Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

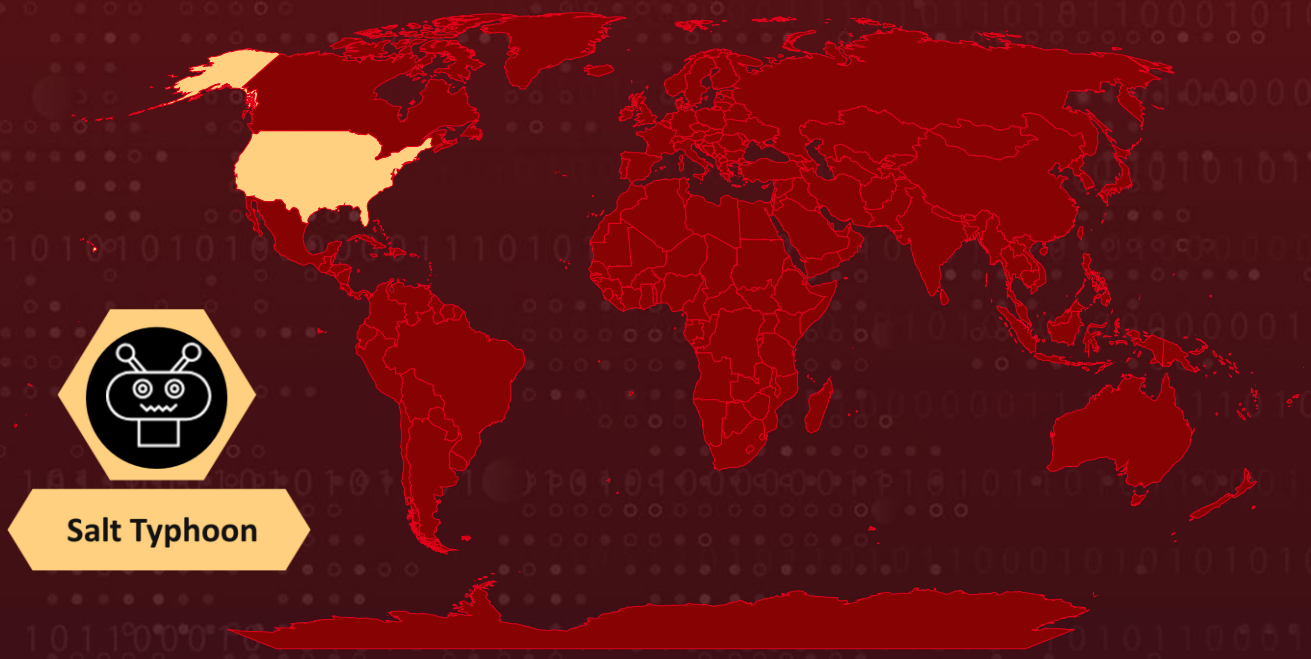
Salt Typhoon's Covert Campaign: Targeting U.S. Telecom Networks

Date of Publication	Admiralty Code	TA Number
February 21, 2025	A1	TA2025053

Summary

Attack Discovered: Late 2024
Targeted Country: U.S.
Affected Industry: Telecommunication
Actor: Salt Typhoon (aka GhostEmperor, UNC2286, FamousSparrow, Earth Estries, RedMike)
Attack: The Chinese state-sponsored group Salt Typhoon has been targeting U.S. telecommunications providers using a custom tool called JumbledPath to stealthily monitor network traffic and capture sensitive data. In several cases, the attackers gained access to core networking infrastructure, primarily by using legitimate login credentials, though in one instance, they likely exploited a known Cisco vulnerability. A key tactic in this campaign is the use of living-off-the-land (LOTL) techniques, enabling the threat actors to blend into existing network environments and evade detection while gathering critical information.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software	✗	✓	✓
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability	Cisco IOS XE Software	✓	✓	✓
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability	Cisco IOS XE Software	✓	✓	✓

Attack Details

#1 Salt Typhoon has been targeting major U.S. telecommunications companies in an extensive intrusion campaign. The campaign focuses on exploiting core networking infrastructure, primarily Cisco devices. In most cases, the attackers gained access using stolen credentials, though one confirmed instance involved the abuse of CVE-2018-0171.

#2 Salt Typhoon has shown the ability to stay hidden in compromised systems for years, with one case lasting over three years. They use living-off-the-land (LOTL) techniques, meaning they rely on built-in system tools instead of external malware. This helps them avoid detection and leave minimal traces,. They have also managed to maintain access across different network equipment from multiple vendors, proving their ability to stay persistent in targeted environments.

#3 Throughout the campaign, Salt Typhoon systematically harvested credentials, extracting configuration files from network devices to decipher weak passwords and intercept SNMP, TACACS, and RADIUS traffic. Stolen device configurations often exfiltrated via TFTP and FTP contained authentication details and network mapping data, enabling reconnaissance and lateral movement. They modified network configurations and critical system settings, ACLs, SNMP community strings, and loopback interface IPs. To maintain long-term access, they created hidden user accounts, altered SSH settings, and deployed GRE tunnels, ensuring a backdoor into the compromised environment.

#4 A key tool in their arsenal is JumbledPath, a custom-built Go-based ELF binary designed to execute packet captures on remote Cisco devices while obfuscating its activity by clearing logs. This utility enabled the attackers to stealthily collect network traffic, encrypting and compressing the data before exfiltration. Salt Typhoon also exploited network loopholes by sourcing SSH connections via loopback interfaces, bypassing ACL restrictions and further concealing their movements.

