August 29, 2025

CTI Intelligence Update

Researchers report that Russian state-backed group **Static Tundra** (linked to FSB Center 16 and the Berserk Bear cluster) is actively exploiting the legacy **CVE-2018-0171 Cisco Smart Install vulnerability** to maintain persistent access to unpatched networking equipment. The group has been observed targeting telecom, manufacturing, and education sectors, with particular focus on Ukraine and allied nations. Once access is established, Static Tundra collects device configurations, manipulates TACACS+ settings, and deploys persistent implants such as *SYNful Knock*. Analysts note the use of SNMP, GRE tunnels, and Shodan-derived scanning data to facilitate reconnaissance and redirect traffic of interest via TFTP/FTP exfiltration. Both Cisco and the FBI warn that despite its age, CVE-2018-0171 remains under active exploitation, urging immediate patching or the disabling of Smart Install features to mitigate ongoing threats.

In parallel, a **joint cybersecurity advisory** issued by the NSA, UK NCSC, and more than a dozen international partners has directly attributed **Salt Typhoon** activity to three Chinese technology companies: Sichuan Juxinhe, Beijing Huanyu Tianqiong, and Sichuan Zhixin Ruijie. These firms are alleged to provide operational support to China's Ministry of State Security and PLA cyber elements. Active since at least 2021, Salt Typhoon campaigns have compromised government, telecom, transportation, and military networks worldwide, often targeting telecom providers to intercept communications. Rather than relying on zero-days, the group exploits known vulnerabilities, including Ivanti (CVE-2024-21887), Palo Alto (CVE-2024-3400), and multiple Cisco IOS XE flaws (CVE-2023-20273, CVE-2023-20198, CVE-2018-0171). Post-compromise, Salt Typhoon has been documented enabling unauthorized SSH access, redirecting TACACS+ servers, abusing Cisco Guest Shell containers, and maintaining persistence via GRE/IPsec tunnels and Golang-based SFTP tools. The advisory stresses that even indirectly connected networks may be leveraged as pivot points, emphasizing the need for aggressive patching, hardening, and monitoring.

A new campaign linked to **UNC6395** has compromised over 700 Salesforce instances between August 8–18, 2025, by abusing OAuth and refresh tokens tied to Salesloft's Drift AI integration. The actor systematically ran SOQL queries against Salesforce objects—extracting sensitive data such as AWS keys, Snowflake tokens, and credentials—before deleting query logs to evade detection. Analysts suggest overlaps with techniques used by UNC6040 and UNC3944 (Scattered Spider), although attribution remains inconclusive. Researchers have released IOCs, including Tor exit node IPs, some of which overlap with infrastructure previously tied to **Sandworm's 2023 campaign against Ukrainian telecom providers**, suggesting shared resources or tooling. Salesloft and Salesforce have since revoked affected tokens and removed Drift from AppExchange, but security teams are urged to rotate API keys, re-authenticate integrations, and review logs for evidence of compromise.

Researchers disclosed an **exploit chain targeting SAP NetWeaver** that combines CVE-2025-31324 (CVSS 10.0) and CVE-2025-42999 (CVSS 9.1). Together, the flaws enable authentication bypass and remote code execution, allowing attackers to upload malicious files, execute OS commands, deploy webshells, and seize admin-level control of SAP environments—often without leaving forensic artifacts. The exploit has been attributed to a group calling itself *Scattered LAPSUS$ Hunters – ShinyHunters* and

has already surfaced on VX Underground, with confirmed in-the-wild use. Analysts warn that the deserialization gadgets involved could be repurposed against additional SAP vulnerabilities disclosed earlier this year. Organizations are strongly urged to apply patches immediately, as exploitation has shifted rapidly from proof-of-concept to operational use.
