Weathering the storm: In the midst of a Typhoon

By Cisco Talos

Published: 2025-02-20 · Archived: 2026-04-05 13:28:08 UTC

Thursday, February 20, 2025 08:00

Summary

Cisco Talos has been closely monitoring reports of widespread intrusion activity against several major U.S. telecommunications companies. The activity, initially reported in late 2024 and later confirmed by the U.S. government, is being carried out by a highly sophisticated threat actor dubbed Salt Typhoon. This blog highlights our observations on this campaign and identifies recommendations for detection and prevention of the actor's activities.

Public reporting has indicated that the threat actor was able to gain access to core networking infrastructure in several instances and then use that infrastructure to collect a variety of information. There was only one case in which we found evidence suggesting that a Cisco vulnerability (CVE-2018-0171) was likely abused. In all the other incidents we have investigated to date, the initial access to Cisco devices was determined to be gained through the threat actor obtaining legitimate victim login credentials. The threat actor then demonstrated their ability to persist in target environments across equipment from multiple vendors for extended periods, maintaining access in one instance for over three years.

A hallmark of this campaign is the use of living-off-the-land (LOTL) techniques on network devices. It is important to note that while the telecommunications industry is the primary victim, the advice contained herein is relevant to, and should be considered by, all infrastructure defenders.

No new Cisco vulnerabilities were discovered during this campaign. While there have been some reports that Salt Typhoon is abusing three other known Cisco vulnerabilities, we have not identified any evidence to confirm these claims. The vulnerabilities in question are listed below. Note that each of these CVEs have security fixes available. Threat actors regularly use publicly available malicious tooling to exploit these vulnerabilities, making patching of these vulnerabilities imperative.

Therefore, our recommendation — which is consistent with our standard guidance independent of this particular case—is always to follow best practices to secure network infrastructure.

- CVE-2018-0171 - Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability (Last Updated: 15-Dec-2022)
- CVE-2023-20198, CVE-2023-20273 - Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature (Last Updated: 1-Nov-2023)
- CVE-2024-20399 - Cisco NX-OS Software CLI Command Injection Vulnerability (Last Updated: 17-Sep-2024)

Activities observed

Credential use and expansion

The use of valid, stolen credentials has been observed throughout this campaign, though it is unknown at this time exactly how the initial credentials in all cases were obtained by the threat actor. We have observed the threat actor actively attempting to acquire additional credentials by obtaining network device configurations and deciphering local accounts with weak password types—a security configuration that allows users to store passwords using cryptographically weak methods. In addition, we have observed the threat actor capturing SNMP, TACACS, and RADIUS traffic, including the secret keys used between network devices and TACACS/RADIUS servers. The intent of this traffic capture is almost certainly to enumerate additional credential details for follow-on use.

Configuration exfiltration

In numerous instances, the threat actor exfiltrated device configurations, often over TFTP and/or FTP. These configurations often contained sensitive authentication material, such as SNMP Read/Write (R/W) community strings and local accounts with weak password encryption types in use. The weak encryption password type would allow an attacker to trivially decrypt the password itself offline. In addition to the sensitive authentication material, configurations often contain named interfaces, which might allow an attacker to better understand the upstream and downstream network segments and use this information for additional reconnaissance and subsequent lateral movement within the network.

Infrastructure pivoting

A significant part of this campaign is marked by the actor’s continued movement, or pivoting, through compromised infrastructure. This “machine to machine” pivoting, or “jumping,” is likely conducted for a couple of reasons. First, it allows the threat actor to move within a trusted infrastructure set where network communications might not otherwise be permitted. Additionally, connections from this type of infrastructure are less likely to be flagged as suspicious by network defenders, allowing the threat actor to remain undetected.

The threat actor also pivoted from a compromised device operated by one telecom to target a device in another telecom. We believe that the device associated with the initial telecom was merely used as a hop point and not the intended final target in several instances. Some of these hop points were also used as a first hop for outbound data exfiltration operations. Much of this pivoting included the use of network equipment from a variety of different manufacturers.

Configuration modification

We observed that the threat actor had modified devices' running configurations as well as the subsystems associated with both Bash and Guest Shell. (Guest Shell is a Linux-based virtual environment that runs on Cisco devices and allows users to execute Linux commands and utilities, including Bash.)

