ADVISORY FOR ICM SECTOR

Salt Typhoon operation – network device exploitation

Original report published on: August 27, 2025[1]

Executive Summary

On 27 August 2025, CISA, NSA, and cyber and intelligence agencies from 13 countries have published a joint advisory on Salt Typhoon APT (also known as OPERATOR PANDA, RedMike, UNC5807, and GhostEmperor), which has been targeting organizations worldwide in sectors including telecommunications, government, transportation, and military infrastructure as part of an ongoing campaign since 2021. The advisory documents the APT's recent campaign targeting backbone and edge routers of major telecom providers. It consolidates findings from multiple government and industry investigations and provides a comprehensive overview of the threat actor's tactics, techniques, and procedures (TTPs) to support detection, threat hunting, and mitigation.

In November 2024, Trend Micro published[2] Salt Typhoon's activity against telecommunications providers that focused primarily on endpoint exploits, whereas the CISA advisory emphasizes attacks against backbone and edge routers, detailing the group's operational techniques across core network infrastructure.

Background

Salt Typhoon gains initial access by exploiting known vulnerabilities, including Ivanti Connect Secure and Policy (CVE-2024-21887), Palo Alto PAN-OS GlobalProtect (CVE-2024-3400), Cisco IOS XE devices (CVE-2023-20273, CVE-2023-20198), and Cisco Smart Install (CVE-2018-0171). The group specifically targets Web Services Management Agent (a web services–based API for managing Cisco devices) endpoints for CVE-2023-20198 exploitation, often employing double encoding to obfuscate activity.

After gaining access, Salt Typhoon employs "living off the land" techniques to evade detection, leveraging built-in tools while using open-source exploits to establish persistence, move laterally, and conduct reconnaissance. The actors modify device configurations, collect network and management data, and prepare the environment to support ongoing operations, including command and control (C2) and data exfiltration.

The actors establish persistence by modifying Access Control List (ACL), typically naming it "access-list 20", opening non-standard ports (SSH on 22x22 or xxx22, and HTTP on 18xxx), creating Generic Routing Encapsulation (GRE) or IPsec tunnels, and abusing Cisco Guest Shell containers to run publicly available malicious Python and Tool Command Language (Tcl) scripts, including siet.py, TCLproxy.tcl, and map.tcl. On Cisco IOS XR devices, they enable sshd_operns, a built-in service that provides an additional SSH endpoint directly into the host Linux OS, maintaining persistent access via TCP/57722. They also exploit SNMP for device enumeration via SNMPwalk and configuration changes through SNMP SET requests, particularly targeting devices with weak community strings such as "public" and "private."

For lateral movement and reconnaissance, Salt Typhoon targets authentication protocols (TACACS+, RADIUS), network infrastructure (BGP routes, MPLS configurations), and management data (device configurations, network diagrams). They collect traffic using Cisco's native packet capture capabilities and enable port mirroring (SPAN, RSPAN, ERSPAN), while redirecting TACACS+ servers to actor-controlled infrastructure for credential harvesting.

Salt Typhoon establishes command and control (C2) by leveraging open-source multi-hop pivoting tools, such as STOWAWAY, to build chained relays and enable interactive remote access. The group also employs anti-forensics techniques, including log deletion and configuration cleanup, to evade detection. Data exfiltration occurs via abuse of peering connections between providers, separate C2 channels within high-traffic nodes, and tunnelled communications over GRE or IPsec.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the Salt Typhoon attacks identified in this advisory:

- Scan for Indicators of Compromise listed in Annex A to detect potential threat activities.
- Refer to the MITRE ATT&CK techniques in Annex B to create, test, and validate detection rules against the observed threat behaviours.
- Ensure updated internet facing network devices (Ivanti Connect Secure, Palo Alto PAN-OS, Cisco IOS XE) to date to prevent exploitation of known CVEs.
- Conduct regular vulnerability assessments of internet-facing systems to identify and remediate weaknesses.
- Implement continuous monitoring for:
    - Unauthorized ACL changes
    - Unexpected, unauthorized or undocumented GRE or IPsec tunnels
    - Packet capture enablement outside normal operations
    - Non-standard port openings on critical network devices
    - TACACS+ server redirections
- Harden device configurations by disabling unnecessary services such as sshd_operns, restrict Cisco Guest Shell usage, and enforce SNMPv3 with proper authentication and privacy settings while disabling SNMPv1 and v2 entirely.
- Limit management interfaces to trusted IPs, ensure they are not directly internet-facing, segment management from user and production networks, and restrict ACLs, open ports, and tunnels to only those required for legitimate operations.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

SHA256 Hash	Description
8b448f47e36909f3a921b4ff803cf3a61985d8a10f0fe594b405b92ed0fc21f1	Golang-based SFTP tool
f2bbba1ea0f34b262f158ff31e00d39d89bbc471d04e8fca60a034cabe18e4f4	
da692ea0b7f24e31696f8b4fe8a130dbbe3c7c15cea6bde24cccc1fb0a73ae9e	
a1abc3d11c16ae83b9a7cf62ebe6d144dfc5e19b579a99bad062a9d31cf30bfe	

