cyberthint

We know what they know about you!

THREAT ACTOR PROFILE · APT-CLASS

SALT TYPHOON

THE GLOBAL THREAT LANDSCAPE, TTPS, AND REGIONAL IMPACT

A long-form intelligence assessment of one of the most active state-aligned espionage clusters of 2025–2026: tradecraft, infrastructure, victimology, and defensive guidance from the Cyberthint research team.

Cyberthint — Unified CTI & DRP Platform

Table of Contents

THREAT LEVEL	TRUST LEVEL	TLP
CRITICAL	HIGH	CLEAR

CHAPTER 01

01 Executive Summary

Salt Typhoon is an advanced persistent threat (APT) group that has been active since at least 2019 and is strongly linked to the Ministry of State Security (MSS) of the People's Republic of China.

Having taken center stage on the U.S. national security agenda since 2024, this group has emerged as a threat actor that, as of 2026, has compromised over 200 organizations in more than 80 countries and deeply infiltrated the global telecommunications infrastructure. A distinctive feature of Salt Typhoon is its ability to gain deep access to the telecommunications backbone by targeting internet-facing infrastructure specifically edge network devices such as Cisco IOS XE, Ivanti Connect Secure, and Palo Alto PAN-OS rather than relying on traditional malware-based attacks.

Through this, it has accessed legal wiretapping systems under the CALEA, telephone records of high-level government officials, and private communications. Despite the U.S. Treasury’s January 2025 sanctions, the CISA/NSA/FBI’s August 2025 joint advisory, and international law enforcement operations, the group has increased its operational pace as of 2026.

RISK MATRIX

Multidimensional Assessment

Size	Level	Reason
Feasibility	HIGH	The group is still active, has extensive resources, and its target list is growing
Level of Impact	CRITICAL	Access to the telecommunications backbone is at the national security level
Industry Risk	CRITICAL / HIGH	For telecommunications, ISPs, government, defense, and IT service providers
Geo Distribution	EXPANDING	Rapid expansion from the U.S. to Europe, the MENA region, and the Asia-Pacific

> The threat group is a classic example of a stealthy APT: it operates quietly and patiently, remaining undetected on the network for years, yet exerts strategic influence at the state level through the data it obtains.

CHAPTER 02

02 Actor Profile

Salt Typhoon has been documented under various names within the vendor ecosystem. The table below summarizes all major naming conventions in the industry:

Vendor	Naming
Microsoft	Salt Typhoon
Trend Micro	Earth Estries
Kaspersky	GhostEmperor
ESET	FamousSparrow
Mandiant	UNC2286 · UNC5807
Recorded Future	RedMike
CISA (2025+)	OPERATOR PANDA

ACTOR PROFILE

Key Qualifications

ORIGIN AND REFERENCE
People's Republic of China Ministry of State Security (MSS)

DATE IT BECAME ACTIVE
Active since at least 2019; accelerated pace from 2024 to 2026

MOTIVATION
Cyber espionage, long-term intelligence gathering

MITRE GROUP ID
G1045 - An official MITRE ATT&CK entry is available

SANCTIONS STATUS
January 2025 - U.S. Treasury sanctions (including Sichuan Juxinhe)

TARGET GEOGRAPHY
Over 80 countries. United States, Canada, United Kingdom, Netherlands, Italy, Singapore

Affiliated Companies: Sichuan Juxinhe Network Technology · Beijing Huanyu Tianqiong Information Technology · Sichuan Zhixin Ruijie Network Technology (explicitly designated by the U.S. Treasury).

CHAPTER 03

03 Tactics, Techniques, and Procedures

3.1 Initial Access Vectors

Salt Typhoon primarily exploits known vulnerabilities (N-day) in internet-facing network devices to gain initial access. The group generally does not require zero-day vulnerabilities; unpatched VPN devices, firewalls, and routers serve as the primary entry points.