Running configuration modifications

- AAA/TACACS+ server modification (server IP address change)
- Loopback interface IP address modifications
- GRE tunnel creation and use
- Creation of unexpected local accounts
- ACL modifications
- SNMP community string modifications
- HTTP/HTTPS server modifications on both standard and non-standard ports

Shell access modifications

- Guest Shell enable and disable commands
- Started SSH alternate servers on high ports for persistent access, such as sshd_operns (on port 57722) on underlying Linux Shell or Guest Shell
    - /usr/bin/sshd -p X
- Created Linux-level users (modification of "/etc/shadow" and "/etc/passwd")
- Added SSH "authorized_keys" under root or other users at Linux level

Packet capture

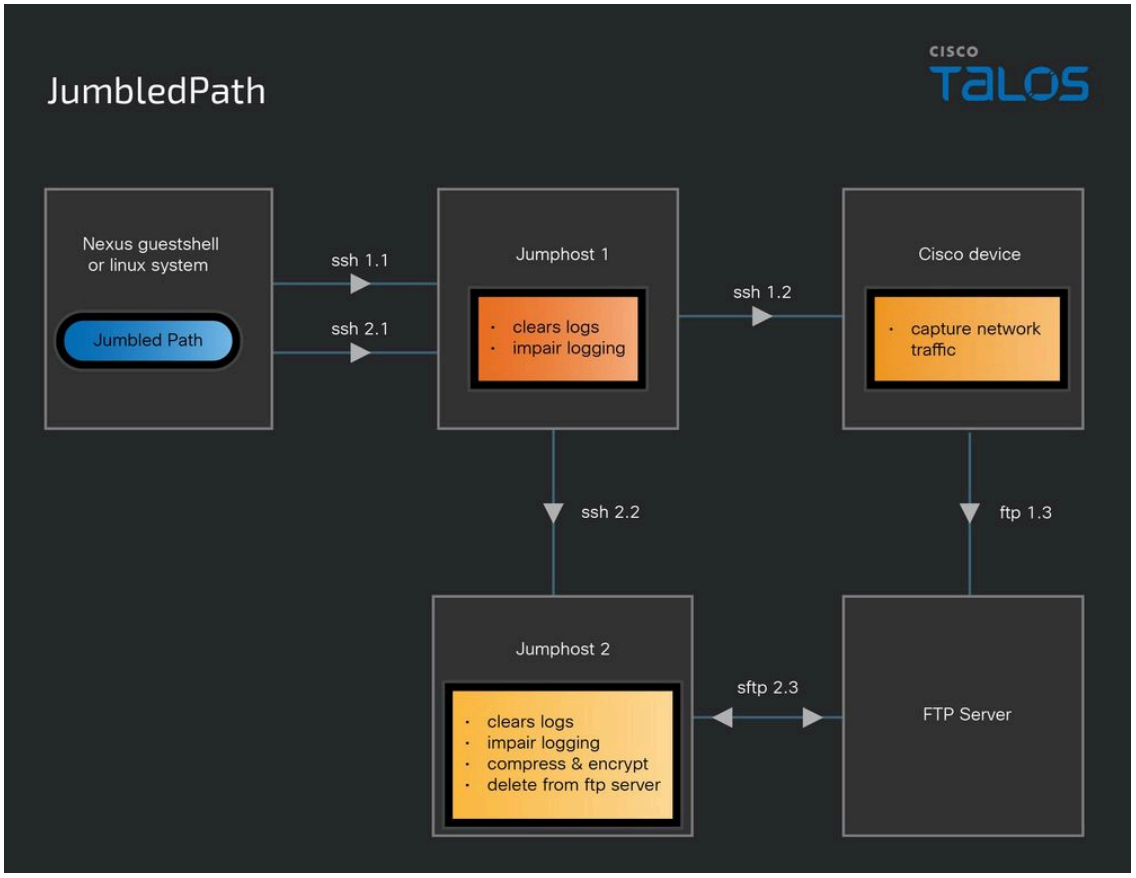
The threat actor used a variety of tools and techniques to capture packet data throughout the course of the campaign, listed below:

- Tcpdump – Portable command-line utility used to capture packet data at the underlying operating system level.
    - Tcpdump –i
- Tpacap – Cisco IOS XR command line utility used to capture packets being sent to or from a given interface via netio at the underlying operating system level.
    - Tpacap –i
- Embedded Packet Capture (EPC) - Cisco IOS feature that allows the capture and export of packet capture data.
    - Monitor capture CAP export ftp://<ftp_server>

