SECURITY ADVISORY

CYBER STASH

December, 2025

CyberStash 2025 Threat Analysis Report

Executive Summary

Over the past year, cyber threat activity has surged in sophistication, blending nation-state espionage tactics with financially motivated cybercrime. Advanced Persistent Threat (APT) groups have expanded their target scope and toolsets, demonstrating agile development and stealth. Campaigns such as those by the Lazarus Group (North Korea) and SideWinder (South Asia) rolled out new malware families and complex infection chains that largely evade traditional defenses.

Meanwhile, cybercriminals are weaponizing fileless malware loaders and info-stealers (e.g. PS1Bot, NonEuclid RAT, StealC v2) to achieve similar stealth and impact. Common threads include heavy abuse of legitimate operating system tools ("living off the land"), in-memory or fileless attack techniques, and exploitation of trusted platforms for Command-and-Control (C2). Attackers increasingly leverage malvertising, cloud services, and "bulletproof" hosting infrastructure to bypass traditional security filters.

This report provides a comprehensive analysis of these trends – mapping adversary tactics to the MITRE ATT&CK framework, highlighting notable campaigns (both APT and criminal), and distilling recurring indicators of compromise (IOCs) and tools. Crucially, we outline enterprise-grade defensive recommendations for each trend, emphasizing proactive threat hunting, attack surface reduction, and resiliency improvements.

Security leaders should take away strategic insights on how threat actors evolved in 2024–2025 and how to bolster defenses against the next wave of attacks.

Included in this Report

- Key Campaigns and Actor Activity
- Notable Criminal Operations
- Malware and Loader Trends
- Techniques and Tactics
- AI, Infrastructure and C2 Abuse Trends
- Recommendations for Enterprise Defense

Threat Landscape Overview

Strategic Shifts in Targeting and Techniques: In 2025, threat actors dramatically broadened their operational scope and refined their methods. State-aligned espionage groups pushed beyond traditional endpoints – embedding malware in virtualization hosts, identity systems, and IT management layers. For example, one campaign codenamed "BRICKSTORM" illustrates how adversaries are moving "beneath the security stack" by persisting in hypervisors and authentication systems that often evade endpoint detection tools. This shift enables long-term, systemic compromise of large networks without triggering standard alarms. At the same time, commodity malware and loaders adopted APT-like stealth. Criminal campaigns increasingly use fileless malware and multi-stage loaders that execute entirely in memory, making forensic detection difficult. Attackers commonly leverage living-off-the-land binaries (LOLBins) – such as PowerShell, mshta.exe, and rundll32.exe – to run payloads, thereby blending malicious actions into legitimate system activity.

Persistent Reliance on Phishing & Social Engineering: Despite advances in security awareness, phishing remained the top initial access vector across both APT and criminal operations. Highly targeted spear-phishing emails with context-specific lures were used by groups like SideWinder and Flax Typhoon to deliver weaponized attachments (e.g. malicious .LNK shortcuts, Office documents). Even well-trained users occasionally fell prey to these convincingly tailored lures – meaning phishing continues to offer attackers a "consistently reliable" entry point into organizations. In a newer twist, malvertising emerged as another potent social engineering avenue: threat actors injected malicious ads into search results for popular software, tricking users into downloading trojanized installers without any email involved. Such campaigns (e.g. the PS1Bot loader in mid-2025) capitalized on users' trust in search engine ads, successfully bypassing email security gateways.

Evasion of "Next-Gen" Defenses: A notable trend was adversaries' ability to evade even advanced Endpoint Detection & Response (EDR) and antivirus solutions. Multiple campaigns deployed in-memory implants, heavily obfuscated scripts, and anti-analysis checks to avoid leaving detectable traces on disk. For instance, the SideWinder APT's custom implant "StealerBot" operates entirely in memory and even terminates itself if forensic or sandbox tools are present. Similarly, the FatalRAT malware uses multi-stage loaders and DLL side-loading to hide its presence, and it rigorously checks for virtual machine or sandbox environments before fully executing. These measures enabled threat actors to prolong dwell time inside networks – often weeks or months of undetected access – despite victims having reputable security products. The clear implication is that technology-centric defenses alone (no matter how "next-gen") are insufficient; only a blend of continuous threat intelligence, behavior-based detection, and periodic compromise assessments can catch these stealthy intrusions.

Convergence of Espionage and Cybercrime Tactics: Another hallmark of 2025's landscape is the blurring line between state-sponsored and criminal operations. North Korea's Lazarus Group, for example, deployed new malware families that serve dual purposes: espionage and financial gain. Their arsenal can steal sensitive military or financial data one day, and facilitate cryptocurrency theft or ransomware deployment the next. Likewise, some criminal tools now exhibit APT-level sophistication – NonEuclid RAT not only exfiltrates data and logs keystrokes, but even has a built-in ransomware module (appending a ".NonEuclid" extension to encrypted files). This convergence means enterprise defenders must be prepared for hybrid threats where actors fluidly shift between spying and monetization. The following sections detail key campaigns and malware that exemplify these trends, followed by an analysis of prevalent tactics and recommendations to counter them.

Key Campaigns and Actor Activity

SideWinder APT – Agile Retooling for Geopolitical Espionage

SideWinder (aka APT-C-17) is a veteran APT group active since 2012 that demonstrated remarkable adaptability in the past year.

Historically focused on South Asian government and military targets, SideWinder expanded its reach to new sectors like maritime logistics and nuclear energy across Asia, the Middle East, and Africa. Recent SideWinder campaigns featured refined spear-phishing with archive attachments containing malicious shortcut (.LNK), INF, and DLL files tailored to victims' thematic interests (e.g. maritime or diplomatic content).

Upon gaining access, SideWinder rapidly retools its malware within hours if a payload is detected, deploying modified variants to avoid signature-based antivirus.

The group's technical sophistication is evident in its complex infection chains and custom implants: a proprietary post-exploitation toolkit called StealerBot runs entirely in memory and is launched via a custom "Backdoor Loader" DLL.

StealerBot harvests sensitive data (screenshots, clipboard, credentials) and communicates with SideWinder's extensive HTTP(S) C2 infrastructure.

SideWinder also abuses legitimate signed software for DLL sideloading – loading malicious DLLs (e.g. propsys.dll, winmm.dll) through trusted applications to evade security alerts. With aggressive anti-analysis features (checking for sandbox processes, unusual libraries, and 137 security tool process names), SideWinder's malware strives to remain hidden from defenders and researchers.

