مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Cyber Espionage Targeting Networks Worldwide

Tracking #:432317652

Date:29-08-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Chinese Advanced Persistent Threat (APT) actors have conducted widespread, persistent cyber espionage campaigns since at least 2021, targeting global networks telecommunications, government, transportation, lodging, and military infrastructure.

## TECHNICAL DETAILS:

Chinese Advanced Persistent Threat (APT) actors have conducted widespread, persistent cyber espionage campaigns since at least 2021, targeting global networks—telecommunications, government, transportation, lodging, and military infrastructure. These actors focus on backbone and edge routers but also pivot into other network segments using compromised devices and trusted connections. Their tactics include exploiting network device vulnerabilities, establishing persistent access, collecting sensitive data, and exfiltrating information via covert channels, sometimes leveraging custom tools and novel protocols. Their activities impact the United States, Australia, Canada, New Zealand, the United Kingdom, and several other countries globally.

**Exploited CVEs:**
The following vulnerabilities have been actively exploited:

- CVE-2024-21887 Ivanti Connect Secure Command injection, chained after CVE-2023-46805
- CVE-2024-3400 Palo Alto PAN-OS Arbitrary file creation; enables RCE on firewalls (GlobalProtect)
- CVE-2023-20273 Cisco IOS XE Command injection/privilege escalation (chained w/CVE-2023-20198)
- CVE-2023-20198 Cisco IOS XE Authentication bypass—creates admin accounts
- CVE-2018-0171 Cisco IOS/IOS XE Smart Install remote code execution vulnerability

**Tactics, Techniques, and Procedures (TTPs)**

- Initial Access: Exploit public-facing CVEs, leverage trusted relationships between providers for lateral movement.
- Persistence: Modify ACLs, open/abuse non-standard ports (SSH/SFTP/HTTP), create local accounts, deploy persistent containers (e.g., Cisco Guest Shell), manipulate SNMP configurations, and establish tunnels (GRE, IPsec).
- Defense Evasion: Obfuscate commands, clear logs, disable or modify logging, use double encoding, delete artifacts, and abuse hosting features.
- Data Collection and Exfiltration: Collect and exfiltrate network captures (PCAP), redirect authentication servers, manipulate AAA, utilize custom SFTP clients, and leverage multi-hop proxies/tools for C2 and data transfer.

**Indicators of Compromise (IOCs)**

**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.
**It is recommended 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**

| IP Address | IP Address | IP Address | IP Address |
|---|---|---|---|
| 1.222.84[.]29 | 167.88.173[.]252 | 37.120.239[.]52 | 45.61.159[.]25 |
| 103.168.91[.]231 | 167.88.173[.]58 | 38.71.99[.]145 | 45.61.165[.]157 |
| 103.199.17[.]238 | 167.88.175[.]175 | 43.254.132[.]118 | 5.181.132[.]95 |
| 103.253.40[.]199 | 167.88.175[.]231 | 45.125.64[.]195 | 59.148.233[.]250 |
| 103.7.58[.]162 | 172.86.101[.]123 | 45.125.67[.]144 | 61.19.148[.]66 |
| 104.194.129[.]137 | 172.86.102[.]83 | 45.125.67[.]226 | 63.141.234[.]109 |
| 104.194.147[.]15 | 172.86.106[.]15 | 45.146.120[.]210 | 63.245.1[.]13 |
| 104.194.150[.]26 | 172.86.106[.]234 | 45.146.120[.]213 | 63.245.1[.]34 |
| 104.194.153[.]181 | 172.86.106[.]39 | 45.59.118[.]136 | 74.48.78[.]66 |
| 104.194.154[.]150 | 172.86.108[.]11 | 45.59.120[.]171 | 74.48.78[.]116 |
| 104.194.154[.]222 | 172.86.124[.]235 | 45.61.128[.]29 | 74.48.84[.]119 |
| 107.189.15[.]206 | 172.86.65[.]145 | 45.61.132[.]125 | 85.195.89[.]94 |
| 14.143.247[.]202 | 172.86.70[.]73 | 45.61.133[.]157 | 89.117.1[.]147 |
| 142.171.227[.]16 | 172.86.80[.]15 | 45.61.133[.]31 | 89.117.2[.]39 |
| 144.172.76[.]213 | 190.131.194[.]90 | 45.61.133[.]61 | 89.41.26[.]142 |
| 144.172.79[.]4 | 193.239.86[.]132 | 45.61.133[.]77 | 91.231.186[.]227 |
| 146.70.24[.]144 | 193.239.86[.]146 | 45.61.133[.]79 | 91.245.253[.]99 |
| 146.70.79[.]68 | 193.43.104[.]185 | 45.61.134[.]134 | 2001:41d0:700:65dc:f656929f |
| 146.70.79[.]78 | 193.56.255[.]209 | 45.61.134[.]22 | 2a10:1fc0:7::f19c[:]39b3 |
| 146.70.79[.]81 | 193.56.255[.]210 | 45.61.134[.]223 | |
| 164.82.20[.]53 | 212.236.17[.]237 | 45.61.149[.]200 | |
| 167.88.164[.]166 | 23.227.196[.]22 | 45.61.149[.]62 | |
| 167.88.172[.]70 | 23.227.199[.]77 | 45.61.151[.]12 | |
| 167.88.173[.]158 | 23.227.202[.]253 | 45.61.154[.]130 | |

**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 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.

**File Name cmd3**

| | |
|---|---|
| MD5 Hash | eba9ae70d1b22de67b0eba160a6762d8 |
| SHA 256 Hash | 8b448f47e36909f3a921b4ff803cf3a61985d8a10f0fe594b405b92ed0fc 21f1 |

**File Name cmd1**

| | |
|---|---|
| MD5 Hash | 33e692f435d6cf3c637ba54836c63373 |
| SHA 256 Hash | f2bbba1ea0f34b262f158ff31e00d39d89bbc471d04e8fca60a034cabe18 e4f4 |

## RECOMMENDATIONS:

- Patch all network edge devices for listed CVEs and review vulnerability status against the Known Exploited Vulnerabilities Catalog.
- Audit device configurations and logs for unauthorized changes: suspicious ACLs, virtual

containers, unexpected tunnels, external TACACS+/RADIUS servers, and capture/mirroring commands.

- Change all default credentials, especially for networking equipment and SNMP community strings, enforce strong cryptography (Type 8/Type 6 for Cisco), and remove weak/deprecated password storage schemes.
- Isolate management networks (dedicated out-of-band management VRF), block unnecessary egress, restrict inbound access to management IPs.
- Enforce logging and auditing: Send logs securely to central servers, track privileged command usage, and retain logs per regulatory standards.
- Monitor for custom SFTP clients and use provided Yara rules for detection.
- Disable unused services and ports; only allow encrypted/authenticated protocols (SSH/SFTP/HTTPS), disable Telnet/FTP/HTTP where possible.
- Restrict and audit SNMP access, enforce SNMPv3, update community strings frequently, monitor SNMP SET operations, and limit write access.
- Harden VPNs, configure strong cryptographic policies, review IKE and Diffie-Hellman group settings, and eliminate unused/default configurations.
- Disable Cisco Smart Install and centralized management features not needed; monitor for unexpected Guest Shell activity and restrict container enablement commands to authorized roles.
- Protect against lateral movement by restricting device-to-device logins and monitoring internal FTP/TFTP usage.
- Perform regular integrity checks of device firmware and storage, comparing hashes against vendor databases.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://www.cisa.gov/sites/default/files/2025-08/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf