Salt Typhoon: An Analysis of Vulnerabilities Exploited by this State-Sponsored Actor

By Scott Caveza

Published: 2025-01-23 · Archived: 2026-04-06 03:26:58 UTC

Salt Typhoon, a state-sponsored actor linked to the People's Republic of China, has breached at least nine U.S.-based telecommunications companies with the intent to target high profile government and political figures. Tenable Research examines the tactics, techniques and procedures of this threat actor.

Background

Throughout 2024, attacks from sophisticated advanced persistent threat (APT) actors associated with the People's Republic of China (PRC) were a major focus for U.S. government organizations, including the Cybersecurity and Infrastructure Security Agency (CISA). In a previous blog post, we examined Volt Typhoon, a PRC state-sponsored actor known to target critical infrastructure. However in September, the Wall Street Journal reported on another PRC actor, Salt Typhoon, citing anonymous sources who said that the group had breached multiple U.S. telecommunications providers. While several outlets reported on speculation of the report, in early October, CISA and the Federal Bureau of Investigation (FBI) offered official confirmation of the attacks when they released a joint statement that "the U.S. Government is investigating the unauthorized access to commercial telecommunications infrastructure by actors affiliated with the People's Republic of China." By December, a White House press call confirmed that at least eight U.S. telecommunications providers had been breached, with that figure increasing to at least nine telecommunications companies by December 27. As new details emerge on Salt Typhoon and its targets, this Tenable Research blog examines the tactics, techniques and procedures (TTPs) employed, including the exploitation of known vulnerabilities associated with this threat actor.

Analysis

Salt Typhoon is a sophisticated threat group whose targets include the telecommunications, government and technology sectors. The group is tracked under several monikers, including FamousSparrow, GhostEmperor, Earth Estries and UNC2286. This APT has most recently been in the news for breaching multiple U.S. telecommunications providers; however it's believed that its targets in this sector span the globe. In the U.S, government officials claimed that Salt Typhoon's targets include government officials primarily involved in "political activity," sparking CISA and joint partners to release guidance on visibility and security hardening of communications infrastructure as well prompting the White House to issue the Executive Order titled "Strengthening and Promoting Innovation in the Nation's Cybersecurity." Based on various reports on Salt Typhoon, its primary objective appears to be espionage.

In mid-December, CISA released the document "Mobile Communications Best Practice Guidance," with an emphasis on using end-to-end encryption for secure communications. While it's unclear what information may have been accessed by Salt Typhoon, CISA and other government agencies, including the Federal

Communications Commission (FCC) have been actively helping and providing security guidance to the impacted organizations, as communications infrastructure is a matter of national security.

Known CVEs commonly exploited by Salt Typhoon

Salt Typhoon typically gains initial access to its victim networks by targeting external-facing assets using known vulnerabilities. While not an exhaustive list, the table below highlights some of the CVEs known to have been exploited by Salt Typhoon.

CVE	Description	CVSSv3 Score	VPR
CVE-2021-26855	Microsoft Exchange Server Server-Side Request Forgery Vulnerability (ProxyLogon)	9.8	9.8
CVE-2022-3236	Sophos Firewall Code Injection Vulnerability	9.8	7.4
CVE-2023-48788	FortiClient Enterprise Management Server (FortiClientEMS) SQL Injection Vulnerability	9.8	9.4
CVE-2024-21887	Ivanti Connect Secure and Ivanti Policy Secure Command Injection Vulnerability	9.1	9.8
CVE-2023-46805	Ivanti Connect Secure and Ivanti Policy Secure Authentication Bypass Vulnerability	8.2	6.7

**Please note: Tenable's Vulnerability Priority Rating (VPR) scores are calculated nightly. This blog post was published on January 23 and reflects VPR at that time.*

Several of these vulnerabilities have been routinely exploited by APT and ransomware groups alike, including CVE-2021-26855, also known as ProxyLogon, and related Microsoft Exchange vulnerabilities including CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065. Ivanti Connect Secure/Policy Secure and Fortinet FortiClientEMS have each been the subject of Tenable Research blog posts and CVE-2022-3236, the SQL injection flaw in Sophos Firewall, was featured in our "2022 Threat Landscape Report."

Of these five CVEs, four of them were exploited in the wild as zero-day vulnerabilities. While it's unknown if Salt Typhoon exploited any of these flaws as zero-days, the level of sophistication from the group does suggest it has the technical ability to develop and exploit zero-day flaws in its attacks.

