Monthly APT activity report – December 2025

Report Id: APT-20260101
Version: 1.0 (08.January.2026)

We start our monthly report with a quick overview of things that have made the headlines, research from other vendors that has caught our eye and some of the more important aspects of research that we've reported in the past month. Then we'll focus on the key activities in each region. We also provide summaries of the private reports that we have published this month. The final section includes Indicators of Compromise we have gathered from different sources, to assist with threat hunting.

Google Threat Intelligence Group reported that Intellexa[1], despite U.S. sanctions, continues operating as one of the most prolific mercenary spyware vendors exploiting mobile zero-day vulnerabilities. Intellexa has been linked to at least 15 zero-days since 2021, spanning Chrome, Android, and iOS, including RCE, sandbox escape, and local privilege escalation flaws used to deploy its Predator spyware. GTIG and partners captured a full iOS zero-day exploit chain, internally named "smack", combining a Safari RCE, kernel exploitation, and a stealthy spyware staging framework (PREYHUNTER). Analysis indicates Intellexa frequently purchases exploit components from external suppliers, reusing mature frameworks such as JSKit. The spyware incorporates extensive anti-analysis, environment detection, and surveillance capabilities, including keylogging, VOIP recording, and notification suppression. Delivery primarily relies on one-time links via encrypted messaging, with newer abuse of malicious advertising for victim fingerprinting. Overall, the activity highlights the continued resilience and evolution of the commercial spyware ecosystem despite growing international pressure.

Amazon Threat Intelligence reported rapid, in-the-wild exploitation of React2Shell[2](CVE-2025-55182) within hours of public disclosure, primarily by Chinese-speaking threat groups including Earth Lamia and Jackpot Panda. The flaw is a CVSS 10.0 unauthenticated RCE affecting React Server Components in React 19.x and Next.js 15.x/16.x using App Router. AWS MadPot honeypots observed both known and previously untracked clusters aggressively operationalizing public PoCs, often simultaneously exploiting other N-day vulnerabilities. Activity showed a volume-driven, trial-and-error exploitation approach, with actors iterating payloads, executing system commands, and attempting file writes on live targets. While many public PoCs were technically flawed, attackers prioritized speed over reliability, generating significant background noise.

Aikido Security uncovered the first sophisticated malware campaign on Maven[3] Central, involving a typosquatted Java package masquerading as the popular Jackson library. The malicious dependency abused the namespace org.fasterxml.jackson.core instead of the legitimate com.fasterxml.jackson.core, enabling stealthy supply-chain compromise via developer builds. Once loaded in a Spring Boot application, the malware auto-executed at startup, contacted a typosquatted C2 domain (fasterxml[.]org), and downloaded platform-specific payloads. The multi-stage loader used AES-encrypted configuration, heavy obfuscation, and persistence markers disguised as IDE files. Retrieved payloads included Cobalt Strike beacons for Windows, Linux, and macOS, indicating advanced post-exploitation intent. The package was removed from Maven Central within 90 minutes, highlighting both the risk and the need for namespace-similarity protections in Java ecosystems

ESET Research disclosed a previously unknown Chinese-speaking APT dubbed LongNosedGoblin[4], targeting governmental entities in Southeast Asia and Japan for cyber-espionage. Active since at least September 2023, the group uniquely abuses Active Directory Group Policy to deploy malware and move laterally across compromised

[1] Sanctioned but Still Spying: Intellexa's Prolific Zero-Day Exploits Continue
[2] China-nexus cyber threat groups rapidly exploit React2Shell vulnerability (CVE-2025-55182)
[3] First Sophisticated Malware Discovered on Maven Central via Typosquatting Attack on Jackson
[4] LongNosedGoblin tries to sniff out governmental affairs in Southeast Asia and Japan

networks. Its custom C#/.NET toolset includes NosyHistorian for browser-history reconnaissance, which guides selective deployment of the NosyDoor backdoor. NosyDoor relies on cloud services (Microsoft OneDrive, Google Drive, Yandex Disk) for command-and-control and uses living-off-the-land techniques such as AppDomainManager injection and AMSI bypasses. Additional tools support credential theft, keylogging, video capture, SOCKS5 tunneling, and in-memory payload delivery. Tool reuse indicators suggest NosyDoor may be shared among multiple Chinese-speaking actors, highlighting an emerging malware-as-a-service–like ecosystem within Chinese espionage operations.