This combination of agile development and stealthy TTPs underscores SideWinder's status as a strategic, well-funded espionage adversary targeting high-value infrastructure.

Lazarus Group – Expanded Malware Arsenal for Espionage and Theft

North Korea's Lazarus Group continued to be one of the most dangerous APT threats in 2025, introducing three new custom malware families: PondRAT, ThemeForestRAT, and RemotePE.

These tools indicate Lazarus's strategic shift toward fileless techniques, faster lateral movement, and long-term persistence inside financial, defense, and critical infrastructure networks.

PondRAT is a fileless modular Trojan that executes almost entirely in memory via reflective DLL injection – typically delivered by malicious Office macros or PowerShell stagers. It maintains stealthy persistence using Run registry keys and scheduled tasks disguised as legitimate updater services. PondRAT's plugin modules (keylogger, browser credential stealer, etc.) emphasize Lazarus's continued focus on credential harvesting and espionage within compromised finance and government systems.

ThemeForestRAT likewise focuses on deception: it hides inside weaponized documents by hollowing out LOLBins like mshta.exe or rundll32.exe for execution. It establishes persistence via innocuous-looking startup shortcuts and features capabilities like screen capture, clipboard monitoring, and even theft of password manager data (e.g. KeePass databases). Its extensive obfuscation (sandbox checks, API call hiding, string encryption) highlights Lazarus's intent to "hide in plain sight" on victim systems.

RemotePE, Lazarus's new lateral movement framework, is an in-memory loader that abuses Windows utilities (e.g. msiexec.exe, notepad.exe) to inject payloads into core processes like svchost.exe. RemotePE was specifically built to propagate across networks using stolen admin credentials (via PsExec/SMB) and to persist as a service on multiple hosts. With these tools, Lazarus can quietly entrench itself in a target for months, gathering intelligence or executing financial heists as needed.

Lazarus operations in 2025 remained heavily focused on financial institutions (for theft and economic intel), defense contractors, and critical infrastructure – aligning with North Korea's dual objectives of revenue generation and strategic espionage. The presence of capabilities like cryptocurrency theft modules alongside LSASS credential-dump routines in the same toolkit illustrates how Lazarus maximizes operational flexibility.

Flax Typhoon (Operation "Cartograph") – Covert Exploitation of GIS Software

Flax Typhoon is a China-aligned espionage actor behind Operation Cartograph, a campaign uncovered in late 2025 that abused trusted geographic information systems (GIS) software for covert access.

The group targeted government and utility organizations (e.g. municipal authorities, transportation, engineering firms) that rely on Esri's ArcGIS platform. Initial access was achieved via spear-phishing emails carrying PowerShell or VBScript loaders embedded in Office docs. These scripts pulled a trojanized "ArcGIS component update" (named geo-component.exe) from attacker servers, which the victims unwittingly installed.

Once inside, the malware blended into normal operations by masquerading as legitimate GIS software: it installed itself as a service and scheduled task under innocuous names, wrote encrypted config data to disk (to survive reboots), and encrypted all outbound C2 traffic to make it look like routine ArcGIS telemetry.

The implant even analyzed local GIS data (maps, topology) to orient itself – using that contextual knowledge to prioritize targets for lateral movement while avoiding noisy scanning that might trigger alarms.

Over its C2 channel (HTTPS with custom encryption), Flax Typhoon could execute remote commands, dump credentials (including LSASS memory, MITRE T1003.001), and exfiltrate internal maps or screenshots.

This campaign underscored the risk of trusted software updates being weaponized: even organizations with well-funded security tools failed to detect an attack that piggybacked on a legitimate platform's traffic patterns.

For defenders, Operation Cartograph was a wake-up call that niche software like GIS can be an attack vector and that continuous validation of update integrity and network baselining is critical.

Silent Lynx – Emerging APT in Central Asia

Silent Lynx surfaced in early 2025 as a new APT group conducting espionage in Central Asia, particularly against government, financial, and policy institutions in Kyrgyzstan, Turkmenistan, and neighboring regions.

The group's operations are highly targeted and methodical. Silent Lynx employs multi-stage infection chains that start with spear-phishing emails carrying ISO file attachments (often inside a RAR archive).

The ISO contains both a decoy document (to trick the user) and a malicious C++ executable loader. When the user opens the decoy PDF, the hidden loader runs and extracts an embedded PowerShell script (Base64-encoded within the C++ binary). Using Windows API calls (CreateProcess with PowerShell -ExecutionPolicy Bypass), the loader executes this PowerShell payload, which in turn drops a Golang-based backdoor implant.

Silent Lynx's Golang implant establishes a reverse shell to the attackers' infrastructure, granting full remote control of the infected system. Notably, the group leverages Telegram bots for C2: the PowerShell stage included a Telegram bot token that allows the malware to send/receive commands via Telegram chats, blending C2 traffic with legitimate messaging services.

Once Silent Lynx gains access, the operators quickly perform internal reconnaissance (running whoami, ipconfig, systeminfo) and then download additional tools or malware onto the host. They establish persistence by adding a new Run key in the registry (e.g., to auto-start a dropped gservice.exe payload) and confirm it's active by querying the registry (receiving a Russian-language success message, suggesting their test environment or targets use Russian OS locales).

Silent Lynx's use of multi-language toolkits (C++, PowerShell, Golang) and cloud-based C2 channels (Telegram) reflects a modern, agile APT approach aimed at long-term espionage.

CyberStash anticipates Silent Lynx will expand operations beyond Central Asia in the near future, given the group's sophistication and broad espionage mandate.

BRICKSTORM – Infrastructure-Level Persistent Access

BRICKSTORM is the codename given to an advanced threat operation identified in 2025 that exemplifies covert, long-term access at the infrastructure level (likely state -sponsored).

Unlike typical endpoint-focused malware, BRICKSTORM targets the "digital arteries" of enterprise and government networks – hypervisors, cloud management consoles, identity providers (Active Directory/AAD), and network appliances. By inhabiting these control-plane layers (often with custom implants or misusing built-in admin tools), BRICKSTORM can silently survey and even manipulate large segments of an environment without detection by standard EDR or SIEM monitoring.

The operators behind BRICKSTORM use this foothold for strategic espionage: quietly harvesting credentials, mapping networks, and preparing for potential future exploits or sabotage – all while avoiding noisy actions like ransomware or defacement. Intriguingly, BRICKSTORM's communications and C2 are highly obfuscated and dynamic. The threat uses multi-layer encryption, proxies, and frequently changes its infrastructure routing, often leveraging professional or "legit" services, which complicates traffic analysis and takedown efforts.

