Daily Intelligence Update | 12 October 2025

Researchers have identified a multi-stage malware campaign abusing malicious Windows LNK files to deliver the REMCOS backdoor through fileless execution. The attack begins with phishing emails or deceptive downloads containing LNK files disguised as documents, which, once clicked, silently launch PowerShell to fetch a Base64-encoded file from a remote URL, decode it into a PIF executable, and execute it, bypassing conventional defenses. REMCOS, a C++ backdoor, enables full remote shell access, keylogging, webcam and microphone capture, and persistent surveillance. The campaign relies on trusted Windows tools to evade detection and is flagged as Trojan.WinLNK.Powershell_S03. Security researchers recommend users avoid opening unknown shortcut files, monitor ProgramData for unusual artifacts, and ensure AV signatures remain current.

In parallel, law enforcement agencies including the U.S. DOJ, FBI, and France's BL2C—with backing from the Paris Prosecutor's Office—have seized the BreachForums clearnet domain (breachforums[.]hn), a site tied to ShinyHunters and the rebranded Scattered LAPSUS$ Hunters, disrupting one of the most active leak and extortion platforms. Visitors to the seized site now see an official takedown banner, although the group's onion service remains live. The forum had been central to distributing Salesforce-derived breach data, with victims including Qantas, Disney, McDonald's, UPS, and others. Despite initially threatening mass disclosures, operators released data from only six organizations on October 11, then abruptly claimed no further leaks would follow, posting and deleting a message suggesting "limitations" before signaling plans to shut down their Telegram channel. Internal friction within the group was evident, with missed timed releases, disputes, and ad hoc hosting on BreachStars and limewire-linked distribution mirrors. As of October 12, no additional datasets have surfaced beyond the six previously disclosed, and a Red Hat sample once available on the clearweb has since been removed, though TOR mirrors remain unchanged. The group continues to threaten Cl0p, solicit insiders within major Australian firms, and claim upcoming plans against CrowdStrike, reflecting instability but also ongoing ambition.

Meanwhile, Cisco has patched three critical zero-day vulnerabilities in the VPN web server component of its Secure Firewall ASA and FTD software, tracked as CVE-2025-20333, CVE-2025-20362, and CVE-2025-20363. These flaws, exploited in the wild since May 2025, have been attributed to China-linked threat group UAT4356 (Storm-1849), which has been targeting legacy ASA 5500-X appliances running older versions without secure boot protections. The vulnerabilities include a path-normalization issue and heap buffer overflow that allow attackers to bypass session validation, achieve information disclosure, and execute remote code. Exploitation has been used to deploy custom malware such as the RayInitiator bootkit and LINE VIPER payload to gain persistence, disable logging, and intercept administrative commands. In response, CISA issued Emergency Directive ED 25-03 instructing organizations to patch immediately, conduct forensic hunts, isolate compromised devices, and reset configurations. Cisco has recommended full rebuilds post-upgrade and stressed the importance of retiring unsupported devices. The campaign appears focused on long-term espionage and data theft from perimeter devices rather than internal lateral movement, reinforcing the need for organizations to minimize VPN exposure and accelerate adoption of zero trust architectures.