A round-up of targeted attack activities by region

Asia

Check Point Research[5] disclosed a sustained cyber-espionage operation attributed to the Ink Dragon cluster (aka Earth Alux / REF7707 / CL-STA-0049). Active since at least 2023, Ink Dragon primarily targets government and public-sector infrastructure, expanding from Southeast Asia and South America into Europe in recent campaigns. Initial access relies on long-known IIS and SharePoint weaknesses, including ASP.NET ViewState deserialization via exposed machineKey values and the ToolShell exploit chain. A defining feature is the deployment of a ShadowPad IIS Listener module, which converts compromised servers into relay nodes, forming a distributed, victim-based C2 mesh. The group achieves lateral movement and domain dominance through credential harvesting, LSASS dumping, and abuse of RDP and native Windows services. Post-exploitation tooling includes FinalDraft, a modular backdoor abusing the Microsoft Graph API for cloud-native C2 and high-throughput exfiltration. Overall, the activity reflects a highly mature espionage model where compromised victims are repurposed as long-term infrastructure rather than isolated targets.

QiAnXin Threat Intelligence Center disclosed Operation Tornado[6], a sustained cyber-espionage campaign attributed primarily to OceanLotus and related clusters targeting domestic “indigenous innovation” platforms alongside Windows systems. Since 2022, attackers have focused on government networks, aiming to steal sensitive data and assess national policies and development strategies. The campaign relied heavily on mass spear-phishing using diverse lures (desktop/LNK-like files, PDF, JAR, EPUB), exploiting both user execution and N-day vulnerabilities (including an Atril EPUB path traversal flaw). OceanLotus adapted tooling for indigenous platforms, deploying custom ELF malware engineered to run only on these systems while failing on standard Linux. Later phases included internal supply-chain compromise, distributing malicious update scripts to both Windows and indigenous terminals. The malware ecosystem featured layered encryption, shellcode-based Rust payloads, lightweight one-time backdoors, and passive IoT implants for persistence.

CloudSEK[7] identified a sophisticated phishing campaign targeting Indian entities attributed to the Silver Fox APT, correcting prior misattribution to SideWinder. The operation used income-tax–themed PDF lures to deliver an NSIS installer, abusing a legitimate signed Thunder.exe binary for DLL search-order hijacking via a malicious libexpat.dll. The chain progressed through process injection, Donut-generated in-memory shellcode, and culminated in deployment of the Valley RAT. Valley RAT featured registry-resident modular plugins, multi-tier C2 failover (HTTP/HTTPS + raw TCP), delayed beaconing, and on-demand capability loading, enabling long-term stealthy persistence. Attackers leveraged signed binary proxy execution, sandbox evasion, and explorer.exe/tracerpt.exe injection to reduce detection. Overall, the campaign represents a high-risk, espionage-focused intrusion with strong indicators of Chinese-speaking APT tradecraft.

[5] Inside Ink Dragon: Revealing the Relay Network and Inner Workings of a Stealthy Offensive Operation
[6] Operation Tornado: Cyber-Espionage Targeting Domestic Information Innovation Platforms
[7] Silver Fox Targeting India Using Tax Themed Phishing Lures

Qi'anxin Threat Intelligence Center reported StreamSpy[8], a newly identified WebSocket-based backdoor attributed to the South Asia–linked Patchwork (APT-Q-36) group. The malware communicates via a hybrid WebSocket/HTTP C2 model, using WebSocket channels for command delivery and result exfiltration while leveraging HTTP for authentication and file transfer, improving stealth and resilience. StreamSpy collects detailed host identifiers and supports multiple persistence mechanisms, including scheduled tasks, registry RunOnce keys, and Startup shortcuts. The backdoor enables remote command execution, file operations, and encrypted payload delivery through password-protected ZIP archives. Analysis shows strong code, infrastructure, and signing overlaps with Patchwork's Spyder downloader and samples historically attributed to the Donot group, indicating continued toolchain reuse and cross-campaign correlation. Minor updates between StreamSpy versions suggest active development rather than a complete redesign. Overall, the activity reflects ongoing refinement of long-term espionage tooling rather than opportunistic or financially motivated malware.