Victim analysis reveals BRICKSTORM is selective: it favors targets whose compromise grants access to many others (e.g. managed service providers, cloud service operators, telecoms, government agencies). By persisting in a single MSP's virtualization cluster or an identity provider, the adversary can indirectly reach dozens of downstream client networks. There is no sign of financially motivated behavior; the targeting is global and driven by strategic intelligence collection needs.

BRICKSTORM represents a paradigm shift in APT tradecraft, proving that well-resourced adversaries are no longer constrained to Windows PCs – they are burrowing into the very infrastructure that enterprises trust and often overlook in monitoring.

Notable Criminal Operations

In parallel to APTs, cybercriminal groups conducted significant campaigns leveraging advanced malware. The threat activities noted below are not exhaustive, but represents the major trends observed.

NonEuclid RAT – Crimeware with APT-Level Evasion

First seen in late 2024, NonEuclid RAT became a prominent tool in 2025 for cybercriminals due to its robust evasion and multi-purpose capabilities.

NonEuclid is sold and promoted openly on platforms like Discord and YouTube, contributing to its rapid adoption by threat actors. It spreads via phishing emails, drive-by downloads, and exploits of unpatched web apps.

Once executed, NonEuclid runs through a sophisticated routine: it delays startup and configures settings, checks for admin rights and kills antivirus processes, bypasses Microsoft's AMSI (Anti-Malware Scan Interface) and User Account Control prompts, then installs itself persistently (often via registry) while ensuring only one instance runs (using mutexes). It also detects virtual environments to avoid sandbox analysis.

The RAT provides backdoor capabilities such as keystroke logging, file theft based on predefined criteria, and even a ransomware module that can encrypt files with AES and append a ".NonEuclid" extension.

This dual ability to act as both espionage tool and ransomware payload makes NonEuclid extremely dangerous. Its rise highlights the trend of readily available malware-as-a-service that can bypass baseline defenses (like Microsoft Defender) unless organizations deploy multi-layered security.

FatalRAT – Multi-Stage Stealth Attacks in Asia

FatalRAT is a sophisticated Remote Access Trojan observed targeting Chinese-speaking users and organizations, with potential to go global.

Likely operated by either a nation-state or advanced cybercriminal group, FatalRAT's infection chain is notably complex. It often starts with phishing or malicious downloads presented as software updates (one case involved a compromised media player installer called PureCodec).

FatalRAT uses DLL side-loading extensively: for example, it drops a benign-looking executable (like a driver installer acvb.exe) along with malicious DLLs that the exe will load (e.g. wke.dll which contains the RAT).

The malware is delivered in stages: an initial loader (Before.dll) contacts a cloud note service (Youdao Note) to retrieve encrypted configuration, including multiple backup URLs for payload download.

A second-stage loader (Fangao.dll) then checks the system locale and environment (time zone, language) to avoid non-target systems or sandboxes. Only if the host matches (e.g. likely Chinese locale) will it decrypt and launch the final FatalRAT payload in memory.

Once active, FatalRAT can log keystrokes, steal data, and even modify OS settings (one observed trick: it disables the ability to lock the workstation, likely to maintain access). Infrastructure clues (use of Chinese cloud hosts and Chinese-language resources) suggest the developers/operators are Chinese-speaking. Cyber intelligence assessments propose FatalRAT may be an evolution of the old Ghost RAT (given overlapping C2 infrastructure) and is perhaps run by a financially motivated non-state actor in the region.

Regardless of origin, FatalRAT's advanced evasion and potential for repurposing mean it poses a threat well beyond its initial locale.

PS1Bot Malvertising Campaign – Fileless Loader for Hire

A major malvertising-driven malware campaign in mid-2025 involved the PS1Bot loader being distributed through tainted online ads.

Cybercriminals purchased ads that appeared in search engine results for popular software and documents, which, when clicked by users, redirected them to fake download pages hosting malicious installers.

The trojanized installer (e.g. an MSI) would display a decoy setup screen while silently launching hidden PowerShell commands (using powershell.exe -EncodedCommand). These commands initiated a multi-stage in-memory attack chain. First, an embedded PowerShell loader script (the "PS1Bot" core) ran and established persistence via registry Run keys and scheduled tasks (ensuring the payload runs at startup).

The loader performed anti-analysis checks for virtual machines or debugging and halted if the environment looked suspicious. It then connected over HTTPS to the attackers' C2 to fetch encrypted secondary payloads (which were decrypted with AES or RC4 on the fly and injected directly into memory).

This loader could deploy a range of malware on-demand – researchers saw infostealers like RedLine and Vidar, RATs such as Remcos, and even full ransomware being loaded by PS1Bot, depending on the operator's intent. Notably, the entire execution remained fileless: final payloads were never written to disk, but executed via reflective DLL injection or chained PowerShell scripts.

The PS1Bot campaign illustrates how criminals are combining LOLBins and modular malware with social engineering (SEO poisoning and malvertising) to infect systems that might not be reachable via email phishing. It also highlights the growing inadequacy of signature-based detection, as PS1Bot's use of PowerShell and memory-only techniques can fly under the radar of traditional AV.

Cross-Family Loader Campaign – PlugX, Bookworm, Turian

In an example of code-sharing across malware "families," one campaign observed in 2025 used related loader techniques to deploy multiple RATs including a PlugX variant, Bookworm RAT, and Turian backdoor.

Delivery was via spear-phishing attachments or trojanized software installers that dropped a malicious DLL next to a legitimate signed EXE (DLL search-order hijacking).

Upon execution, the signed host program would load the rogue DLL, which then read an encrypted payload blob (often stored as a .dat or .afx file on disk or embedded as a resource).

The loader would decrypt this blob through multiple layers – typically XOR then RC4 encryption, followed by LZNT1 compression – to reconstruct the actual malware payload in memory.

Finally, it mapped the payload into a process by allocating memory and using WriteProcessMemory and CreateRemoteThread to execute it, leaving minimal traces on disk beyond the initial DLL and data file.

The threat actors behind this campaign leveraged the loader for different implants:

- PlugX (a long-used Chinese RAT) was observed with custom plugins for keylogging and credential theft, using HTTPS for C2 with domain names that blend in or dynamic DNS.

