Hive Pro

Threat Level

Red

CISA: AA25-239A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Salt Typhoon Cyber Attacks Hit 200 Organizations in the United States

Date of Publication

August 29, 2025

Admiralty Code

A1

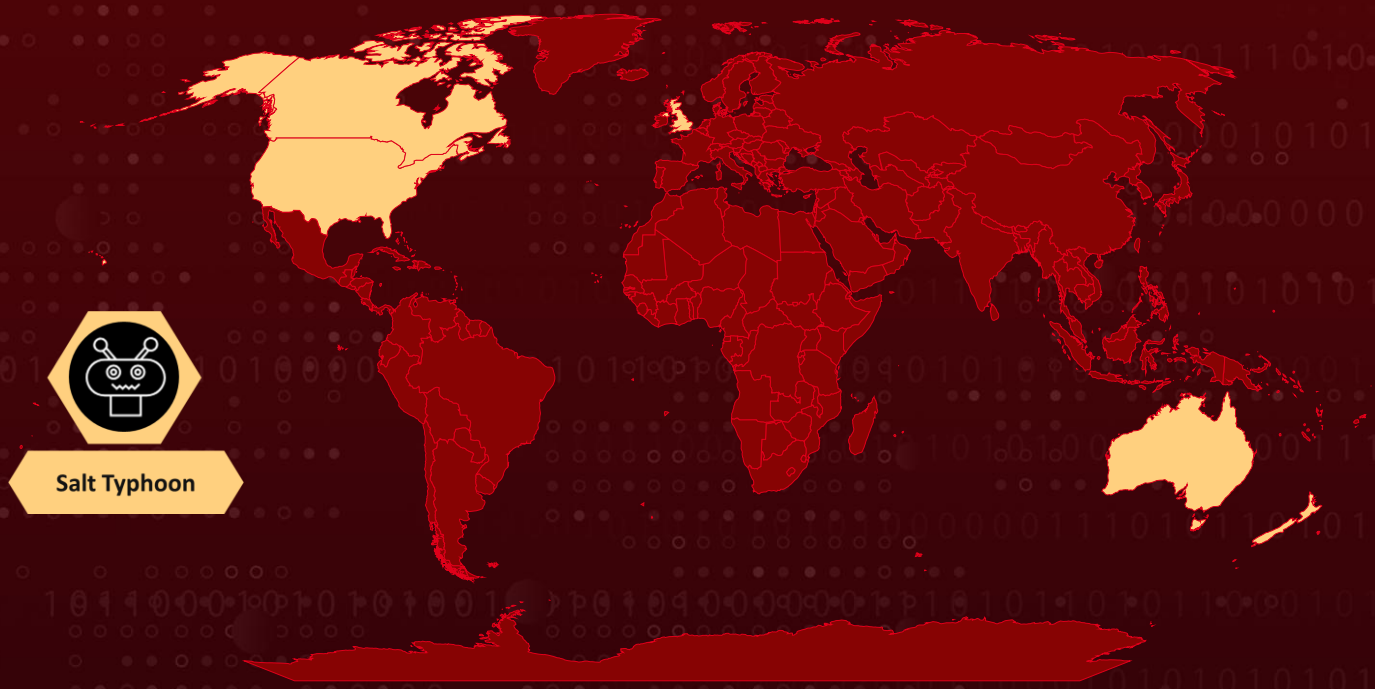
TA Number

TA2025263

Summary

Active Since: 2019
Threat Actor: Salt Typhoon (alias GhostEmperor, OPERATOR PANDA, RedMike, UNC5807, FamousSparrow)
Top Targeted Countries: United States, Australia, Canada, New Zealand, United Kingdom
Targeted Industries: Telecommunications, Government, Transportation, Lodging, Military
Targeted Devices: Fortinet firewalls, Juniper firewalls, Microsoft Exchange, Nokia routers and switches, Sierra Wireless devices, Sonicwall firewalls
Attack: Salt Typhoon, a Chinese state-sponsored hacking group, has expanded its global operations, impacting over 600 organizations across 80 countries, including 200 in the U.S. Most of its attacks begin by exploiting publicly known vulnerabilities, making telecoms and critical sectors prime targets.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	✓	✓	✓
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability	Cisco IOS XE Software	✓	✓	✓
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability	Cisco IOS XE Software	✓	✓	✓
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software	✗	✓	✓

Attack Details

#1 Salt Typhoon, a Chinese state-sponsored threat group active since 2019, has consistently targeted the telecommunications sector and other critical industries, including government, transportation, and military. Their primary focus is on compromising large backbone routers of major telecom providers. Once inside, they exploit compromised devices and trusted connections to pivot into additional networks, often modifying routers to secure long-term, persistent access.

