2 September 2025

Researchers report that MURKY PANDA (Silk Typhoon), a China-linked espionage group, has conducted sustained campaigns since at least 2023 against North American government, technology, academic, and legal sectors. The group has exploited internet-facing appliances and deployed web shells such as Neo-reGeorg, while relying on custom malware including CloudedHope, a Golang-based Linux RAT with strong anti-analysis capabilities. MURKY PANDA has rapidly weaponized vulnerabilities such as CVE-2023-3519 and abused trusted cloud relationships to move laterally into downstream victims. Analysts observed compromises of SaaS providers through theft of Microsoft Entra ID application registration secrets, enabling authentication as service principals to access customer emails. The group has also abused Delegated Administrative Privileges (DAP) in Microsoft Cloud Solution Providers to create covert admin accounts within customer tenants. Advanced OPSEC measures, including log sanitization and indicator deletion, complicate detection. Defenders are urged to audit service principal credentials, enable Microsoft Graph logging, and closely monitor identity infrastructure for abnormal activity.

A new backdoor dubbed PipeMagic has been discovered disguised as an open-source ChatGPT desktop application. Attributed to threat actor Storm-2460, PipeMagic is delivered via malicious MSBuild payloads and exploits CVE-2025-29824, a CLFS privilege escalation flaw, to deploy ransomware. The malware uses a named pipe format linked to unique bot IDs and employs a modular configuration system that dynamically loads encrypted payloads, verified through SHA-1. Researchers believe PipeMagic supports global financially motivated attacks targeting IT, finance, and real estate.

Separately, researchers uncovered campaigns exploiting exposed Java Debug Wire Protocol (JDWP) interfaces to deploy customized XMRig cryptocurrency miners. By abusing JDWP—often inadvertently enabled in development environments—threat actors executed arbitrary commands to drop miners from domains like awarmcorner[.]world. The malware installs persistence via cron jobs, mimics legitimate processes such as logrotate, and deletes itself after execution to reduce forensic footprint. Targets include systems running Jenkins, Elasticsearch, Spring Boot, and Apache Tomcat.

A new ransomware-as-a-service group, Desolator, launched its dark web leak site on August 28, 2025, listing initial victims CONSTRUSEÑALES and Tri Thuc Software. Desolator offers Windows/Linux/ESXi lockers, affiliate payouts of up to 90%, and comprehensive operational support including privilege escalation, negotiation, and leak site management. Recruitment advertisements posted since June 2025 on forums such as CryptBB and Dread have solicited access brokers, insiders, and pentesters, suggesting the group lined up victims prior to launching its site. The group's affiliate model is still partly manual but includes free lockers for initial access, double extortion practices, and TOX/Session-based victim communications. Researchers note that Desolator may emerge as a competitive new entrant in the RaaS ecosystem given its aggressive revenue-sharing strategy.

August 2025 saw active campaigns by hacktivist groups tied to #OpIsrael and Pro-Palestinian operations, including XSec404, Mr Hamza, Babayo Eror System, BD Anonymous, and AnonXF34rl3ss. These groups primarily claimed DDoS and defacement operations, with some evidence provided through accessibility reports of targeted domains. Pro-Russian actors also re-emerged: Zarya resurfaced with new leak threats, while NoName057(16) announced an alliance with Kurdish actor Hezi Rash and conducted retaliatory DDoS against Western portals. Other hacktivist collectives, including Cyber Jihad Movement and RuskiNet, launched #OpCounterAttack and #OpIndia, threatening disruptions around Indian

Independence Day. RuskiNet later suspended operations against Australia following its policy stance on Palestine, reflecting the politically responsive nature of hacktivist campaigns.

Two new exploit chains raise urgent patching concerns. First, researchers released proof-of-concept exploits for Commvault affecting unpatched instances, chaining CVE-2025-57791 (argument injection), CVE-2025-57790 (path traversal), and related flaws to achieve unauthenticated RCE. A second chain allows attackers to escalate privileges and decrypt admin passwords, again leading to remote access. Commvault patched in version 11.38.25. Additionally, researchers disclosed a chained exploit against the Sitecore Experience Platform involving CVE-2025-53693 (HTML cache poisoning), CVE-2025-53691 (deserialization RCE), and CVE-2025-53694 (information disclosure). Exploitation could allow cache key poisoning followed by unrestricted code execution, expanding upon earlier flaws disclosed in June. Sitecore has issued fixes and urges immediate updates.

This week's developments emphasize the breadth of global cyber activity: nation-state actors weaponizing cloud trust models, financially motivated groups deploying modular backdoors, opportunistic cryptojacking through exposed developer tools, and the rapid launch of new ransomware ecosystems. Enterprises must remain vigilant against both legacy vulnerabilities and evolving access abuse, with priority placed on patching, monitoring cloud provider activity, and defending against DDoS and extortion campaigns driven by shifting geopolitical narratives.