Middle East

ESET Research disclosed a refined cyberespionage campaign by MuddyWater[9] targeting critical infrastructure and government-linked entities in Israel and Egypt. The operation introduces previously undocumented custom tooling, including the Fooder in-memory loader and MuddyViper, a C/C++ backdoor designed for stealthy persistence, credential theft, and remote control. Fooder uses game-inspired delay logic and reflective loading to evade detection, while MuddyViper supports extensive command execution, data exfiltration, and multiple persistence mechanisms. The campaign also deploys credential and browser data stealers (CE-Notes, LP-Notes, Blub) and go-socks5 reverse tunnels for covert C2 routing. ESET observed reduced hands-on-keyboard activity and increased operational discipline compared to earlier MuddyWater campaigns. Notably, the activity shows operational overlap with the Lyceum (OilRig) subgroup, suggesting cooperation or access-broker behavior. Overall, the campaign reflects a clear maturation in MuddyWater's tooling and tradecraft while retaining a predictable espionage-focused playbook.

SafeBreach Labs published a decade-spanning analysis of Prince[10] of Persia threat actor, revealing continuous, previously unseen activity through December 2025 despite the group appearing dormant since 2022. The research uncovered multiple parallel malware lines (Foudre and Tonnerre) with evolving DGA algorithms, C2 architectures, and tooling, including Tonnerre v50 and Foudre v34. SafeBreach identified a major shift toward Telegram-based C2, with bots and operator accounts used for command delivery and data exfiltration. The group operates numerous testing and production C2 servers, enabling long-term victim management and selective cleanup of low-value infections. Victimology remains centered on Iranian targets and dissidents, with additional victims in Europe, the Middle East, and beyond. Overall, the findings show Prince of Persia as a highly persistent, well-resourced espionage actor that never went dark, but instead refined its infrastructure, OPSEC, and malware ecosystem over time.

FortiGuard Labs reported multiple UDPGangster[11] campaigns attributed to MuddyWater, targeting organizations in Turkey, Israel, and Azerbaijan. UDPGangster is a UDP-based backdoor that enables remote command execution, file exfiltration, and payload delivery while evading traditional network monitoring. The campaigns relied on spear-phishing emails impersonating government entities and delivering macro-enabled Microsoft Word documents as droppers. Once executed, the malware establishes persistence via registry startup keys and communicates with its C2 over UDP port 1269. Samples implement extensive anti-analysis and anti-VM checks, including hardware, memory, process, registry, and sandbox detection routines. Infrastructure and code overlaps link these operations to prior MuddyWater tooling, including Phoenix Backdoor campaigns. Overall, the activity reflects continued use of

[8] Analysis of StreamSpy, a New Trojan Using WebSocket by Patchwork (APT-Q-36)
[9] MuddyWater: Snakes by the riverbank
[10] Prince of Persia: A Decade of Iranian Nation-State APT Campaign Activity under the Microscope
[11] MuddyWater: Snakes by the riverbank

custom espionage malware and social engineering by MuddyWater to maintain regional intelligence collection operations.

Europe

BI.ZONE reported renewed activity by Arcane[12] Werewolf (aka Mythic Likho) targeting Russian manufacturing enterprises in October–November 2025. Initial access was assessed to rely on phishing emails directing victims to spoofed websites impersonating legitimate industrial organizations. The campaigns delivered malicious ZIP archives containing LNK files, which executed PowerShell to retrieve Go-based and C++ droppers disguised as images or documents. These droppers deployed an updated Loki 2.1 loader, compatible with Mythic and Havoc post-exploitation frameworks, while opening PDF decoys to distract users. Loki 2.1 collects host metadata, encrypts and exfiltrates it to attacker-controlled C2 infrastructure hosted on look-alike domains. Unlike earlier versions, Loki 2.1 embeds the implant directly within the loader and executes it in memory. Overall, the activity highlights continuous malware evolution, infrastructure spoofing, and sector-focused targeting by Arcane Werewolf.