- Monitor capture CAP start
- Monitor capture CAP clear

Operational utility (JumbledPath)

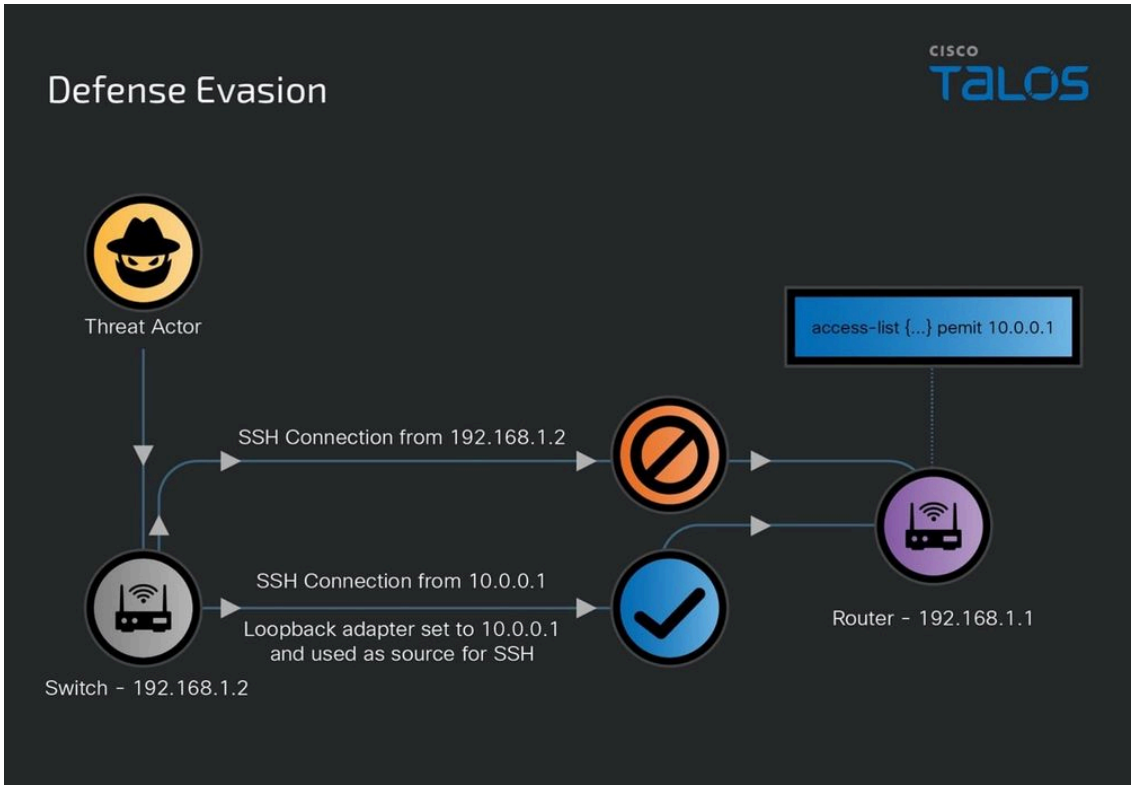
The threat actor used a custom-built utility, dubbed JumbledPath, which allowed them to execute a packet capture on a remote Cisco device through an actor-defined jump-host. This tool also attempted to clear logs and impair logging along the jump-path and return the resultant compressed, encrypted capture via another unique series of actor-defined connections or jumps. This allowed the threat actor to create a chain of connections and perform the capture on a remote device. The use of this utility would help to obfuscate the original source, and ultimate destination, of the request and would also allow its operator to move through potentially otherwise non-publicly-reachable (or routable) devices or infrastructure.



This utility was written in GO and compiled as an ELF binary using an x86-64 architecture. Compiling the utility using this architecture makes it widely useable across Linux operating systems, which also includes a variety of multi-vendor network devices. This utility was found in actor configured Guestshell instances on Cisco Nexus devices.

Defense evasion

The threat actor repeatedly modified the address of the loopback interface on a compromised switch and used that interface as the source of SSH connections to additional devices within the target environment, allowing them to effectively bypass access control lists (ACLs) in place on those devices (see "Infrastructure pivoting" section).



The threat actor routinely cleared relevant logs, including .bash_history, auth.log, lastlog, wtmp, and btmp, where applicable, to obfuscate their activities. Shell access was restored to a normal state in many cases through the use of the “guestshell disable” command.

