Daily Intelligence Update | 17 September 2025

Researchers have identified dozens of previously unreported domains tied to the Chinese APT group Salt Typhoon and related PRC-backed actors, with infrastructure dating back to 2020. These domains were reportedly used in long-running campaigns targeting telecom providers and ISPs worldwide, including in the U.S. and more than 80 other countries. Salt Typhoon is known for exploiting vulnerabilities to infiltrate telecom networks and access sensitive data such as phone user metadata and even court-authorized wiretap systems. Analysts also noted overlaps with UNC4841, another China-linked group that exploited a Barracuda vulnerability, with several of the discovered domains tied to ProtonMail addresses suggesting shared or cooperative infrastructure. At the same time, researchers reported that the North Korea–linked Kimsuky group has evolved its attack methods to incorporate generative AI and deepfake technology, including use of OpenAI's ChatGPT, to forge convincing South Korean military ID cards and government documents for spear-phishing campaigns. Malicious emails carrying trojans were disguised as official invitations, using obfuscated scripts and delayed execution to bypass antivirus detection. In some cases, phishing lures even claimed that AI was "managing emails on your behalf," furthering the deception. Analysts emphasized that these developments align with wider concerns about AI misuse in cyber espionage and disinformation, with North Korean IT operatives also using AI to create fake identities and bypass sanctions.

A significant data leak also made headlines when a pro-Russian hacktivist group called TwoNet claimed responsibility for stealing the attendee database from C1b3rWall 2025, Spain's largest cybersecurity congress held earlier this year. The stolen data, released as a CSV file, reportedly contained 700 entries including email addresses and IPs belonging to law enforcement, intelligence agencies, corporate employees, and students. Notably, seven internal "@policia[.]es" addresses were included, though their authenticity could not be independently verified. The dataset also featured domains from organizations such as Google, Cisco, Repsol, and ITC Colombia, highlighting the wide potential impact. Given the sensitivity of the attendees which included Spain's CNI, Guardia Civil, and major cybersecurity subcontractors researchers advise treating the dataset as credible until disproven, recommending password resets, MFA enforcement, and monitoring for phishing or extortion attempts.

On the malware front, analysts tracked the resurgence of a Mirai-based botnet strain known as "Gayfemboy," which reappeared in July 2025 targeting vulnerabilities in products from DrayTek, TP-Link, Raisecom, and Cisco. The campaign has been observed across a wide range of countries and industries, from manufacturing and technology to media and construction. The malware employs custom architecture-specific binaries, anti-sandbox timing techniques, and modified packer headers to evade detection. Once deployed, it kills competing malware, maintains persistence, and installs watchdog functions. Its modules enable DDoS attacks, backdoor access, and process termination of security tools, with C2 communications routed through domains such as twinkfinder[.]nl and i-kiss-boys[.]com using multi-port rotation. Another campaign, tracked since 2021, showed continued activity from the Greedy Sponge malware family targeting Mexican organizations. Initially spread via trojanized Microsoft MSI installers, the malware has since adopted server-side geofencing, trojanized zip installers, and secondary infections with SystemBC. Its primary payload, the AllaKore RAT, supports keylogging, screenshots, remote access, and credential theft, particularly for financial fraud. Researchers reported that Greedy Sponge's infrastructure, including phishing sites and C2 servers hosted by Hostwinds, has remained stable, with recent campaigns affecting retail, banking, and manufacturing sectors.

In the vulnerability space, Adobe issued patches for several critical flaws, most notably CVE-2025-54236 dubbed SessionReaperin its Commerce and Magento Open Source platforms. The vulnerability, with a CVSS score of 9.1, could allow attackers to take over customer accounts via the REST API due to improper input validation. While no active exploitation has been confirmed, Adobe rolled out patches and WAF rules, urging immediate updates. The flaw affects Adobe Commerce (2.4.9-alpha2 and earlier), Magento Open Source (2.4.9-alpha2 and earlier), and related modules, and has been compared to other major Magento exploits such as Shoplift (2015) and CosmicSting (2024). Adobe also addressed CVE-2025-54261, a critical path traversal flaw in ColdFusion that could enable arbitrary file system writes, reinforcing the ongoing risks in widely deployed enterprise software.
