8 September 2025

Researchers have attributed a newly discovered espionage tool, GONEPOSTAL, to Russia-linked APT28 (Fancy Bear/KTA007). Delivered through a malicious DLL masquerading as Microsoft's SSPICLI.dll, the malware weaponizes Microsoft Outlook as a backdoor for command-and-control. Once installed, it enables macros via registry changes and deploys a password-protected VbaProject.OTM file, establishing persistence through email-triggered macros. These macros parse hidden commands in incoming messages, execute file operations or PowerShell commands, and exfiltrate data via outbound emails. Capabilities include command execution, file transfer, and chunked data exfiltration, all hidden within normal Outlook activity. This approach exemplifies "living-off-the-land" tradecraft, enabling espionage operations to blend into trusted enterprise workflows.

In parallel, fallout continues from the Salesloft Drift compromise, a supply chain intrusion that exploited stolen OAuth tokens to infiltrate Salesforce environments at scale. Attackers leveraged Salesforce Object Query Language to mine for high-value credentials such as AWS keys and Snowflake tokens embedded in records, while systematically deleting queries to cover their tracks. Attribution remains complex: extortion claims have been made by ShinyHunters and actors associated with Scattered Spider, yet Google's threat intelligence team attributes the activity to a distinct group tracked as UNC6395. Multiple victim organizations have confirmed exposure, with analysis showing reconnaissance activity dating back to March 2025. Recommended mitigations include revoking compromised tokens, auditing integrations, rotating keys, and implementing long-term SaaS supply chain hardening.

Additional extortion threats were observed from the Warlock ransomware group, which in August claimed theft of more than one million Colt Technology Services documents and offered the data for $200,000. While only a partial list of file names has been published, no data has been leaked as of early September. Analysts assess possible overlaps with Storm-2603 and AK47/X2ANYLOCK. Meanwhile, two new ransomware leak sites appeared: Obscura, with seven listed victims though its site is currently offline, and Yurei, which on September 5 named Midcity Marketing of Sri Lanka as its first victim and threatened to leak sensitive financial and commercial records.

On the malware front, researchers uncovered a new scam abusing Grok AI on X (formerly Twitter) to amplify malicious campaigns. Attackers embedded URLs in ad metadata fields and prompted Grok to surface them as clickable links, bypassing platform controls and giving the appearance of legitimacy. Victims were redirected to fake CAPTCHA sites hosting info-stealers. Campaigns attracted millions of views, highlighting risks when AI systems can be manipulated into serving as "megaphones" for adversaries. Separately, VirusTotal identified a phishing campaign leveraging malicious SVG files to mimic Colombia's judicial system and deliver malware through DLL side-loading. Over 500 related files were detected, with AI analysis accelerating discovery of the campaign's scope.

Threat researchers also detailed activity from TAG-150, a newly designated actor active since March 2025. TAG-150 operates an extensive infrastructure and has deployed multiple malware families including CastleLoader, CastleBot, and CastleRAT. CastleRAT is available in both Python and C builds, offering capabilities from system information gathering and command execution to keylogging, screen capture, and data exfiltration. TAG-150's phishing lures and GitHub abuse have produced infection rates approaching 30 percent among targets, and its tools are used to deliver both RATs and commodity

infostealers. Analysts debate whether this is a closed affiliate program or an in-house operation, but its rapid development pace and evasion techniques suggest sustained threat potential.

Finally, CISA issued an emergency directive requiring federal agencies to patch CVE-2025-53690, a Sitecore vulnerability under active exploitation. The flaw stems from publicly documented ASP.NET machine keys reused across deployments, enabling ViewState deserialization attacks leading to remote code execution. Exploitation has involved deployment of malware like WEEPSTEEL, credential dumping, tunneling, Active Directory reconnaissance, and lateral movement. Organizations are urged to rotate machine keys, patch immediately, and scan for indicators of compromise, as adversaries have already operationalized this weakness.

---