CVE	Affected Product	Vulnerability Type
CVE-2018-0171	Cisco Smart Install	Remote code execution
CVE-2021-26855	Microsoft Exchange (ProxyLogon)	SSRF / identity spoofing
CVE-2023-20198	Cisco IOS XE Web UI	Privilege escalation (CVSS 10.0)
CVE-2023-20273	Cisco IOS XE Web UI	Command injection
CVE-2023-46805	Ivanti Connect Secure	Bypassing identity verification
CVE-2024-21887	Ivanti Connect Secure	Command injection
CVE-2024-3400	Palo Alto PAN-OS GlobalProtect	Command injection
CVE-2023-48788	Fortinet FortiClientEMS	SQL injection
CVE-2024-12356	BeyondTrust PRA / RS	Command injection
CVE-2024-12686	BeyondTrust PRA / RS	OS command injection

3.2 Command-and-Control and Signature Techniques

Salt Typhoon’s signature technique involves remotely intercepting packets via a jump host specified by the attacker using a custom Go program called JumbledPath. The intercepted traffic is compressed, encrypted, and routed through multiple hops to cover its tracks. This approach conceals both the original source and the final destination.

It has been documented that in campaigns reported in February 2026, the group used a technique to conceal its C2 traffic within Google Sheets APIs, making it invisible behind legitimate cloud services. Additionally, SoftEther VPN is actively used to create a legitimate appearance.

> Cisco Talos has documented that a group remained undetected within a victim’s telecommunications network for three years. This case highlights that traditional EDR and perimeter security controls are insufficient on their own.

3.3 MITRE ATT&CK TTP Mapping

Tactic	TTP	Technique Name	Observed Behaviour
Initial Access	T1190	Exploit Public-Facing App	Exploitation of Cisco IOS XE, Ivanti, PAN-OS
Initial Access	T1566.001	Spearphishing Attachment	Spear-phishing emails
Persistence	T1505.003	Web Shell	Deployment of customized web shells
Persistence	T1543	Create System Service	Device-level service creation (router persistence)
Defense Evasion	T1070.004	File Deletion	Log deletion, audit trail clearing
Defense Evasion	T1027	Obfuscated Files	Encrypted packet capture, multi-hop jump-host
Defense Evasion	T1562.001	Impair Defenses	ACL bypass via loopback IP assignment
Credential Access	T1040	Network Sniffing	SNMP, TACACS+, RADIUS traffic sniffing
Credential Access	T1552.001	Credentials in Files	Credential extraction from configuration files
Lateral Movement	T1021	Remote Services	Lateral movement via GRE / IPsec tunnels
Command & Control	T1071	Application Layer Protocol	Multi-hop encrypted C2 via JumbledPath
Command & Control	T1090.003	Multi-hop Proxy	Multi-proxy chaining via SoftEther VPN
Exfiltration	T1041	Exfil Over C2 Channel	Data exfiltration over C2 channel

CHAPTER 04

04 Operational Timeline

The following timeline outlines key milestones in Salt Typhoon's operational evolution from 2019 to the present (May 2026). Each event represents either a leap in the group's operational scale, a tactical evolution, or an international response.

Date	Phase	Event
2019	Inception	Start of Salt Typhoon activity (per Microsoft attribution)
2020-23	Stealth phase	Low-profile espionage in Southeast Asia, Africa, and the Middle East
Oct 2024	Disclosure	WSJ disclosed the U.S. telecom breach. CALEA access confirmed
Nov 2024	Naming	Trend Micro Earth Estries report; Microsoft coins the name "Salt Typhoon"
Jan 2025	Sanctions	U.S. Treasury sanctions; access to Trump/Harris campaign communications revealed
Feb 2025	Talos analysis	Cisco Talos "Weathering the storm" report; JumbledPath documented
Apr 2025	FBI bounty	A USD 10 million bounty announced for individuals linked to Salt Typhoon
Aug 2025	Five Eyes	CISA-NSA-FBI joint advisory AA25-239A published
Sep 2025	Singapore	Four telecom breaches; Operation CYBER GUARDIAN launched
Jan 2026	Congress	U.S. Congressional Committee email systems compromised (FT)
Feb 2026	Norway	Government breach officially confirmed (first EU case)
Feb 2026	42 countries	50+ organization campaign; Google Sheets concealment technique
Mar 2026	Scale	FBI: 200+ companies breached across 80+ countries (TechCrunch)
Apr 2026	Italy	Sistemi Informativi (IBM subsidiary) breach; suspected attribution

