (The DPRK Economic Outlook)." Accessed July 16, 2026, at: Link.

21 Feike Hacquebord and Stephen Hilt. (April 23, 2025). *Trend Micro.* "Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations." Accessed July 16, 2026, at: Link.

22 Peter Girnus and Jacob Santos. (March 31, 2026). *Trend Micro.* "Axios NPM Package Compromised: Supply Chain Attack Hits JavaScript HTTP Client with 100M+ Weekly Downloads." Accessed July 16, 2026, at: Link.

23 Lucas Silva. (April 21, 2026). *Trend Micro.* "Void Dokkaebi Uses Fake Job Interview Lure to Spread Malware via Code Repositories." Accessed July 16, 2026, at: Link.

24 TRM Team. (April 2, 2026). *TRM Labs.* "North Korean Hackers Attack Drift Protocol in USD 285 Million Heist." Accessed July 16, 2026, at: Link.

25 Chainalysis Team. (April 23, 2026). *Chainalysis.* "Inside the KelpDAO Bridge Exploit: How ~$292 Million in rsETH Was Released Against a Non-Existent Burn." Accessed July 16, 2026, at: Link.

26 U.S. Department of the Treasury. (March 12, 2026). *U.S. Department of the Treasury.* "Treasury Sanctions Facilitators of DPRK IT Worker Fraud Targeting U.S. Businesses." Accessed July 16, 2026, at: Link.

27 U.S. Attorney's Office, District of Columbia. (Feb. 19, 2026). *U.S. Department of Justice.* "Ukrainian National Sentenced in 'Laptop Farm' Scheme That Generated Income for North Korean IT Workers." Accessed July 16, 2026, at: Link.

28 U.S. Department of Justice, Office of Public Affairs. (April 15, 2026). *U.S. Department of Justice.* "Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote Information Technology Worker Scheme that Generated $5M in Revenue for the Democratic People's Republic of Korea." Accessed July 16, 2026, at: Link.

29 U.S. Department of Justice, Office of Public Affairs. (May 6, 2026). *U.S. Department of Justice.* "Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote Information Technology Worker Schemes to Generate Revenue for the Democratic People's Republic of Korea." Accessed July 16, 2026, at: Link.

30 President of Russia. (Feb. 26, 2026). *President of Russia.* "Presidential Commission on the Development of Artificial Intelligence Technologies Established." Accessed July 16, 2026, at: Link.

31 Skye Lucas. (Feb. 23, 2026). *FRONTLINE, PBS.* "The Russia-Ukraine War Enters Its Fifth Year." Accessed July 16, 2026, at: Link.

32 The Associated Press. (July 1, 2026). *U.S. News & World Report.* "Ukrainian Drone Attacks on Oil Refineries Plunge Russia into a Summer Fuel Crisis." Accessed July 16, 2026, at: Link.

33 CNN. (Feb. 5, 2026). *CNN.* "Ukrainian Defense Ministry Says Starlink Terminals Used by Russia in Ukraine Are 'Cut Off'." Accessed July 16, 2026, at: Link.

34 Bloomberg News. (March 24, 2026). *Bloomberg.* "Russia Puts First Internet Satellites Into Orbit as SpaceX Rival." Accessed July 16, 2026, at: Link.

35 Human Rights Watch. (March 31, 2026). Human Rights Watch. "Russia: Internet Shutdowns Escalate — Peaceful Protests Over Lack of Access Suppressed." Accessed July 16, 2026, at: Link.

36 Bloomberg News. (March 4, 2026). *Bloomberg.* "Russian Support for Peace With Ukraine Hits New High, Poll Shows." Accessed July 16, 2026, at: Link.

37 Bloomberg News. (Jan. 15, 2026). *Bloomberg.* "Russia Oil and Gas Revenue Dives to Five-Year Low in Budget Hit." Accessed July 16, 2026, at: Link.

38 Feike Hacquebord and Hiroyuki Kakara. (March 26, 2026). *Trend Micro.* "Pawn Storm Campaign Deploys PRISMEX, Targets Government and Critical Infrastructure Entities." Accessed July 16, 2026, at: Link.

39 Microsoft Corporation. (Jan. 26, 2026). *National Vulnerability Database (NVD), NIST.* "CVE-2026-21509 Detail." Accessed July 16, 2026, at: Link.

40 Feike Hacquebord and Hiroyuki Kakara. (June 8, 2026). *Trend Micro.* "Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software Keeps the Door Open." Accessed July 16, 2026, at: Link.

41 Anton Cherepanov, Peter Košinár, and Peter Strýček. (Aug. 8, 2025). *National Vulnerability Database (NVD), NIST.* "CVE-2025-8088 Detail." Accessed July 16, 2026, at: Link.

42 Feike Hacquebord and Hiroyuki Kakara. (March 26, 2026). *Trend Micro.* "Pawn Storm Campaign Deploys PRISMEX, Targets Government and Critical Infrastructure Entities." Accessed July 16, 2026, at: Link.