IP Address	Description
1.222.84[.]29	Salt-Typhoon-controlled IP addresses first seen in August 2021 and may no longer be used
5.181.132[.]95	
14.143.247[.]202	
23.227.196[.]22	
23.227.199[.]77	
23.227.202[.]253	
37.120.239[.]52	
38.71.99[.]145	
43.254.132[.]118	
45.59.118[.]136	
45.59.120[.]171	
45.61.128[.]29	
45.61.132[.]125	
45.61.133[.]31	
45.61.133[.]61	
45.61.133[.]77	
45.61.133[.]79	
45.61.133[.]157	
45.61.134[.]22	
45.61.134[.]134	
45.61.134[.]223	
45.61.149[.]62	
45.61.149[.]200	
45.61.151[.]12	
45.61.154[.]130	
45.61.159[.]25	
45.61.165[.]157	
45.125.64[.]195	
45.125.67[.]144	
45.125.67[.]226	
45.146.120[.]210	
45.146.120[.]213	
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	
89.41.26[.]142	

89.117.1[.]147	
89.117.2[.]39	
91.231.186[.]227	
91.245.253[.]99	
103.7.58[.]162	
103.168.91[.]231	
103.199.17[.]238	
103.253.40[.]199	
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	
142.171.227[.]16	
144.172.76[.]213	
144.172.79[.]4	
146.70.24[.]144	
146.70.79[.]68	
146.70.79[.]78	
146.70.79[.]81	
164.82.20[.]53	
167.88.164[.]166	
167.88.172[.]70	
167.88.173[.]58	
167.88.173[.]158	
167.88.173[.]252	
167.88.175[.]175	
167.88.175[.]231	
172.86.65[.]145	
172.86.70[.]73	
172.86.80[.]15	
172.86.101[.]123	
172.86.102[.]83	
172.86.106[.]15	
172.86.106[.]39	
172.86.106[.]234	
172.86.108[.]11	
172.86.124[.]235	
190.131.194[.]90	
193.43.104[.]185	
193.56.255[.]210	
193.239.86[.]132	
193.239.86[.]146	
212.236.17[.]237	
2001:41d0:700:65dc::f656[:]929f	
2a10:1fc0:7::f19c[:]39b3	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	T1595	Active Scanning
Reconnaissance	T1590.004	Gather Victim Network Information: Network Topology
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Servers
Resource Development	T1584.008	Compromise Infrastructure: Network Devices
Resource Development	T1588.005	Obtain Capabilities: Exploits
Resource Development	T1588.002	Obtain Capabilities: Tool
Initial Access	T1190	Exploit Public-Facing Application
Initial Access	T1199	Trusted Relationship
Execution	T1569	System Services
Execution	T1609	Container Administration Command
Execution	T1059.006	Command and Scripting Interpreter: Python
Execution	T1059.008	Command and Scripting Interpreter: Network Device CLI
Persistence	T1136.001	Create Account: Local Account
Persistence	T1543.005	Container Service
Persistence	T1098.004	Account Manipulation: SSH Authorized Keys
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Privilege Escalation	T1110.002	Brute Force: Password Cracking
Defense Evasion	T1027.010	Obfuscated Files or Information: Command Obfuscation
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1562.004	Impair Defenses: Disable or Modify System Firewall
Defense Evasion	T1610	Deploy Container
Defense Evasion	T1070	Indicator Removal
Defense Evasion	T1070.009	Indicator Removal: Clear Persistence
Defense Evasion	T1599	Network Boundary Bridging
Credential Access	T1040	Network Sniffing
Credential Access	T1556	Modify Authentication Process
Credential Access	T1003	OS Credential Dumping
Credential Access	T1110.002	Brute Force: Password Cracking
Discovery	T1082	System Information Discovery
Discovery	T1016	System Network Configuration Discovery
Lateral Movement	T1021	Remote Services
Lateral Movement	T1021.004	Remote Services: SSH
Collection	T1560	Archive Collected Data
Collection	T1602.001	Data from Configuration Repository: SNMP MIB Dump

Collection	T1602.002	Data from Configuration Repository: Network Device Configuration Dump
Collection	T1005	Data from Local System
Command and Control	T1090	Proxy
Command and Control	T1090.003	Proxy: Multi-hop Proxy
Command and Control	T1071	Application Layer Protocol
Command and Control	T1571	Non-Standard Port
Command and Control	T1572	Protocol Tunneling
Command and Control	T1095	Non-Application Layer Protocol
Exfiltration	T1048.003	Exfiltration over Alternative Protocol

References

1. Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System
2. Weathering the storm: In the midst of a Typhoon