Americas

CrowdStrike disclosed a previously unidentified Chinese-speaking intrusion set dubbed WARP[13] PANDA, responsible for long-term, covert intrusions targeting VMware vCenter and ESXi environments at U.S.-based organizations. Active since at least 2022, the group demonstrates advanced operational security (OPSEC) and cloud expertise, with a primary focus on persistent intelligence collection. WARP PANDA deployed a unique malware stack that includes BRICKSTORM[14], a Golang-based backdoor leveraging WebSockets, DNS-over-HTTPS (DoH), and cloud services for stealthy command-and-control (C2). The group also introduced two previously unknown ESXi-focused implants, Junction and GuestConduit, which enable traffic tunneling via VSOCK. Initial access was commonly achieved through the exploitation of internet-facing edge devices and vCenter vulnerabilities, followed by lateral movement using SSH and the highly privileged vpxuser account. The adversary staged and exfiltrated data from live virtual machine snapshots, cloned domain controller VMs, and abused cloud access to harvest Microsoft 365 data. Overall, the activity reflects a highly resourced espionage actor specializing in virtualization- and cloud-centric tradecraft designed to evade detection and maintain long-term, durable access. Notably, Kaspersky GReAT researchers earlier reported activity attributed to the same threat actor in September, in a campaign we dubbed SlackJack[15].

Zscaler ThreatLabz reported a spear-phishing campaign by BlindEagle[16] targeting a Colombian government agency under the Ministry of Commerce, Industry and Tourism in September 2025. The attack abused a compromised internal email account to bypass trust controls and delivered a legal-themed lure containing a clickable SVG attachment. Victims were redirected to a fake judicial web portal, which triggered a fileless execution chain using nested JavaScript and PowerShell. The campaign leveraged steganography to hide payloads in an image hosted on legitimate services, including Internet Archive and Discord. BlindEagle deployed Caminho, a MaaS-style downloader, which injected the final payload via process hollowing. The end payload was DCRAT (AsyncRAT variant) with AMSI bypass, encrypted configuration, and certificate-based C2 authentication. Overall, the activity highlights BlindEagle's shift toward multi-stage, memory-resident tradecraft and continued focus on Colombian government targets.

[12] Arcane Werewolf revamps its arsenal with Loki 2.1 implant
[13] Unveiling WARP PANDA: A New Sophisticated China-Nexus Adversary
[14] Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors
[15] Researcher Notes – SlackJack: A Linux Slack API-Based Backdoor Targeting VMware vCenter SSO Systems
[16] Sharpening the knife:GOLDBLADE's strategic evolution

For more information, please contact: intelreports@kaspersky.com.

C2C9A2B090CD81EF3BD76A0CBE7517F60FB2E530

The monthly brief – summary of Kaspersky's private reports for December 2025

Researcher Notes – Suspected OceanLotus activities in the Middle East and East Asia utilizing new tools

Our recent[17] threat hunting activities led to the discovery of a new malicious backdoor, Rust Backdoor, which appears to be targeting Chinese-speaking organizations and individuals. The backdoor is written in Rust language and is wrapped in multiple layers of loader modules archived in an ISO file. The ISO file contains a decoy document, suggesting that the targets are Chinese-speaking, and is likely used in phishing attacks. Further analysis revealed a new Remote Access Trojan (RAT) tool, written in C++ which shares code similarities with the Rust Backdoor. The CPP RAT has been used in attacks against government entities in Turkey and Egypt, with a focus on Turkish government entities, since early 2025. Furthermore, we found other malicious tools, including Havoc RAT and a lateral movement tool, GoHttpScanner, on the same victim machines. Havoc Rat is deployed through unique loader modules and GoHttpScanner is used in post-exploitation and lateral movement activities. While public reports suggest a connection to the OceanLotus APT group, known for their advanced threat actor capabilities, we were unable to establish a direct link. However, our analysis revealed strong similarities in Tactics, Techniques, and Procedures (TTPs) between the malware used in these attacks and those used against Chinese-speaking victims, indicating a possible connection to the group. In this report, we will provide technical details of the newly found malware families and examine their similarities.

