4 September 2025

Researchers report that a China-linked actor tracked as CL-STA-0969, part of the Liminal Panda ecosystem, conducted an extended campaign targeting telecommunications providers in Southeast Asia between February and November 2024. Sharing tooling with Light Basin and UNC3886, the group leveraged both custom malware and commodity tools such as Microsocks, FRP, Responder, and FScan, along with exploits for CVE-2016-5195, CVE-2021-4034, and CVE-2021-3156. The campaign featured SSH brute-force with tailored account dictionaries, followed by deployment of malware including AuthDoor, GTPDoor, ChronosRAT, and NoDepDNS to abuse telecom protocols like SSH, DNS, ICMP, and GTP for command-and-control. OPSEC techniques included DNS tunneling, log tampering, SELinux disabling, and PAM backdoors. Tools like Cordscan and SGSN Emulator suggested an interest in mobile location data, though no confirmed exfiltration was observed.

On the ransomware front, researchers identified a new group known as LunaLock, which launched a dark web leak site on September 2, 2025. Its first listed victim is Artists&Clients, a U.S.-based firm in the Media & Entertainment sector. The group threatens not only traditional double-extortion by publishing stolen data but also a novel pressure tactic: submitting stolen artwork to AI companies for use in training datasets. LunaLock claims ransom must be paid in Bitcoin or Monero, while communication occurs via a custom platform dubbed LunaChat, where victims must provide a unique support ID found in a ransom note. This layered extortion strategy, combined with explicit threats to compromise both corporate assets and customer trust, highlights the diversification of psychological pressure used by new RaaS operators.

Researchers also identified a new phishing technique called “ADFSjacking,” in which attackers exploit Microsoft’s Active Directory Federation Services (ADFS) redirects to deliver victims to phishing portals via legitimate Microsoft login URLs. Observed in malicious Google ads for “Office 265,” the campaign redirected users through a fake travel site before presenting a phishing page that impersonated Microsoft’s login portal. By creating a rogue Microsoft tenant configured with ADFS, attackers leveraged legitimate redirects to bypass traditional URL filtering. The use of malvertising and proxy phishing kits complicates detection and highlights the importance of tenant monitoring and federated login auditing.

Meanwhile, Amazon’s threat intelligence team disrupted a watering hole campaign attributed to APT29 (Midnight Blizzard), which compromised legitimate websites to redirect users to attacker-controlled domains exploiting Microsoft’s device code authentication flow. The campaign, which injected obfuscated JavaScript to redirect a portion of site visitors to domains resembling Cloudflare verification portals, attempted to trick victims into authorizing attacker-controlled devices. While AWS infrastructure was briefly abused in early stages, Amazon confirmed no compromise to its systems and partnered with Cloudflare and Microsoft to dismantle malicious infrastructure.

Two critical vulnerabilities were also disclosed this week. IBM issued fixes for CVE-2025-36157, a 9.8 CVSS unauthenticated RCE in Jazz Team Server, which underpins multiple products in its Engineering Lifecycle Management suite. Exploitation could allow attackers to overwrite configuration files, disrupt services, or gain unauthorized access. Patches are available in the latest iFix releases. Separately, CVE-2025-54782 was disclosed in the NestJS framework’s @nestjs/devtools-integration package, affecting versions ≤0.2.0. The flaw allows malicious websites to execute arbitrary code on a developer’s machine by exploiting unsafe JavaScript sandboxing and weak CORS validation. Exploitation requires only that a developer visit a malicious site while running a local dev server with NestJS devtools enabled. A patched version (0.2.1) has been released with stronger sandboxing, origin validation, and authentication requirements.

Taken together, these developments reflect the range of threats confronting enterprises: sophisticated state-linked intrusions into telecom networks, the rapid emergence of new ransomware groups with novel extortion models, phishing campaigns exploiting trusted authentication flows, and critical flaws in widely used enterprise and developer software. Organizations should prioritize patching, monitor federated identity abuse, and assess the risk of both legacy and development environments as adversaries increasingly exploit overlooked entry points.