The threat actor modified authentication, authorization, and accounting (AAA) server settings with supplemental addresses under their control to bypass access control systems.

Detection

We recommend taking the following steps to identify suspicious activity that may be related to this campaign:

- Conduct comprehensive configuration management (inclusive of auditing), in line with best practices.
- Conduct comprehensive authentication/authorization/command issuance monitoring.
- Monitor syslog and AAA logs for unusual activity, including a decrease in normal logging events, or a gap in logged activity.
- Monitor your environment for unusual changes in behavior or configuration.
- Profile (fingerprint via NetFlow and port scanning) network devices for a shift in surface view, including new ports opening/closing and traffic to/from (not traversing).
- Where possible, develop NetFlow visibility to identify unusual volumetric changes.
- Look for non-empty or unusually large .bash_history files.
- Additional identification and detection can be performed using the Cisco forensic guides.

Preventative measures

The following guidance applies to entities in all sectors.

- **Cisco-specific measures**
    - Leverage Cisco Hardening Guides when configuring devices
    - Always disable the underlying non-encrypted web server using the “no ip http server” command. If web management is not required, disable all of the underlying web servers using “no ip http server” and “no ip http secure-server" commands.
    - Disable telnet and ensure it is not available on any of the Virtual Teletype (VTY) lines on Cisco devices by configuring all VTY stanzas with “transport input ssh” and “transport output none”.
    - If not required, disable the guestshell access using “guestshell disable” for those versions which support the guestshell service.
    - Disable Cisco’s Smart Install service using “no vstack”.
    - Utilize type 8 passwords for local account credential configuration.
    - Use type 6 for TACACS+ key configuration.
- **General measures**
    - Rigorously adhere to security best practices, including updating, access controls, user education, and network segmentation.
    - Stay up-to-date on security advisories from the U.S. government and industry, and consider suggested configuration changes to mitigate described issues.
    - Update devices as aggressively as possible. This includes patching current hardware and software against known vulnerabilities and replacing end-of-life hardware and software.
        - Select complex passwords and community strings and avoid default credentials.
    - Use multi-factor authentication (MFA).
    - Encrypt all monitoring and configuration traffic (SNMPv3, HTTPS, SSH, NETCONF, RESTCONF).
    - Lockdown and aggressively monitor credential systems, such as TACACS+ and any jump hosts.
    - Utilize AAA to deny configuration modifications of key device protections (e.g., local accounts, TACACS+, RADIUS).
    - Prevent and monitor for exposure of administrative or unusual interfaces (e.g., SNMP, SSH, HTTP(s)).
    - Disable all non-encrypted web management capabilities.
    - Verify existence and correctness of access control lists for all management protocols (e.g., SNMP, SSH, Netconf, etc.).
    - Enhance overall credential and password management practices with stronger keys and/or encryption.
        - Use type 8 passwords for local account credential configuration.
        - Use type 6 for TACACS+ key configuration.
    - Store configurations centrally and push to devices. Do NOT allow devices to be the trusted source of truth for their configurations.

There are several reasons to believe this activity is being carried out by a highly sophisticated, well-funded threat actor, including the targeted nature of this campaign, the deep levels of developed access into victim networks, and the threat actor’s extensive technical knowledge. Furthermore, the long timeline of this campaign suggests a high degree of coordination, planning, and patience—standard hallmarks of advanced persistent threat (APT) and state-sponsored actors.

During this investigation, we also observed additional pervasive targeting of Cisco devices with exposed Smart Install (SMI) and the subsequent abuse of CVE-2018-0171, a vulnerability in the Smart Install feature of Cisco IOS and Cisco IOS XE software. This activity appears to be unrelated to the Salt Typhoon operations, and we have not yet been able to attribute it to a specific actor. The IP addresses provided as observables below are associated with this potentially unrelated SMI activity.

Legacy devices with known vulnerabilities, such as Smart Install (CVE-2018-0171), should be patched or decommissioned if no longer in use. Even if the device is a non-critical device, or carries no traffic, it may be used as an entry door for the threat actor to pivot to other more critical devices.

The findings in this blog represent Cisco Talos' understanding of the attacks outlined herein. This campaign and its impact are still being researched, and the situation continues to evolve. As such, this post may be updated at any time to reflect new findings or adjustments to assessments.

Indicators of Compromise (IOCs)

IP Addresses:

(Smart Install Abuse not associated with Salt Typhoon)

185[.]141[.]24[.]28

185[.]82[.]200[.]181

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