#5 Beyond these tactics, Salt Typhoon expanded its operations in December 2024 – January 2025, compromising over 1,000 Cisco devices, with more than half located in the U.S., South America, and India. The group specifically targeted internet-exposed Cisco routers, exploiting two high-profile vulnerabilities, CVE-2023-20198 which is a privilege escalation flaw in Cisco IOS XE Web UI and CVE-2023-20273 which is a Command Injection Vulnerability that is used post-initial access to escalate privileges and gain root control.

#6 By chaining these exploits, Salt Typhoon created privileged user accounts, modified device configurations, and established persistence using GRE tunnels, enabling long-term access to critical telecom infrastructure. Salt Typhoon remains an active threat to Cisco users, making patching crucial to mitigating future attacks.

Recommendations

Apply Patch: Make sure all Cisco devices are running the latest firmware to protect against known vulnerabilities like CVE-2018-0171, CVE-2023-20198 and CVE-2023-20273. Regularly check for security updates from Cisco and apply patches as soon as they're available to stay ahead of potential threats.

Strengthen Network Security with Access Controls: Restrict internet exposure of network management interfaces and enforce strict access control lists (ACLs) to limit unauthorized access. Implement network segmentation to contain potential threats and prevent attackers from moving laterally within your infrastructure.

Enforce MFA: Enable multi-factor authentication (MFA) on all network devices to prevent unauthorized access, even if credentials are compromised. Implement strict password policies with regular updates and enforce strong, complex passwords to reduce the risk of credential-based attacks.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Secure Network Traffic with Encryption: Ensure all monitoring and configuration traffic is encrypted by using secure protocols such as SNMPv3, HTTPS, SSH, NETCONF, and RESTCONF. This prevents attackers from intercepting sensitive data and strengthens overall network security.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0010 Exfiltration	TA0011 Command and Control	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1059 Command and Scripting Interpreter	T1059.004 Unix Shell
T1600 Weaken Encryption	T1027 Obfuscated Files or Information	T1556 Modify Authentication Process	T1016 System Network Configuration Discovery
T1222 File and Directory Permissions Modification	T1190 Exploit Public-Facing Application	T1021 Remote Services	T1021.004 SSH
T1068 Exploitation for Privilege Escalation	T1584 Compromise Infrastructure	T1105 Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	185[.]141[.]24[.]28, 185[.]82[.]200[.]181

Patch Details

Update all Cisco devices are running the latest firmware to protect against known vulnerabilities like CVE-2018-0171, CVE-2023-20198 and CVE-2023-20273.

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

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

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

References

https://blog.talosintelligence.com/salt-typhoon-analysis/

https://hivepro.com/threat-advisory/unpatched-zero-day-vulnerability-actively-exploited-in-cisco-ios-xe/

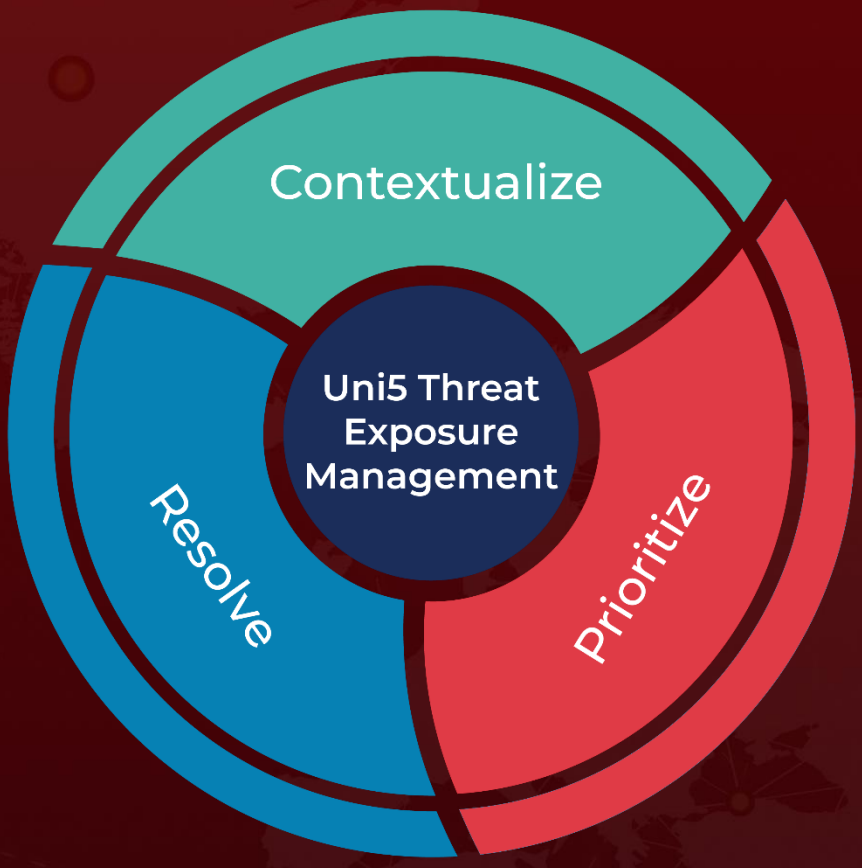
https://hivepro.com/threat-advisory/growing-threat-of-earth-estries-group-behind-major-telecom-breaches/

https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf

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

February 21, 2025 • 4:00 AM

More at www.hivepro.com