#2 This cluster of activity has been observed across the United States, Australia, Canada, New Zealand, the United Kingdom, and other regions worldwide. Salt Typhoon has broadened its operations, impacting more than 600 organizations in 80 countries, including 200 in the U.S. Most intrusions begin with the exploitation of publicly known vulnerabilities.

#3 Key exploits include Ivanti Connect Secure and Ivanti Policy Secure flaws (CVE-2024-21887), typically chained with the authentication bypass vulnerability CVE-2023-46805. The group has also exploited exposed network edge devices from Cisco (CVE-2018-0171, CVE-2023-20198, CVE-2023-20273) and Palo Alto Networks (CVE-2024-3400).

#4 Salt Typhoon relies on infrastructure such as virtual private servers (VPSs) and compromised intermediate routers, which are not linked to any publicly known botnets, to target telecommunications and network service providers, including ISPs. Their operations do not discriminate by device ownership; any vulnerable edge device can be used as an entry point into networks of interest.

#5 Once compromised, devices are frequently altered to enable persistent access. This includes changing configurations, deploying Generic Routing Encapsulation (GRE) tunnels for data exfiltration, and modifying Access Control Lists (ACLs) to whitelist attacker-controlled IP addresses. They also open standard and non-standard ports, and on supported Cisco devices, run commands inside Linux containers to stage tools, process data, and move laterally.

#6 The group often targets authentication-related protocols and infrastructure. They exploit the Terminal Access Controller Access Control System Plus (TACACS+) protocol, utilizing SNMP enumeration and SSH to traverse networks. From these footholds, they passively collect packet captures (PCAP) from specific ISP customer networks, enabling further intelligence gathering and persistence.

Recommendations

Prioritize Patching and Vulnerability Management: Patch known exploited vulnerabilities immediately, prioritizing edge devices. Address critical CVEs highlighted in this advisory: CVE-2024-21887, CVE-2023-46805, CVE-2024-3400, CVE-2023-20273, CVE-2023-20198, CVE-2018-0171. Upgrade unsupported network devices to vendor-supported models with security updates.

Hardening Management Protocols and Services: Isolate device management services within a dedicated out-of-band management network or Virtual Routing and Forwarding (VRF). Prevent route leakage between management VRFs and customer or peering networks. Restrict management-plane access with explicit Access Control Lists (ACLs) and Control Plane Policing (CoPP), enforcing a default-deny policy while allowing only trusted management IPs or subnets. Use Secure Shell version 2 (SSHv2) exclusively, disable Telnet, and restrict SSH on non-default ports. Apply per-protocol rate limits to slow brute force attempts.

Authentication and Access Control: Change all default credentials across routers, switches, and network appliances. Require public-key authentication for administrative accounts; disable password authentication where feasible. Enforce account lockouts after failed login attempts to slow brute force activity. Implement role-based access controls (RBAC) to minimize privilege exposure.

Network Segmentation & Zero Trust Implementation: Segment critical infrastructure to isolate sensitive data and limit lateral movement. Implement Zero Trust Network Access (ZTNA) by enforcing identity-based policies rather than traditional perimeter security.

Logging and Centralized Monitoring: Enable detailed logging on all devices and forward to a centralized Security Information and Event Management (SIEM) platform. Transmit logs securely over encrypted channels (IPsec, TLS, SSH). Retain logs for sufficient time to support investigations and compliance requirements. Enable alarms for critical configuration changes, privilege escalations, and authentication anomalies.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0003 Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0008** Lateral Movement	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1090** Proxy	**T1090.003** Multi-hop Proxy	**T1071** Application Layer Protocol
T1595 Active Scanning	**T1590** Gather Victim Network Information	**T1590.004** Network Topology	**T1583** Acquire Infrastructure
T1583.003 Virtual Private Server	**T1584** Compromise Infrastructure	**T1584.008** Network Devices	**T1588** Obtain Capabilities
T1588.005 Exploits	**T1588.002** Tool	**T1190** Exploit Public-Facing Application	**T1199** Trusted Relationship
T1569 System Services	**T1609** Container Administration Command	**T1059** Command and Scripting Interpreter	**T1059.006** Python
T1059.008 Network Device CLI	**T1136** Create Account	**T1136.001** Local Account	**T1543** Create or Modify System Process
T1543.005 Container Service	**T1098** Account Manipulation	**T1098.004** SSH Authorized Keys	**T1068** Exploitation for Privilege Escalation
T1110 Brute Force	**T1110.002** Password Cracking	**T1027** Obfuscated Files or Information	**T1027.010** Command Obfuscation