Despite these CVEs having had patches available, an analysis of anonymized Tenable scan data reveals that of nearly 30,000 instances impacted by ProxyLogon, a staggering 91% remain unpatched. In a stark contrast, an analysis of over 20,000 devices impacted by both Ivanti vulnerabilities (CVE-2023-46805 and CVE-2024-21887), our data found that these devices were fully remediated in over 92% of cases.

As part of CISA's guidance for enhanced visibility and hardening, the agency mentioned Cisco network equipment. While CISA didn't mention specific Cisco device models or vulnerabilities, its guidance does note that

PRC-affiliated actors have targeted Cisco-specific devices and as such, care should be taken to ensure organizations in the communications sector and beyond are properly securing and hardening their Cisco network devices. CISA's recommendations include disabling Cisco's Smart Install service, which is often abused by attackers and should be properly configured or disabled to prevent abuse.

Post-Compromise Activity

Salt Typhoon is known for maintaining a stealthy presence on victim networks and remaining undetected for a significant time period. It maintains persistence by utilizing custom malware including GhostSpider, SnappyBee and the Masol remote access trojan (RAT).

It's been reported that the group has been active for several years and may have breached and maintained access at telecommunications providers for months before being detected. In a recent blog by outgoing CISA Director Jen Easterly, she revealed that "CISA threat hunters previously detected the same actors in U.S. government networks."

The "eyes" of the various "Typhoons"

Each suspected state-sponsored PRC actor includes the family name of "Typhoon." In recent months, CISA and security vendors have issued several warnings regarding the various "Typhoon" groups, including Volt Typhoon, Flax Typhoon, and Salt Typhoon. Volt Typhoon's focus is persistence and stealth, targeting critical infrastructure while Flax Typhoon's focus is on attack infrastructure, building botnets from compromised Internet of Things (IoT) devices.

While each group's targets and activities are unique, the "eye" of each of these typhoons is they target unpatched and often well-known vulnerabilities for initial access, targeting public-facing servers. Despite the persistence of these threat actors, it's vital that organizations routinely patch public-facing devices and quickly mitigate known and exploited vulnerabilities. This is underscored in commentary from the Federal Communications Commission (FCC) Chairwoman Jessica Rosenworcel:

> *"In light of the vulnerabilities exposed by Salt Typhoon, we need to take action to secure our networks. Our existing rules are not modern. It is time we update them to reflect current threats so that we have a fighting chance to ensure that state-sponsored cyberattacks do not succeed. The time to take this action is now. We do not have the luxury of waiting."*

Identifying affected systems

Tenable offers several solutions to help identify potential exposures and attack paths as well as to identify systems vulnerable to the CVEs mentioned in this blog. For a holistic approach, we recommend using the Tenable One Exposure Management Platform. Tenable One extends beyond traditional vulnerability management, which concentrates on the discovery and remediation of publicly disclosed CVEs. A foundational part of any exposure management program, Tenable One includes data about configuration issues, vulnerabilities and attack paths across a spectrum of assets and technologies — including identity solutions (e.g., Active Directory); cloud configurations and deployments; and web applications.

Tenable Plugin Coverage

A list of Tenable plugins for these vulnerabilities can be found on the individual CVE pages for CVE-2021-26855, CVE-2022-3236, CVE-2023-48788, CVE-2024-21887 and CVE-2023-46805. These links will display all available plugins for these vulnerabilities, including upcoming plugins in our Plugins Pipeline. In addition to these CVEs, we also recommend scanning with plugin ID 105161 to identify if Cisco Smart Install is enabled on any Cisco devices in your network.

Tenable Attack Path Analysis techniques

The following are a list of attack paths associated with Salt Typhoon and the associated Tenable Attack Path Analysis techniques:

MITRE ATT&CK ID	Description	Tenable Attack Path techniques
T1003.003	OS Credential Dumping: NTDS	T1003.003_Windows
T1021	Remote Services	T1021.002_Windows
T1047	Windows Management Instrumentation	T1047_Windows
T1053.005	Create or Modify System Process: Windows Service	T1053.005_Windows
T1059.001	Command and Scripting Interpreter: PowerShell	T1059.001_Windows
T1059.003	Command and Scripting Interpreter: Windows Command Shell	T1059.003_Windows
T1068	Exploitation for Privilege Escalation	T1068_Windows
T1078	Valid Accounts	T1078.001_ICS T1078.003_Windows T1078.004_Azure
T1078.002	Valid Accounts: Domain Accounts	T1078.002_Windows
T1082	System Information Discovery	T1082
T1087	Account Discovery	T1087.004_Azure T1087.004_AWS
T1134	Access Token Manipulation	T1134.005_Windows
T1190	Exploit Public-Facing Application	T1190_Aws