43 CERT-UA (Computer Emergency Response Team of Ukraine). (Jan. 14, 2026). *CERT-UA.* "PLUGGYAPE Backdoor Deployed Against Ukrainian Defense Forces." Accessed July 16, 2026, at: Link.

44 HarfangLab Cyber Threat Research Team. (May 13, 2026). *HarfangLab.* "Gamaredon's Infection Chain: Spoofed Emails, GammaDrop and GammaLoad." Accessed July 16, 2026, at: Link.

45 ESET Research. (n.d.). *ESET.* “APT Activity Report: Russia-Aligned APTs Ramp Up Attacks Against Ukraine and Its Strategic Partners (April 2025 – September 2025).” Accessed July 16, 2026, at: Link.

46 ClearSky Research Team. (March 3, 2026). *ClearSky Cyber Security.* “Exposing a Russian Campaign Targeting Ukraine Using New Malware Duo: BadPaw and MeowMeow.” Accessed July 16, 2026, at: Link.

47 Microsoft Threat Intelligence. (May 14, 2026). *Microsoft Security Blog.* “Kazuar: Anatomy of a Nation-State Botnet.” Accessed July 16, 2026, at: Link.

48 Feike Hacquebord and Hiroyuki Kakara. (March 26, 2026). *Trend Micro.* “Pawn Storm Campaign Deploys PRISMEX, Targets Government and Critical Infrastructure Entities.” Accessed July 16, 2026, at: Link.

49 Kyle Wilhoit and Stephen Hilt. (2015). *TrendLabs (Trend Micro).* “The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems.” Accessed July 16, 2026, at: Link.

50 Team82. (Dec. 10, 2024). *Claroty.* “Inside a New OT/IoT Cyberweapon: IOCONTROL.” Accessed July 16, 2026, at: Link.

51 Cybersecurity and Infrastructure Security Agency (CISA), FBI, NSA, DOE, EPA, TSA, DOT, and USDA. (June 2, 2026). *CISA.* “CISA and Partners Urge Hardening Automatic Tank Gauge Systems.” Accessed July 16, 2026, at: Link.

52 Sean Lyngaas. (May 15, 2026). *CNN.* “Exclusive: Hackers Have Breached Tank Readers at US Gas Stations; Officials Suspect Iran Is Responsible.” Accessed July 16, 2026, at: Link.

53 ICS-CERT. (Sept. 24, 2024). *National Vulnerability Database (NVD), NIST.* “CVE-2024-45066 Detail.” Accessed July 16, 2026, at: Link.

54 CISA. (Oct. 23, 2025). *National Vulnerability Database (NVD), NIST.* “CVE-2025-58428 Detail.” Accessed July 16, 2026, at: Link.

55 Sean Moran. (April 7, 2026). *JUMPSEC.* “ChainShell: MuddyWater’s Russian MaaS Link.” Accessed July 16, 2026, at: Link.

56 Ivanti. (Jan. 29, 2026). *National Vulnerability Database (NVD), NIST.* “CVE-2026-1281 Detail.” Accessed July 16, 2026, at: Link.

57 Fortinet, Inc. (Jan. 14, 2025). *National Vulnerability Database (NVD), NIST.* “CVE-2024-55591 Detail.” Accessed July 16, 2026, at: Link.

58 Joseph Keyes and Daxton Wirth. (March 17, 2026). *ReliaQuest.* “Casting a Wider Net: ClickFix, Deno, and LeakNet’s Scaling Threat.” Accessed July 16, 2026, at: Link.

59 Check Point Research. (March 10, 2026). *Check Point Research.* “Iranian MOIS Actors & the Cyber Crime Connection.” Accessed July 16, 2026, at: Link.

60 Ctrl-Alt-Intel. (March 4, 2026). *Ctrl-Alt-Intel.* “MuddyWater Exposed: Inside an Iranian APT Operation.” Accessed July 16, 2026, at: Link.

61 Lisandro Ubiedo. (Nov. 20, 2025). *Securelist (Kaspersky).* “Blockchain and Node.js Abused by Tsundere: An Emerging Botnet.” Accessed July 16, 2026, at: Link.

62 Brian Krebs. (Oct. 23, 2024). *Krebs on Security.* “The Global Surveillance Free-for-All in Mobile Ad Data.” Accessed July 16, 2026, at: Link.

63 Raphael Satter. (May 28, 2026). *Reuters.* “Exclusive: Pentagon Says US Military Personnel Are Reportedly Being Targeted Using Location Data.” Accessed July 16, 2026, at: Link.

Want more insights like this?

TrendAI | Resources and Insights

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**

Copyright © 2026. Trend Micro Incorporated. All rights reserved. [REP00_2026_H1_APT_Report_290726US]