- Bookworm RAT, another modular malware, used a two-stage approach where a small "leader" DLL from the loader fetched additional modules from C2 at runtime (functionality delivered on-demand). Interestingly, Bookworm employed a novel obfuscation by encoding shellcode as sequences of UUID strings – the malware would decode long strings of UUIDs into binary code, then load that into memory, making static detection very hard.

- Turian, yet another RAT in this campaign, shared a near-identical loader mechanism (DLL sideload + XOR/RC4/LZNT1 decryption) and overlapped code with the PlugX variant, suggesting a common developer or kit being used by multiple groups.

All three payloads had capabilities for remote command execution, file transfer, and credential theft, underlining how threat actors can mix and match components from a shared toolkit to suit their needs.

For defenders, this cross-family campaign reinforces the need to detect behaviors (like unusual DLLs next to legitimate EXEs and in-memory injection patterns) rather than focusing on specific malware signatures.

Malware and Loader Trends

Fileless and In-Memory Malware: One of the clearest trends is the surge in malware that avoids writing to disk. Many campaigns deployed in-memory loaders that use Windows API calls (e.g. VirtualAlloc, WriteProcessMemory, CreateRemoteThread) to inject payloads and execute them directly in RAM. Lazarus Group's PondRAT exemplifies this – delivered by a macro or script, it lives in memory via reflective DLL injection into processes like explorer.exe or svchost.exe, leaving almost no file artefacts. Similarly, the PS1Bot loader runs entirely as an obfuscated PowerShell script, pulling down additional payloads which it decrypts and runs in memory without touching the filesystem. Attack frameworks like RemotePE and the PlugX/Bookworm loaders further demonstrate how core implants are now designed to be fileless: they use staging files (often innocuous-looking .dat, .ini, or .lnk files) and legitimate host processes to conceal the injection of the actual malicious code. This approach confounds traditional antivirus (which scans files on disk) and demands that defenders have capabilities like memory scanning, heuristic detection of injection patterns, and robust EDR telemetry analysis.

Living-off-the-Land (LOLBins) Abuse: Adversaries heavily embraced the tactic of using legitimate system binaries to execute malicious code, both to avoid suspicion and to bypass application control. Many malware strains now come with options to invoke LOLBins. For example, Lazarus's ThemeForestRAT and PondRAT can spawn via `mshta.exe`, `rundll32.exe`, or use `regsvr32.exe` – all signed Windows binaries often allowed by default policies. The PS1Bot campaign similarly used Windows Installer (`msiexec.exe`) to run a malicious MSI and then PowerShell to stage the rest. SideWinder APT was noted to abuse trusted third-party applications for DLL sideloading (placing malicious DLLs such as `UxTheme.dll` alongside a real app). By piggybacking on binaries that are normally present and trusted, malware can execute under the guise of legitimate processes, making it harder for security tools to differentiate good from bad. This trend underscores the importance of baseline monitoring of process behavior (e.g. why is `mshta.exe` launching a PowerShell script?) and the locking down of high-risk LOLBins in enterprise environments.

Multi-Stage Modular Loaders: 2025 threats increasingly rely on multi-stage architectures where a lightweight initial dropper fetches and decrypts the main payload and optional modules. This modular design complicates analysis and detection because functionality is delivered incrementally rather than as a single artifact. FatalRAT, for example, used a four-stage infection chain—an initial loader to establish configuration, a second stage to download and decrypt the RAT, exploitation of a legitimate application (PureCodec) for DLL sideloading, and a final in-memory payload—each stage obfuscated differently to frustrate detection. Bookworm RAT pushed this further by keeping its core "leader" extremely small and pulling capability modules only at runtime from C2 infrastructure, meaning little or nothing is ever written to disk. StealC v2 follows a similar model, acting as both stealer and loader and staging components and exfiltration to avoid noisy transfers. As a result, effective threat hunting must focus on behavioural "shadows" such as abnormal process chains, memory allocation and injection patterns, and suspicious network callbacks, rather than relying solely on static malware signatures.

Malware and Loader Trends

Advanced Evasion Techniques: Attackers deployed increasingly advanced techniques to evade detection at runtime. Many malware families now include virtual machine and sandbox detection logic. For example, FatalRAT's loader checks system language and timezone (likely to ensure it's on a Chinese system, not an analyst's sandbox) before proceeding. PS1Bot's PowerShell will abort if it detects sandbox or forensic artifacts in the environment. NonEuclid RAT specifically bypasses Microsoft AMSI scanning to avoid script-based detection and uses UAC bypass to elevate privileges without user prompts. On the more cutting-edge end, the updated Hijack Loader introduced call-stack spoofing (MITRE T1036) and "Heaven's Gate" technique (64-bit code in 32-bit process) to defeat behavior monitoring and hooking by EDR tools. By forging return addresses and directly invoking syscalls, this loader can perform malicious actions (like injecting Cobalt Strike beacons) while appearing benign to security products that rely on user-mode hooking. All these evasions point to a cat-and-mouse dynamic: as defenders improve detection, malware authors now routinely test their creations against modern EDR and sandboxes, and iterate to remove any "noisy" indicators. The outcome is malware that is quieter, adapts in real-time (as SideWinder does, re-deploying new variants within hours of detection), and slips through gaps in coverage. This elevates the need for out-of-band monitoring (like monitoring memory, telemetry from outside the OS, or anomaly-based detection) beyond what traditional endpoint agents do.

Blending Malware Ecosystems: Another trend is the sharing or reusing of components across different malware families and threat groups, blurring distinct categories. The cross-family loader campaign (PlugX, Bookworm, Turian) is one example, where common loader code and cryptography (RC4, XOR) were seen in multiple malware strains. Lazarus Group's use of commodity tools (like adopting open-source or criminal malware techniques) is another – their "ThemeForestRAT" name itself references a public template resource (likely as a deception), and they even mimic user-agent strings ("ThemeForest" in HTTP headers) to appear legitimate. We also observed info-stealers evolving to have loader capabilities (StealC v2, noted in May 2025, essentially became a platform for both stealing and secondary payload delivery). This mixing of toolsets means analysts can no longer silo "APT malware" vs "crimeware" – there is overlap. Campaigns can involve custom APT malware delivering ransomware, or criminal loaders deploying nation-state spyware. Defense teams must operate under the assumption that any foothold could lead to any outcome, and thus apply comprehensive detection and response processes regardless of the perceived threat actor.