Video game industry continues to be targeted by Winnti malware

The Winnti[18] group (aka Wicked Panda, Wicked Spider, APT41), active since at least 2007, was first named as a group by Kaspersky in 2013. At the time, Winnti was referred to as a Chinese speaking cybercriminal hacking group that conducted focused attacks against the video game industry using Winnti malware (aka HIGHNOON). We discovered that the Winnti group remains interested in the video game industry. The threat actor successfully infiltrated the victim organization's internal network and infected at least three additional internal servers using Winnti malware. Across the compromised servers, we found that the Winnti malware was used to maintain persistence by hijacking the execution flow of the legitimate WinMgmt service, achieved by replacing the wbemcomn.dll file with a malicious version. Upon further analysis of the Winnti malware, we determined that it is a slightly updated version built on the code base of an earlier iteration. The plugins it loads remain consistent with previous versions; however, the main function has been modified, self-updating capabilities have been added, and there are some changes in how commands are processed. Based on our investigation, we assess with medium confidence that the Winnti malware in question is a forked version of its mainstream counterpart, specialized for maintaining persistence. Regarding the code similarities between the modified version of the Winnti backdoor and the Spyder backdoor, we assess with low confidence that the same actor or developer is likely responsible for both.

GriffiThRat updates (Part 2): Post-exploitation activities

GriffiThRat[19] (a.k.a GTRAT) is a sophisticated malware likely used in targeted cyber-mercenary attacks against the FinTech industry. This report (Part 2) details the post-exploitation techniques, tactics, and procedures (TTPs) employed by the threat actors, revealing a focus on stealth and maintaining long-term access. Building on our analysis in Part 1, we observed the threat actors employing a range of techniques to achieve their objectives, and adapting their toolset possibly based on the value of the compromised system or organization. This report details these post-exploitation TTPs, including recent campaign insights, changes in communication channels, and new findings in the attack chain. Intrusion analysis indicates the threat actors performs actions tailored to each victim. After initial compromise, the threat actors select tools and scripts possibly based on the target's value, data, or

[17] Suspected OceanLotus activities in the Middle East and East Asia utilizing new tools
[18] Video game industry continues to be targeted by Winnti malware
[19] GriffiThRat updates (Part 2): Post-exploitation activities

security controls. While the initial GriffiThRat implant is large in size, post-exploitation variants are often smaller but include additional capabilities, such as keylogging and screen capture. In several compromised systems, we also found PureHVNC RAT executed in memory and delivered/installed through obfuscated CloudEye (a.k.a GuLoader) loaders, primarily VBS/PowerShell scripts dropped during post-exploitation. We hypothesize that PureHVNC RAT was deployed in attacks targeting victims with potential value to the threat actors, based on our observations across multiple intrusions. Overall, a key feature of the post-exploitation and action-on-objective activities is the heavy reliance on in-memory execution, which enables the threat actors to remain hidden and maintain prolonged access.

Researcher Notes – SilkLurk: Tailored Backdoor in a Cyber Espionage Campaign in Central Asia

We have discovered a new backdoor, SilkLurk[20], which has been observed in attacks targeting government organizations in Central Asia since January 2025. The backdoor loaders used in the attacks are tailored to each victim and utilize information from the victim's machine to decrypt the backdoor. The loader and backdoor code are heavily obfuscated, making analysis more complicated. SilkLurk is capable of downloading and injecting additional payloads into memory. In post-compromise attacks, threat actors used the command shell to search for and exfiltrate confidential documents. Our investigation revealed that SilkLurk and OctLurk are used by the same threat actor, with some victims infected by the SilkLurk also found to have the OctLurk malware. We attribute both SilkLurk and OctLurk to a Chinese-speaking group, although attribution to a specific group has not yet been confirmed.