MITRE ATT&CK ID	Description	Tenable Attack Path techniques
		T1190_WAS
T1203	Exploitation for Client Execution	T1203_Windows
T1482	Domain Trust Discovery	T1482_Windows
T1547	Boot or Logon Autostart Execution	T1547.002_Windows T1547.005_Windows
T1574	Hijack execution flow	T1574.007_Windows T1574.009_Windows T1574.010_Windows T1574.011_Windows

Tenable Identity Exposure Indicators of Exposure and Indicators of Attack

The following are a list of Indicators of Exposure and Indicators of Attack for Tenable Identity Exposure:

MITRE ATT&CK ID	Description	Indicators
T1003.003	OS Credential Dumping: NTDS	I-NtdsExtraction
T1021	Remote Services	C-LAPS-UNSECURE-CONFIG C-AAD-PRIV-SYNC C-USERS-REVER-PWDS
T1036	Masquerading	C-CONFLICTED-OBJECTS
T1055.001	Process Injection: Dynamic-link Library Injection	I-DnsAdmins
T1068	Exploitation for Privilege Escalation	I-SamNameImpersonation

MITRE ATT&CK ID	Description	Indicators
T1078	Valid Accounts	MISSING-MFA-FOR-NON-PRIVILEGED-ACCOUNT C-PASSWORD-DONT-EXPIRE C-USER-PASSWORD C-PRIV-ACCOUNTS-SPN C-NATIVE-ADM-GROUP-MEMBERS C-AAD-SSO-PASSWORD C-MSA-COMPLIANCE C-PASSWORD-POLICY C-REVER-PWD-GPO C-CLEARTEXT-PASSWORD C-DC-ACCESS-CONSISTENCY C-PROP-SET-SANITY C-SLEEPING-ACCOUNTS C-KERBEROS-CONFIG-ACCOUNT HIGH-NUMBER-OF-ADMINISTRATORS MISSING-MFA-FOR-PRIVILEGED-ACCOUNT C-AUTH-SILO C-KRBTGT-PASSWORD C-AAD-PRIV-SYNC C-SERVICE-ACCOUNT C-PASSWORD-NOT-REQUIRED C-ADMIN-RESTRICT-AUTH C-ADMINCOUNT-ACCOUNT-PROPS

MITRE ATT&CK ID	Description	Indicators
		C-DANGEROUS-SENSITIVE-PRIVILEGES C-PKI-DANG-ACCESS C-EXCHANGE-MEMBERS C-PASSWORD-HASHES-ANALYSIS C-ADM-ACC-USAGE C-DANG-PRIMGROUPID C-DSHEURISTICS
T1134	Access Token Manipulation	C-ACCOUNTS-DANG-SID-HISTORY
T1190	Exploit Public-Facing Application	APPLICATION-ALLOWING-MULTI-TENANT-AUTHENTICATION
T1203	Exploitation for Client Execution	C-OBSOLETE-SYSTEMS

Tenable Web App Scanning

MITRE ATT&CK ID	Description	Indicators
T1190	Exploit Public-Facing Application	T1190_WAS

Join Tenable's Security Response Team on the Tenable Community.

Learn more about Tenable One, the Exposure Management Platform for the modern attack surface.

Scott Caveza

Senior Staff Research Engineer, Research Special Operations

Scott joined Tenable in 2012 as a Research Engineer on the Nessus Plugins team. Over the years, he has written hundreds of plugins for Nessus, and reviewed code for even more from his time being a team lead and manager of the Plugins team. Previously leading the Security Response team and the Zero Day Research team, Scott is currently a member of the Research Special Operations team, helping the research organization respond to the latest threats. He has over a decade of experience in the industry with previous work in the Security Operations Center (SOC) for a major domain registrar and web hosting provider. Scott is a current CISSP and actively maintains his GIAC GWAPT Web Application Penetration Tester certification.

Interests outside of work: Scott enjoys spending time with his family, camping, fishing and being outdoors. He also enjoys finding ways to break web applications and home renovation projects.