T1562.004 Disable or Modify System Firewall	**T1610** Deploy Container	**T1070** Indicator Removal	**T1070.009** Clear Persistence
T1599 Network Boundary Bridging	**T1040** Network Sniffing	**T1556** Modify Authentication Process	**T1003** OS Credential Dumping
T1082 System Information Discovery	**T1016** System Network Configuration Discovery	**T1021** Remote Services	**T1021.004** SSH
T1560 Archive Collected Data	**T1602.001** SNMP (MIB Dump)	**T1602.002** Network Device Configuration Dump	**T1005** Data from Local System
T1571 Non-Standard Port	**T1572** Protocol Tunneling	**T1095** Non-Application Layer Protocol	**T1048** Exfiltration Over Alternative Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv6	2001[:]41d0[:]700[:]65dc[: :]f656[:]929f, 2a10[:]1fc0[:]7[: :]f19c[:]39b3
IPv4	1[.]222[.]84[.]29, 103[.]168[.]91[.]231, 103[.]199[.]17[.]238, 103[.]253[.]40[.]199, 103[.]7[.]58[.]162, 104[.]194[.]129[.]137, 104[.]194[.]147[.]15, 104[.]194[.]150[.]26, 104[.]194[.]153[.]181, 104[.]194[.]154[.]150, 104[.]194[.]154[.]222, 107[.]189[.]15[.]206, 14[.]143[.]247[.]202, 142[.]171[.]227[.]16, 144[.]172[.]76[.]213, 144[.]172[.]79[.]4, 146[.]70[.]24[.]144, 146[.]70[.]79[.]68, 146[.]70[.]79[.]81,

TYPE	VALUE
IPv4	164[.]82[.]20[.]53, 167[.]88[.]164[.]166, 167[.]88[.]172[.]70, 167[.]88[.]173[.]158, 167[.]88[.]173[.]252, 167[.]88[.]173[.]58, 167[.]88[.]175[.]175, 167[.]88[.]175[.]231, 172[.]86[.]101[.]123, 172[.]86[.]102[.]83, 172[.]86[.]106[.]15, 172[.]86[.]106[.]234, 172[.]86[.]106[.]39, 172[.]86[.]108[.]11, 172[.]86[.]124[.]235, 172[.]86[.]65[.]145, 172[.]86[.]70[.]73, 172[.]86[.]80[.]15, 190[.]131[.]194[.]90, 193[.]239[.]86[.]132, 193[.]239[.]86[.]146, 193[.]43[.]104[.]185, 193[.]56[.]255[.]210, 212[.]236[.]17[.]237, 23[.]227[.]196[.]22, 23[.]227[.]199[.]77, 23[.]227[.]202[.]253, 37[.]120[.]239[.]52, 38[.]71[.]99[.]145, 43[.]254[.]132[.]118, 45[.]125[.]64[.]195, 45[.]125[.]67[.]144, 45[.]125[.]67[.]226, 45[.]146[.]120[.]210, 45[.]146[.]120[.]213, 45[.]59[.]118[.]136, 45[.]59[.]120[.]171, 45[.]61[.]128[.]29, 45[.]61[.]132[.]125, 45[.]61[.]133[.]157, 45[.]61[.]133[.]31, 45[.]61[.]133[.]61, 45[.]61[.]133[.]77, 45[.]61[.]133[.]79, 45[.]61[.]134[.]134, 45[.]61[.]134[.]223,