Adversary Techniques and Tactics

The cyber operations of 2024–2025 spanned the full spectrum of ATT&CK tactics. Table 1 below summarizes some of the most frequently observed techniques in the past year's campaigns, mapped to their MITRE tactic categories and example usage:

Technique (MITRE ID)	Tactic	Description & Examples
Spear Phishing Attachment (T1566.001)	Initial Access	Using targeted emails with malicious attachments (Office docs, ISO, ZIP containing LNK, etc.) to infect victims. *Seen in virtually all APT campaigns (SideWinder, Lazarus, Silent Lynx, Flax Typhoon) and many crimeware ops.*
Drive-by Malvertising (T1598.003)	Initial Access	Luring users via malicious online ads or SEO-poisoned search results to download trojanized installers. *Seen in PS1Bot campaign instead of email phishing.*
Command & Scripting Interpreter: PowerShell (T1059.001)	Execution	Using PowerShell for malicious code execution, often with `-EncodedCommand` to obfuscate. *Extensively used in fileless attacks (PS1Bot, PondRAT loaders).*
Signed Binary Proxy Execution (LOLBins) (T1218)	Execution	Abusing trusted binaries to execute payloads (e.g. `mshta.exe` running an HTA for malware, `rundll32.exe` loading a malicious DLL). *Used by Lazarus (mshta/rundll32), Silent Lynx (ISO auto-mount exec), FatalRAT (sideload via DriverAssistant).*
DLL Side-Loading (T1574.002)	Persistence / Execution	Placing malicious DLLs in the search path of a legitimate exe so the exe loads them. *Used by SideWinder, FatalRAT, and the PlugX/Bookworm/Turian loaders for stealthy execution.*
Boot/Logon Autostart (Registry Run Keys) (T1547.001)	Persistence	Creating or modifying Registry Run entries or startup folders to launch malware on login. *Used across many campaigns: Silent Lynx's `gservice.exe` Run key, Lazarus's fake AdobeUpdate service in Run key, NonEuclid's run key for persistence.*
Scheduled Task/Job (T1053)	Persistence	Using scheduled tasks to achieve persistence or delayed execution. *Seen in Lazarus (disguised tasks), Flax Typhoon (tasks masquerading as routine GIS tasks).*
User Execution (Malicious File) (T1204.002)	Execution	Relying on user opening a file to trigger malware (e.g. mounting ISO and clicking a shortcut). *Observed in Silent Lynx (user opens ISO's decoy) and many phishing scenarios.*
Process Injection (T1055)	Defense Evasion / Execution	Injecting malicious code into processes to hide execution. *Nearly every sophisticated malware used this: SideWinder's in-memory StealerBot injects into processes, PS1Bot injects Remcos shellcode into memory, PlugX/Bookworm loaders allocate and write to remote process memory.*
Obfuscated Files or Information (T1027)	Defense Evasion	Heavy use of encryption, packing, or code obfuscation to hide malicious content. *Examples: Virtually all (PS1Bot's Base64 + XOR payloads, ThemeForestRAT's string obfuscation, Bookworm's UUID-encoded shellcode).*
Virtualization/Sandbox Evasion (T1497)	Defense Evasion	Detecting virtual machines, analyst tools, or sandbox artifacts to terminate or alter malware behavior. *Seen in SideWinder (checks RAM size, processes), FatalRAT (checks language/timezone), NonEuclid (detects sandbox), PS1Bot (VM check).*
Credentials from Password Stores (T1555)	Credential Access	Stealing credentials from password managers or browsers. *Observed in Lazarus's ThemeForestRAT (targets KeePass DB) and PondRAT (browser credential dumping).*
OS Credential Dumping (LSASS) (T1003.001)	Credential Access	Dumping memory of LSASS process to obtain Windows credentials. *Used by Flax Typhoon's implant to elevate privileges. Likely in other APT implants as well for lateral movement.*
Lateral Movement via SMB/PsExec (T1021.002)	Lateral Movement	Using stolen admin credentials and SMB (PsExec or similar) to move to other systems. *Used by Lazarus RemotePE for propagation, and common in many post-exploitation toolkits.*
Command and Control over HTTP/HTTPS (T1071.001)	C2	Using web protocols for C2 communications to blend in with normal web traffic. *Very common: SideWinder's HTTP(S) C2, Lazarus's use of HTTPS with fake domains, PlugX using HTTPS to compromised domains, PS1Bot's HTTPS beaconing.*
Encrypted C2 Channel (T1573)	C2	Encrypting command and control traffic on top of TLS (custom encryption or encoding). *Observed in Flax Typhoon (AES-encrypted payload traffic mimicking GIS data), Lazarus (RC4-encrypted payloads over HTTPS), PS1Bot (TLS + RC4 encryption for configs).*
Data Staged/Exfiltrated Over C2 (T1041)	Exfiltration	Sending collected data out via the C2 channel. *Standard practice: SideWinder exfiltrates via custom HTTP(S), Flax Typhoon exfiltrates internal telemetry via its HTTPS channel, NonEuclid and Lazarus do similar with their HTTP/S C2.*
Impact – Data Encrypted for Impact (T1486)	Impact	Encrypting files (ransomware) on victim systems. *Seen in NonEuclid RAT's ransomware feature and as a final stage in some PS1Bot deployments (ransomware dropped on selected targets).*

Table 1: Prevalent ATT&CK Techniques in 2025 Threat Campaigns

Key Observations

Initial access was dominated by social engineering (phishing, malvertising), while execution and persistence heavily leaned on abusing legitimate tools (scripting engines and signed binaries) and in-memory techniques to avoid detection.

Defense Evasion techniques like obfuscation and sandbox checks were near-universal. Once inside, threat actors prioritized credential access (to facilitate lateral movement or financial theft) and stealthy C2 communications.

These techniques underscore that many adversaries are successfully exploiting gaps in standard defenses – for example, endpoint solutions that might not inspect process memory or encrypted traffic.

Mapping these behaviors to ATT&CK helps organizations ensure their detection coverage aligns with the tactics currently favoured by attackers.

Notable Trends

Infrastructure and C2 Abuse Trends

Abuse of Trusted Cloud Services & Platforms: Attackers continued to exploit popular legitimate services to host malware and conduct C2 in order to blend with normal traffic. A notable example is the abuse of GitHub for C2: the SHELBY malware discovered in 2025 uses GitHub repositories as dead-drop locations for commands, essentially hiding its communication in what appears to be normal GitHub API traffic. This tactic makes detection challenging, since many enterprises allow GitHub and similar services through their firewalls. We also saw malware using cloud storage and note-taking services: FatalRAT retrieved config and payloads from Youdao Cloud Notes, a legitimate Chinese cloud note service, and SideWinder's phishing sometimes leveraged known cloud file services to host payloads (as indicated by their use of trusted domains to reduce suspicion). These trends illustrate that legitimate platforms can be turned into covert channels. Attackers are leveraging everything from code repositories to messaging apps (e.g., Silent Lynx's use of Telegram bots for C2) to hide their communications in plain sight.

