Daily Intelligence Update | 16 September 2025

On September 11, 2025, the Great Firewall of China experienced its largest-ever document leak, with nearly 600 GB of source code, internal communications, and work logs released online by the hacktivist group Enlace Hacktivista. The breach reportedly originated from Geedge Networks—founded by Fang Binxing, widely regarded as the “Father of the GFW”—and the MESA Lab at the Chinese Academy of Sciences’ Institute of Information Engineering. The leaked files reveal both domestic censorship operations tied to Xinjiang, Jiangsu, and Fujian, and the export of surveillance technologies to countries such as Myanmar, Pakistan, Ethiopia, and Kazakhstan under Belt and Road initiatives. One archive, mirror/repo.tar, alone accounts for 500 GB of the trove, alongside Jira data and project documentation. While analysts have confirmed overlap with previous media reports, much of the source code remains unexplored, and researchers caution that the files may contain malware or tracking beacons, urging examination only in isolated environments.

Meanwhile, researchers uncovered a malware campaign abusing Microsoft 365 accounts to spread fake OneDrive file-sharing emails. Phishing messages sent from compromised accounts linked to Discord-hosted installers that masqueraded as .docx files but actually contained malicious MSI packages. The installers deployed both Atera and Splashtop Streamer remote monitoring tools, alongside .NET Runtime 8, ensuring persistence even if one tool was removed. By blending legitimate RMM software with trusted content delivery platforms, the campaign effectively bypassed conventional defenses. In another discovery, analysts found a malicious Go package masquerading as an SSH brute forcer but secretly exfiltrating credentials to a Telegram bot. The module, golang-random-ip-ssh-bruteforce, used an embedded wordlist of weak credentials to scan and compromise IoT and misconfigured Linux hosts, forwarding the first successful login to a hardcoded Telegram channel controlled by a Russian-speaking threat actor known as “IllDieAnyway.” Researchers warned that using the tool not only exposes operators to legal risk but also directly hands compromised systems over to the attacker.

Targeted financial organizations in Hong Kong were also hit by a new wave of SquidLoader malware. Delivered via spear-phishing emails with password-protected RAR archives, the payload mimicked legitimate system files but unpacked into an obfuscated infection chain culminating in the in-memory deployment of Cobalt Strike Beacons. SquidLoader leveraged anti-sandbox and anti-debugging tactics—including control flow obfuscation, process blacklisting, and thread-based evasion—achieving near-zero detection rates. The malware also employed Kubernetes-themed URLs for C2 communications and deceptive Mandarin-language error messages to evade automated analysis environments. Related samples were found targeting financial institutions in Singapore and Australia, suggesting a broader regional campaign. Separately, researchers reported a phishing operation targeting Japanese users with a new RAT dubbed MostereRAT. The campaign used weaponized Word documents that installed EPL-based payloads capable of encrypted communications, disabling security tools, creating hidden administrator accounts, and deploying remote access software such as AnyDesk and TightVNC. MostereRAT also featured screen capture, keystroke logging, and RDP configuration via RDP Wrapper, while leveraging mTLS for secure C2 operations.

On the cybercrime front, researchers identified a new leak site launched by a group calling itself Coinbase Cartel. Unlike ransomware operators, Coinbase Cartel does not encrypt files but instead focuses on data theft and staged disclosure as leverage. First advertised on the BreachStars forum by an actor using the handle “coinbasecarell,” the group claims to sell stolen information in “sample packages” for verification before negotiating payment. At launch, the site listed ten victims, with the group framing itself as a data exfiltration and monetization service that seeks “partnerships” with insiders or those holding corporate access. Analysts noted that while Coinbase Cartel is being tracked on forums frequented by groups like Shiny Hunters and Scattered Spider, no confirmed link has been established.

Finally, Microsoft released its September 2025 Patch Tuesday update, addressing 80 vulnerabilities across Windows, Office, Azure, SQL Server, Hyper-V, Edge, Defender Firewall, and even Xbox. Among them were two zero-days: CVE-2025-55234, a Windows SMB Server privilege escalation flaw exploitable via relay attacks, and CVE-2024-21907, a denial-of-service vulnerability in Newtonsoft.Json used by SQL Server. Neither is known to be actively exploited. The most critical issue, CVE-2025-55232, is a remote code execution flaw in Microsoft HPC Pack rated CVSS 9.8 that enables wormable, unauthenticated attacks over TCP port 5999. Microsoft urged immediate patching, strict network segmentation for clusters, and the blocking of exposed ports to prevent exploitation.
