Daily Intelligence Update | 26 September 2025

Researchers have identified a stealthy and evolving espionage campaign attributed to the Iran-linked APT group *Nimbus Manticore*, which has been active since early 2025 and is increasingly focused on Western Europe, particularly Denmark, Sweden, and Portugal. The operation relies on tailored spear phishing lures and fake recruiting portals that deliver malicious archives, which in turn use a novel multi-stage DLL sideloading technique via low-level NT APIs. Once deployed, the campaign drops the heavily obfuscated *MiniJunk* backdoor and *MiniBrowse* stealer, the latter designed to extract Chrome and Edge credentials. To maintain persistence and evade tracking, the actors employ Cloudflare and Azure App Service for rotating command-and-control infrastructure, sign and inflate binaries to evade detection, and leverage redundancy mechanisms. Analysts also note a related but simpler cluster, dxgi[.]dll, that shares code and infrastructure overlap. Activity from Nimbus Manticore has been linked to UNC1549, Smoke Sandstorm, and the so-called “Dream Job” campaigns, reinforcing the group’s established focus on covert and adaptive operations.

In parallel, researchers uncovered a China-nexus espionage campaign attributed to UNC6384, which specifically targets diplomats in Southeast Asia and other global entities. The campaign hijacks browser captive portal checks to redirect users to fake plugin update pages, delivering a digitally signed dropper known as *STATICPLUGIN* that leads to in-memory deployment of the *SOGU[.]SEC* backdoor. The actor’s tradecraft includes adversary-in-the-middle attacks, valid TLS certificates, DLL sideloading, and indirect execution through Windows message queues to evade endpoint detection. Analysts further tied activity to Chengdu Nuoxin Times Technology Co., Ltd. code signing certificates, with overlaps noted to Mustang Panda (TEMP.Hex).

On the ransomware front, researchers reported the emergence of *LockBit 5.0*, a major evolution of one of the most prolific ransomware families. This version targets Windows, Linux, and VMware ESXi with enhanced obfuscation, anti-analysis features, and streamlined cross-platform execution. The Windows variant reportedly uses DLL reflection to load payloads while disabling security services, whereas the Linux version mirrors its capabilities with directory and file targeting options. A dedicated ESXi variant is particularly destructive, encrypting entire VM infrastructures in single attacks. LockBit 5.0 introduces randomized 16-character file extensions, clears event logs, and incorporates geolocation checks to avoid Russian-language systems. Although much of its foundation stems from LockBit 4.0, the speed, evasion, and refinements suggest an ongoing maturation of the franchise. Victims are directed to the group’s redesigned leak sites, which maintain familiar ransom negotiation mechanisms.

Meanwhile, a Chinese-speaking actor has been linked to a PlugX campaign active since 2022, targeting telecommunications and manufacturing firms across Central and South Asia. The variant observed mirrors RainyDay configurations and shares unique XOR RC4 decryption routines and identical RC4 keys with Turian backdoors. These overlaps, combined with DLL sideloading, loader-based shellcode injection, and consistent key reuse, suggest either unification of Naikon and BackdoorDiplomacy or a shared vendor supplying tools across multiple groups. Analysts place medium confidence on attribution to a Chinese-speaking actor due to code heritage and targeting patterns.

Ransomware monitoring also surfaced a new leak site, *Arachna Leak*, which currently lists two victims—Clínica Armstrong Internacional and KiranaKart Technologies. The site is minimal, consisting solely of a

single page displaying the victims' data for download without any "About" page, contact details, or apparent negotiation infrastructure.

Finally, researchers issued warnings regarding a newly discovered critical remote code execution vulnerability in *WatchGuard Firebox* firewalls, now tracked as CVE-2025-9242. The flaw, stemming from an out-of-bounds write in the iked VPN process, affects Fireware OS versions 11.x, 12.x, and 2025.1, and allows unauthenticated remote attackers to execute arbitrary code if IKEv2 VPN features are enabled. While removal of vulnerable configurations reduces exposure, devices may still be at risk if Branch Office VPNs to static peers remain active. Impacted hardware includes the T15, T20–T85, M270–M5800, Firebox Cloud, Firebox NV5, and FireboxV models. WatchGuard has released patches in versions 12.3.1_Update3, 12.5.13, 12.11.4, and 2025.1.1, along with mitigations for those unable to patch, such as disabling dynamic peer BOVPNs and adjusting firewall policies. Although no exploitation has yet been observed in the wild, researchers caution that edge firewalls remain prime targets for attackers and urge immediate patching or mitigations.