Bulletproof Hosting & Dedicated Infrastructure: Many threat actors rely on so-called bulletproof hosting (BPH) providers – hosting services that knowingly or negligently cater to cybercriminal clientele and are resilient against takedowns. Across multiple campaigns, we see C2 servers and malware delivery sites hosted in a small set of autonomous systems (ASNs) and top-level domains that are notorious for abuse. For instance, Lazarus Group registered numerous domains on uncommon TLDs like .live, .co, .net that were likely obtained through bulletproof hosts. Security analysis showed Lazarus domains such as calendly[.]live and azuredeploypackages[.]net – which mimic legitimate services – were part of their rotating infrastructure. Similarly, commodity malware like RedLine stealer and PS1Bot often utilize bulletproof hosting in regions with lax cyber law enforcement. A CyberStash study highlighted that for many organizations, 5–10 ASNs and a handful of TLDs account for 70–95% of malicious traffic targeting them. This indicates that adversaries repeatedly abuse the same infrastructure zones. Attackers also use Dynamic DNS and ever-changing domain generation to make their C2 more resilient. The PlugX/Bookworm campaign, for example, used dynamic DNS domains and compromised websites as C2 to evade static blocking. The persistence of bulletproof hosting calls for a more aggressive defense strategy (discussed in the Recommendations) to proactively cut off entire hostile network blocks rather than whack-a-mole on individual IPs.

Use of Social Media and Mesh for Distribution/Exfiltration: Apart from Telegram (used by Silent Lynx), there's growing abuse of platforms like Discord for malware distribution and data exfiltration. While not detailed in the above campaigns, CyberStash notes that some info-stealers and RATs use Discord webhooks to exfiltrate stolen credentials (because Discord's traffic is often allowed and not seen as suspicious). In our dataset, NonEuclid RAT was openly marketed on Discord channels, demonstrating how threat actors exploit social platforms both for their operations and for community building. Additionally, peer-to-peer or mesh networking tools have started to appear for C2 in sophisticated malware (though not prominent in this year's reports, we anticipate more threats employing decentralized C2 to resist takedown).

Trends in C2 Communication: Encrypted web traffic (HTTPS with custom encryption layers) is now the norm for C2. Many APTs used port 443 and domain fronting or mimicry to hide C2. For example, Flax Typhoon's malware encrypted its C2 payloads to look like normal ArcGIS map data over HTTPS. Lazarus infrastructure included domains referencing cloud or tech terms (e.g., azureglobalaccelerator[.]com) to appear legitimate in logs. Some malware also employed low-frequency beaconing and jitter to avoid pattern-based detection – e.g., sending beacons at irregular intervals or with randomized payload sizes, which Flax Typhoon and RemotePE both did. Finally, when traditional ports were used, malware often leveraged non-standard ports or legitimate-looking protocols. A few campaigns (like FatalRAT's predecessors linked to Ghost RAT) even used custom TCP protocols or uncommon ports to blend in with weird but allowed traffic. The bottom line is that attacker infrastructure is increasingly agile, distributed, and intermingled with legitimate internet services. Defenders must monitor outbound connections closely – e.g., egress filtering that flags connections to unexpected countries, ASN ranges, or new domains – and leverage threat intelligence to identify abuse of popular platforms (like sudden spikes of GitHub or Discord traffic from a server that doesn't normally use it). anticipate more threats employing decentralized C2 to resist takedown).

Trends in Operational Use of AI by Adversaries

Adversaries in 2024–2025 moved beyond theoretical AI experiments to actively leveraging artificial intelligence in their cyber operations. Advanced persistent threat (APT) groups and cybercriminals are incorporating generative AI tools to boost the scale, sophistication, and success rate of attacks. Unlike early speculative discussions, recent campaigns show AI being used in practical, observable ways that materially enhance adversary tradecraft.

AI-Enhanced Social Engineering and Phishing

Threat actors are using large language models (LLMs) to craft highly convincing phishing lures and social engineering content at scale. Generative AI enables grammatically perfect, tailored emails with context that resonates with the target, reducing the tell-tale signs of fraud. For example, Iran's APT42 was observed using an AI assistant to generate spear-phishing materials themed for a US defense organization, even translating and localizing content for specific audiences. Criminal groups likewise exploit generative text to remove errors and personalize scams – the FBI warned that AI-written messages have made social engineering and fraud "more believable," allowing criminals to reach wider audiences with less effort. This AI-driven polish has led to higher click-through and response rates, pressuring enterprises to strengthen phishing detection and user skepticism.

Synthetic Identities and Deepfakes: 2024 saw threat actors operationalize generative AI for creating fake personas and media that bypass human trust filters. Synthetic profile photos and fictitious identities generated by AI have been used in espionage and fraud campaigns. Google's threat team noted North Korean groups fabricating profile pictures and content for fake social media personas via AI, bolstering their credibility in phishing and reconnaissance efforts. Even more striking, criminals have employed deepfake audio/video to impersonate trusted individuals in real time. In one early-2024 case, scammers used an AI-generated video call to convincingly mimic a company's executives – tricking an employee into transferring $25 million to the attackers. Similar deepfake "voice clone" scams targeted financial departments with urgent requests that sounded eerily authentic. These incidents underscore how AI can weaponize trust, forcing enterprises to implement strict verification (e.g. secondary offline confirmation) for any high-stakes requests, even those appearing to come from senior personnel.

Malware Automation and AI-augmented Attack Tools: Beyond social engineering, adversaries have begun embedding AI directly into malware and operational tools. 2025 witnessed the first malware families with in-execution AI capabilities. Notably, experimental strains like PROMPTFLUX use an LLM at runtime to rewrite their own code and generate new malicious scripts on the fly, enabling "just-in-time" adaptation to evade detection. This development – malware autonomously improving itself using AI – marks a significant step toward more autonomous and resilient attacks. Similarly, other samples (e.g. PROMPTSTEAL) have leveraged AI APIs to dynamically generate system reconnaissance commands. On the cybercrime side, the underground marketplace is now offering illicit AI tools explicitly for offenders. By late 2025, multiple "jailbroken" LLM-based services (such as community-named "WormGPT" or "FraudGPT") were being advertised, providing unfiltered assistance with writing malware, finding exploits, or crafting phishing content. This lowers the barrier for less-skilled actors to execute advanced tactics. State-sponsored operators are also augmenting their full attack lifecycle with AI – from using AI agents to summarize reconnaissance data to generating customized command-and-control code and automating data exfiltration workflows. Overall, AI is acting as a force-multiplier for threat actors, increasing the speed and scale of campaigns without a corresponding increase in attacker labor.