TYPE	VALUE
IPv4	45[.]61[.]149[.]200, 45[.]61[.]149[.]62, 45[.]61[.]151[.]12, 45[.]61[.]154[.]130, 45[.]61[.]159[.]25, 45[.]61[.]165[.]157, 5[.]181[.]132[.]95, 59[.]148[.]233[.]250, 61[.]19[.]148[.]66, 63[.]141[.]234[.]109, 63[.]245[.]1[.]13, 63[.]245[.]1[.]34, 74[.]48[.]78[.]66, 74[.]48[.]78[.]116, 74[.]48[.]84[.]119, 85[.]195[.]89[.]94, 89[.]117[.]1[.]147, 89[.]117[.]2[.]39, 89[.]41[.]26[.]142, 91[.]231[.]186[.]227, 91[.]245[.]253[.]99
MD5	eba9ae70d1b22de67b0eba160a6762d8, 33e692f435d6cf3c637ba54836c63373
SHA256	8b448f47e36909f3a921b4ff803cf3a61985d8a10f0fe594b405b92ed0fc21f1, f2bbba1ea0f34b262f158ff31e00d39d89bbc471d04e8fca60a034cabe18e4f4, da692ea0b7f24e31696f8b4fe8a130dbbe3c7c15cea6bde24cccc1fb0a73ae9e, a1abc3d11c16ae83b9a7cf62ebe6d144dfc5e19b579a99bad062a9d31cf30bfe

Patch Details

CVE-2024-21887 & CVE-2023-46805:
https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

CVE-2024-3400:
https://security.paloaltonetworks.com/CVE-2024-3400

CVE-2023-20273:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

CVE-2023-20198:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

CVE-2018-0171:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

References

https://www.cisa.gov/sites/default/files/2025-08/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf

https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a?utm_source=SaltTyphoon&utm_medium=AlertAdvisory

https://www.fbi.gov/video-repository/salttyphoon082725.mp4/view

https://www.washingtonpost.com/technology/2025/08/27/fbi-advisory-china-hacking-expansion/

https://www.wsj.com/politics/national-security/chinese-spies-hit-more-than-80-countries-in-salt-typhoon-breach-fbi-reveals-59b2108f

https://hivepro.com/threat-advisory/salt-typhoons-covert-campaign-targeting-u-s-telecom-networks/

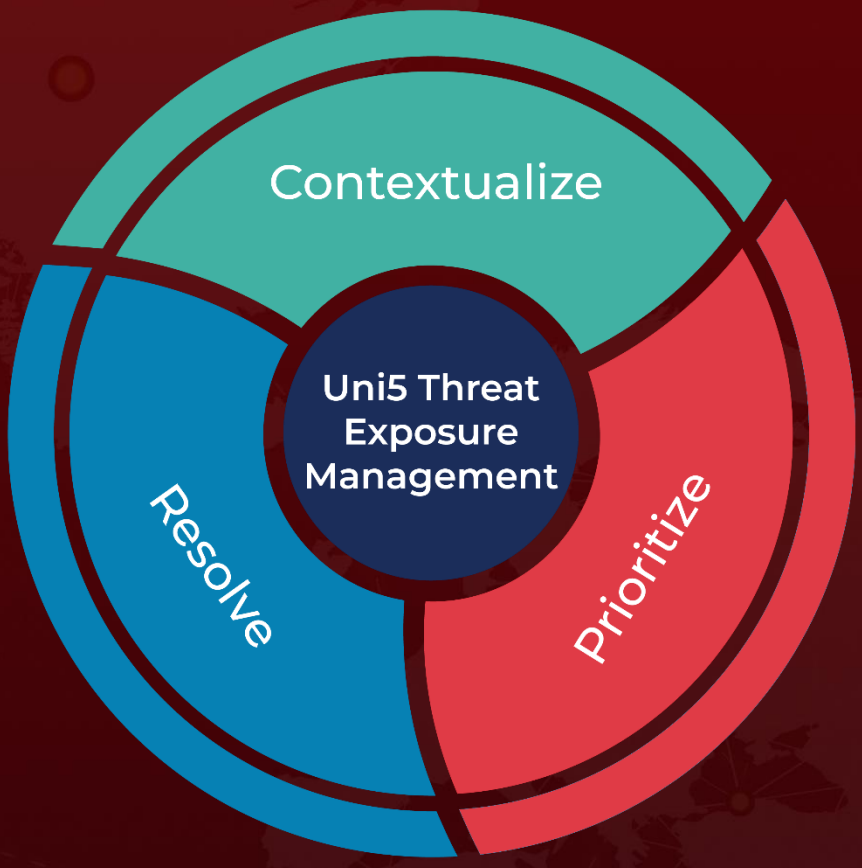
https://hivepro.com/threat-advisory/rondodox-botnet-campaign-targets-tbk-dvrs-and-four-faith-routers/

https://attack.mitre.org/groups/G1045/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 29, 2025 • 5:30 AM

More at www.hivepro.com