Daily Intelligence Update | 6 November 2025

Researchers report that North Korea–aligned APT groups Kimsuky and Lazarus continued targeted espionage operations, deploying new variants of HttpTroy, Comebacker, and BLINDINGCAN across multiple regions. In the latest activity, Kimsuky distributed a VPN-themed phishing lure that delivered a multi-stage chain involving a dropper, the MemLoad_V3 loader, and a revamped HttpTroy backdoor capable of file manipulation, screenshot capture, remote shell access, and encrypted C2 over HTTP. In parallel, Lazarus targeted Canadian entities through a new Comebacker variation leading to an upgraded BLINDINGCAN RAT, which employs layered encryption using HC256, RC4, and AES-128-CBC, dynamic API resolution, and persistence via stealthy Windows services. Analysts note that both clusters relied heavily on obfuscation, memory-resident payloads, and modular loaders designed to reduce forensic visibility and evade behavior-based detections.

Meanwhile, researchers have uncovered a supply-chain attack linked to the Stargazers Ghost Network, which used Ethereum smart contracts as hidden C2 infrastructure to distribute downloader malware through malicious npm packages. Two packages uploaded in July 2025, colortoolsv2 and mimelib2, were found to fetch second-stage payloads from attacker servers, with URLs stored inside Ethereum smart contracts in a technique reminiscent of EtherHiding. The threat actor also created fraudulent GitHub repositories mimicking cryptocurrency trading bots such as solana-trading-bot-v2 and arbitrage-bot to increase legitimacy and lure cryptocurrency developers into integrating the compromised libraries. Analysts assess that the campaign likely targeted crypto-focused developers and users through social engineering and dependency hijacking.

Elsewhere, researchers identified a new FileFix-style social engineering campaign that impersonates a Fortinet VPN Compliance Checker and abuses a cache-smuggling technique to bypass endpoint security. Victims are instructed to paste a seemingly harmless network path into File Explorer, which silently executes hidden PowerShell commands that extract Chrome cache files, decode an embedded ZIP hidden inside an image file, and execute a malicious payload without direct file download. Analysts note that the campaign reflects a significant evolution of FileFix tactics, relying on obfuscation, covert execution, and filesystem deception to evade inspection. Additional findings include a newly observed “IUAM ClickFix Generator” kit that automates phishing-page creation mimicking Cloudflare, Microsoft, and Speedtest, distributing infostealers such as DeerStealer and Odyssey.

In ransomware activity, researchers say the BlackLock group—rebranded from El Dorado in late 2024—has expanded its cross-platform targeting with a Go-based ransomware family developed for Windows, Linux, and VMware ESXi environments. Operating under a RaaS model advertised on Russian-speaking forums, BlackLock has impacted government, consulting, education, transportation, and manufacturing organizations across the U.S., South Korea, Japan, and beyond. The malware supports configurable command-line parameters for encryption scope, scanning, and execution timing, and uses ChaCha20 for file encryption with per-file keys secured through Elliptic Curve Diffie-Hellman (ECDH). The ransomware deletes Volume Shadow Copies and uses in-memory shellcode to obstruct recovery before dropping ransom notes titled HOW_RETURN_YOUR_DATA[.]TXT demanding payment under threat of leaks and service disruption.

Finally, researchers have confirmed active exploitation of a zero-day vulnerability in Gladinet’s CentreStack and Triofox platforms (CVE-2025-11371), which allows unauthenticated Local File Inclusion and retrieval of sensitive system files, including machine keys. Attackers have combined the flaw with an older deserialization issue (CVE-2025-30406) to achieve remote code execution via ViewState manipulation, affecting at least three organizations to date. The vulnerability arises from a misconfigured temp handler in the UploadDownloadProxy component, enabling hostile access to critical configuration data. Gladinet has acknowledged the issue, directing customers to disable the temp handler pending an official fix, noting that the mitigation may impair certain platform functions but effectively blocks exploitation.

Critical Start is a leading provider of Managed Detection and Response (MDR) services, combining AI acceleration with expert human validation to eliminate false positives, reduce alert noise, and deliver fast, reliable threat resolution.

With a US-based, 24/7/365 Security Operations Center and a 90% analyst retention rate, Critical Start delivers both proactive and reactive MDR for large enterprises across North America. Its MDR is built to detect threats early and respond quickly, with every action backed by contractual service-level agreements that ensure trusted outcomes for security teams. For more information, visit www.criticalstart.com.