Researcher Notes – Starkpity conducts cyber espionage against targets in the Middle East

StarkPity[21] — also known as Marbled Dust, Teal Kurma, CosmicWolf, and Sea Turtle — is a Turkish-speaking advanced persistent threat (APT) group engaged in cyber-espionage operations. Active since at least 2017, the group primarily targets organizations across Europe, the Middle East, and North Africa, focusing on government, telecommunications, and IT sectors. In mid-May 2025, Microsoft Threat Intelligence reported active exploitation of a zero-day vulnerability (CVE-2025-27920) in the Output Messenger platform. StarkPity leveraged this server-side directory traversal flaw to achieve remote code execution and deploy custom malware implants during ongoing espionage operations. Building on Microsoft's findings and our own monitoring, we identified a large-scale campaign in Iraq targeting multiple organizations within government and defense-related sectors. The attackers masqueraded a popular Kurdish keyboard software to distribute malware and perform surveillance activities. Following the infection stage, we observed deployment of a novel malware aimed at PowerBeam devices — wireless bridge hardware commonly used by ISPs, defense entities, and infrastructure operators. This component is designed to hijack communication channels and establish covert access within high-value networks, advancing the group's objectives.

[20] SilkLurk: Tailored Backdoor in a Cyber Espionage Campaign in Central Asia
[21] Starkpity conducts cyber espionage against targets in the Middle East

Indicators of Compromise

This section includes Indicators of Compromise obtained from OSINT sources during the last month. We include them for the sake of completeness for our customers, discarding false positives as we find them. However, we cannot guarantee their reliability and we advise against using them in a production environment and double-checking any potential hit.

Infrastructure

Earth Lamia & Jackpot Panda

```
206.237.3[.]150
45.77.33[.]136
143.198.92[.]82
183.6.80[.]214
```

Maven Centeral Malware

```
fasterxml[.]org
m[.]fasterxml[.]org
103.127.243[.]82
```

LongNosedGoblin

```
www[.]sslvpnserver[.]com
www[.]threadstub[.]com
www[.]blazenewso[.]com
www[.]privacypolicy-my[.]com
118.107.234[.]26
103.159.132[.]30
101.99.88[.]113
118.107.234[.]29
101.99.88[.]188
38.54.17[.]131
```

Silver Fox

```
gov-c[.]club
gov-a[.]club
govk[.]club
dingtalki[.]cn
hhiioo[.]cn
kkyui[.]club
hhimm[.]work
swjc2025bjkb[.]cn
2025swmm[.]cn
hhiioo[.]work
ggwk[.]cc
b[.]yuxuanow[.]top
itdd[.]club
xzghjec[.]com
gov-a[.]work
gov-a[.]fit
gvo-b[.]club
45.207.231[.]94
103.20.195[.]147
```

StreamSpy

```
firebasescloudemail[.]com
mydropboxbackup[.]com
virtualworldsapinner[.]com
adobefileshare[.]com
azureinternalupdates[.]com
scrollzshare[.]info
brityservice[.]info
```

MuddyWater

```
api[.]tikavodot[.]co[.]il
magicallyday[.]com
processplanet[.]org
3.95.7[.]142
35.175.224[.]64
51.16.209[.]105
62.106.66[.]112
157.20.182[.]45
161.35.172[.]55
167.99.224[.]13
194.11.246[.]78
194.11.246[.]101
206.71.149[.]51
212.232.22[.]136
```

UDPGangster

```
157.20.182[.]75
64.7.198[.]12
reminders[.]trahum[.]org
```

Arcane Werewolf

```
cdn[.]electropriborzavod[.]ru
electropriborzavod[.]ru
cloud[.]electropriborzavod[.]ru
```

WARP PANDA

```
208.83.233[.]14
149.28.120[.]31
```

BlindEagle

```
startmenuexperiencehost[.]ydns[.]eu
```