Strategic Implications: The operational use of AI by adversaries creates a moving target for defenders. Detection becomes more challenging as phishing emails and social media bait no longer exhibit the grammar mistakes or awkward phrasing that users might spot. Security awareness programs must evolve to teach employees that even impeccably written messages or lifelike voices can be faked. Technical defenses should incorporate AI as well – for example, using AI-driven anomaly detection that might pick up on subtle indicators of AI-generated content or on-the-fly malware code changes. Governance is key: organizations should establish guidelines on acceptable AI usage (to prevent inadvertent exposure of data to public AI services) and invest in controls to detect synthetic media. From a policy perspective, identity verification processes need bolstering (e.g. callback verification for financial transactions, multi-factor authentication that can't be bypassed by a deepfaked voice). In summary, enterprises should assume that any content – text, image, or voice – could be artificially generated, and build layered controls to counter the "at scale" social engineering and adaptive malware that AI enables.

Recommendations for Enterprise Defense

To counter the above trends, organizations should adopt a layered and proactive defense strategy that addresses both technical gaps and process gaps. Below are key recommendations aligned to the observed threat trends:

1. **Harden Email and Web Gateways:** Since phishing remains rampant, deploy advanced email filtering to quarantine or block suspicious attachments (e.g. block incoming emails containing .RAR, .ISO, or shortcut files unless absolutely necessary). Incorporate attachment sandboxing with file detonation to catch malicious macros or scripts. Equally important, implement web filtering and DNS security solutions to tackle malvertising and SEO poisoning – block known malicious domains and categories (such as newly registered domains, or those with no business relevance). Use DNS sinkholing for domains that threat intel flags as C2, and consider browser isolation for high-risk web content to mitigate drive-by downloads.

2. **Restrict and Monitor LOLBins:** Enforce policies to limit the abuse of living-off-the-land binaries. For critical servers and high-risk endpoints, disable or constrain unneeded interpreters and scripting engines. For instance, enable PowerShell Constrained Language Mode and robust logging (module logging, script block logging) so that any PowerShell usage is auditable. Use application control (AppLocker or similar) to block execution of MSHTA, WScript, or other rarely-used binaries from user directories. If those tools must be allowed, tightly monitor their usage: e.g., generate alerts if mshta.exe or rundll32.exe spawns a PowerShell or makes network connections. Several APTs specifically abused these, so cutting off that avenue disrupts many fileless techniques.

3. **Strengthen Endpoint Defenses with Behavior Detection:** Traditional AV signatures are no match for the in-memory, obfuscated attacks we've seen. Ensure your Endpoint Detection & Response (EDR) or XDR is configured to detect behavioural indicators such as: processes injecting code into others, unusual API call patterns (e.g., a process calling VirtualAlloc > WriteProcessMemory > CreateRemoteThread sequence), and suspicious parent-child process relationships (like an Office document spawning a command prompt or script engine). Tune EDR to flag rapid sequence of process spawns that match known chains (e.g., winword.exe -> powershell.exe -> svchost.exe as seen in fileless attacks). Deploy memory protection features if available (some EDRs can detect reflective injection or common shellcode patterns). Additionally, monitor for anti-VM and API anomaly signals – e.g., if a process loads the ntdll.dll and starts making direct syscalls or uses rarely used syscalls, that could indicate evasion like Heaven's Gate or direct syscalls. Behavioral analytics that focus on these low-level tricks can catch advanced loaders such as Hijack Loader.

4. **Proactive Threat Hunting and Compromise Assessments:** Given that some adversaries can bypass preventative controls entirely, it's essential to assume breach and hunt for signs of intrusion regularly. Conduct periodic compromise assessments focusing on the tactics described: search for the presence of known IoCs, but also for behaviors like new services or tasks with strange names, unexpected files in system directories, or network connections to odd domains. Use threat hunting queries to look for persistent techniques – e.g., any new DLL dropped in directories of legitimate programs (to spot DLL side-loading), any registry Run key pointing to unusual executables or PowerShell commands, any scheduled task that was created by a non-admin user, etc. Employ independent breach detection tools or services to augment your internal monitoring. These can catch what standard tools miss. The goal is to identify stealthy threats before they accomplish their objectives – for example, discovering a hidden Backdoor in a virtualization host (as with BRICKSTORM) by analyzing hypervisor logs and configurations for anomalies.

5. **Secure the Core (Tier-0) Infrastructure:** In light of threats like BRICKSTORM, treat your core infrastructure (identity systems, virtualization platforms, backup servers, network appliances) as high-value assets that need extra hardening and visibility. Apply the concept of Zero Trust at the control plane: no implicit trust for administrative networks. Implement strong access controls (MFA, just-in-time admin access) for hypervisors, directory services, and cloud management portals. Regularly audit these systems for backdoors or unknown users. Deploy specialized logging or monitoring for them since EDR may not cover these platforms – for example, ensure your SIEM or a separate system ingests hypervisor logs, Azure AD audit logs, etc. Consider network segmentation that isolates management interfaces (so that even if an endpoint is compromised, it's hard for the attacker to jump into hypervisor or domain controller networks). Also, restrict outbound internet access from Tier-0 systems – e.g., your hypervisors and domain controllers should not normally initiate outbound connections, so block them by default. This will "break" many covert channels if an attacker does get in there.

6. **Attack Surface Reduction – Block High-Risk Infrastructure:** Leverage threat intelligence to proactively block traffic to known malicious infrastructure. As detailed in CyberStash's bulletproof hosting advisory, organizations can significantly reduce exposure by filtering network egress to certain ASNs, countries, and TLDs that have no legitimate business purpose. For example, if you observe no legitimate need to communicate with domains in *.xyz or *.top TLD, or with IP ranges of certain bulletproof hosts, consider blocking those entirely at your firewall or secure web gateway. Implement an ASN-based block list for notorious ISPs that harbor threat actor servers. Likewise, geoblock regions that your company doesn't do business in but are sources of constant attacks. These steps can preemptively neutralize threats – cutting off malware delivery, C2 call-backs, and phishing pages hosted on those infrastructures. Regularly tune these policies with threat intel updates (many security providers and national CERTs publish lists of bulletproof host networks). Reports show that such measures can reduce hostile traffic by 70–95% within weeks, drastically shrinking the window for attackers to operate.

7. **Persistence Management – Hunt for Odd Persistence Mechanisms:** Many threats achieved stealthy persistence by blending in with normal startup items (e.g. naming a malicious service AdobeUpdateService or using hidden registry keys). Security teams should conduct periodic baseline checks of all autoruns: services, startup tasks, run keys, scheduled tasks. Use automated scripts to compare current entries to a known-good baseline or a whitelist of approved entries. Anything new or unusual (like a service pointing to C:\Windows\Temp*.exe as found with RemotePE) should be investigated immediately. Employ "drift detection" – if a new task or service appears on a critical server unexpectedly, generate an alert. In incident response, have rapid memory capture and analysis playbooks ready so that when a suspected persistence mechanism is found, you can dump process memory to see if it's harboring an in-memory implant. This reduces containment time and helps ensure the threat is fully eradicated (fileless malware often requires dumping memory for IOC extraction).

8. **Network Anomaly Detection and Egress Monitoring:** Given the stealthy C2 techniques, investing in network detection is key. Use your network security monitoring tools to look for anomalous outbound connections – e.g., a client that never talked to an IP in Country X suddenly does so, or systems making DNS queries for domains with patterns matching DGA or recently registered domains. Monitor for encrypted DNS (DoH) or VPN-like traffic that might indicate tunneling. Also set up decoy "honeypot" credentials and services internally to catch lateral movement (for example, a fake admin credential stored in an endpoint's memory – if an attacker dumps it and tries to use it, you'll detect that attempt). In addition, deploy TLS inspection or SSL logging on outbound traffic where privacy rules permit, focusing on uncommon destinations (this could catch something like Flax Typhoon's ArcGIS-lookalike traffic if the domain or certificate doesn't match the real ArcGIS servers). While encryption makes content inspection harder, even analyzing connection metadata (JA3/SHA fingerprints, packet sizes, timing) can reveal automated C2 vs normal browsing.

9. **Incident Response Readiness and Intelligence Integration:** Finally, ensure that your incident response plan is updated to handle these advanced threats. This means having procedures to deal with fileless malware (e.g., gathering Volatile data, memory forensics), isolating entire segments of the network if something like BRICKSTORM is suspected (since just wiping a PC won't help if a hypervisor is backdoored), and involving your threat intelligence team to continuously feed new IOCs and context into your detection stack. Integrate threat intel subscriptions that include indicators for the kinds of campaigns discussed. Make sure your security tools ingest these and alert if seen. And importantly, test your defenses regularly – run simulated attacks (red team exercises or breach-and-attack simulations) that mimic fileless malware, phishing, and lateral movement to ensure your people and tools can detect and respond to the techniques highlighted in this report.

10. **Rigorous Patching and Third-Party Software Security:** Some campaigns exploited known vulnerabilities (e.g., SideWinder was noted using an old Office exploit CVE-2017-11882 and even a 2025 vulnerability), which underscores the need for timely patching of software, especially client-side apps like browsers and Office. Keep these updated to reduce exploit-driven attacks. Equally crucial is scrutinizing third-party software supply chain: Operation Flax Typhoon taught that even legitimate software updates (ArcGIS in that case) can be subverted. So, verify checksums or signatures of critical software updates, restrict where servers can download updates from (e.g. only allow connections to official vendor update sites), and consider hosting internal update mirrors so you can audit the files. For highly sensitive environments, treat new software or updates with a sandbox detonation before wide deployment.

By implementing the above measures, enterprises can significantly improve their resilience against the evolving threat landscape of 2025. The emphasis is on early detection and deterrence: cutting off attacker infrastructure, catching their stealth techniques via behavior, and not relying on any single security control. Threat actors may be raising their game, but a well-prepared and adaptive defense can thwart even these advanced attacks or at least limit the damage they cause.

Closing Perspective

The 2024–2025 threat landscape demonstrates a clear and sustained shift in adversary behaviour. Modern cyber operations prioritise stealth, persistence, and abuse of trust over speed or disruption. Successful intrusions increasingly rely not on novel exploits, but on exploiting architectural blind spots, implicit trust, and gaps in visibility.

For boards, cyber risk is no longer defined solely by the likelihood of a breach, but by the risk of undetected, long-term access to systems that underpin business operations and decision-making. In this environment, the absence of alerts does not equate to the absence of threat.

Organisations best positioned to manage this risk are those that move beyond reactive detection toward assurance and resilience—validating that controls operate as intended, challenging assumptions, and recognising that compromise is a scenario to be governed, not denied.

The purpose of this report is to support informed oversight and disciplined decision-making. Boards that consistently ask where trust is placed, how it is verified, and what remains unseen will be best placed to ensure their organisations remain resilient in a threat landscape designed to reward silence.

References

- CyberStash Advisory – *SideWinder APT: Agile Retool and Evolving Tactics* (April 2025).
- CyberStash Advisory – *FatalRAT: A Stealthy and Dangerous RAT* (Feb 2025).
- CyberStash Advisory – *Silent Lynx: An Emerging APT Group* (Feb 2025).
- CyberStash Threat Brief – *NonEuclid RAT* (Jan 2025).
- CyberStash Analysis – *BRICKSTORM: Beneath the Security Stack* (Mid 2025).
- CyberStash Whitepaper – *Reducing Exposure to Bulletproof Hosting* (2025).
- CyberStash Advisory – *Lazarus Group Expands Malware Arsenal with New RAT Families* (Sept 2025).
- CyberStash Advisory – *Operation Cartograph: Flax Typhoon's ArcGIS Exploitation Campaign* (Oct 2025).
- CyberStash Advisory – *Cross-Family Loader Campaign: PlugX, Turian, Bookworm* (2025).
- CyberStash Advisory – *Malvertising-Driven PS1Bot Loader Executes In-Memory Attack Chains* (Aug 2025).
- CyberStash Threat Alert – *Hijack Loader and SHELBY Campaigns: Evasive Malware Trends* (Apr 2025).
- CyberStash Threat Bulletin – *Silent, Modular, Dangerous: The Rise of StealC v2* (May 2025)