CHAPTER 05

05 Known Tools and IOCs

5.1 Documented Tool Inventory

Tool	Type	Function
JumbledPath	Custom tool (Go/ELF)	Remote packet capture, multi-hop jump-host, encrypted transmission, Salt Typhoon's signature tool
GhostSpider	Modular backdoor	Persistent access tailored to telecom networks, different hashes across endpoints
Demodex	Kernel rootkit	Original archive of the GhostEmperor cluster, Windows kernel-level concealment
SnappyBee / Deed RAT	Shared RAT	ShadowPad evolution; tool shared among multiple Chinese APTs
Crowdoor	Backdoor	Associated with FamousSparrow; evolutionary variant of ShadowPad
SoftEther VPN	Legitimate tool (abused)	Used to disguise C2 traffic as legitimate VPN traffic
LOLBins	System utilities	WMIC.exe, PSEXEC.exe, PowerShell, netsh, lateral movement, discovery

5.2 IOC List (Defang Format)

Type	Context	Value
Domain	C2 (SNAPPYBEE)	api[.]solveblemten[.]com
Domain	C2 (SNAPPYBEE)	esh[.]hoovernamosong[.]com
Domain	GHOSTSPIDER	clothworls[.]com
Domain	GHOSTSPIDER	colourtinctem[.]com
Domain	GHOSTSPIDER	dateupdata[.]com
Domain	GHOSTSPIDER	infraredsen[.]com
Domain	GHOSTSPIDER	materialplies[.]com
Domain	GHOSTSPIDER	royalnas[.]com
IPv4	C2 GHOSTSPIDER	141[.]255[.]164[.]98:2096
IPv4	C2 Earth Estries	23[.]81[.]41[.]166
IPv4	C2 SNAPPYBEE	158[.]247[.]222[.]165
VPN	SoftEther endpoint	vpn114240349[.]softether[.]net
Cert	Typosquat - fake!	palloaltonetworks[.]com

CHAPTER 06

06 Defense and Risk Mitigation

6.1 Action Plan by Time Horizon

0-30 DAYS

IMMEDIATE ACTIONS

Inventory scan for the 10 CVEs listed in Section 5.1 · Prioritized patching on edge devices · Disable Cisco Smart Install · Block internet exposure of Web UI management interfaces · Enforce MFA on all administrator accounts

1-3 MONTHS

DETECTION & MONITORING

Continuous monitoring of unauthorized ACL changes · Detection of unexpected GRE/IPsec tunnels · Detection of IP assignments to loopback interfaces · Deployment of NDR solutions · Monitoring of TACACS+ server redirection

3-12 MONTHS

ARCHITECTURAL HARDENING

Adoption of Zero Trust principles · Review of vendor and third-party access · Prohibition of plaintext passwords in configuration files · Secret management solution · Authoring of MITRE G1045 detection rules

12-24 MONTHS

STRATEGIC PREPAREDNESS

Continuous monitoring of CISA AA25-239A and sector ISAC bulletins · Salt Typhoon simulation via Atomic Red Team / Caldera · Telecom backbone scenarios in incident response plans · Dedicated threat-hunting team

CHAPTER 07

07 Latest Developments 2025–2026

FEB 2026

U.S. Senate Crisis

Senator Maria Cantwell requested the Mandiant assessment reports concerning the Salt Typhoon breaches from the CEOs of AT&T and Verizon. The companies refused to share the reports with Congress. Expert witnesses stated that Salt Typhoon may still be active inside U.S. telecom networks.

FEB 2026

FBI E2EE Advisory

The FBI and other federal agencies officially advised U.S. citizens to use only end-to-end encrypted messaging applications (Signal, WhatsApp), an exceptionally rare move in U.S. history.

FEB 2026

Norway Disclosure

The Norwegian National Security Authority (NSM) officially confirmed a Salt Typhoon-attributed breach in government networks. It became the first European government to publicly disclose a Salt Typhoon breach.

FEB 2026

42-Country Campaign

A campaign affecting 50+ telecom and government institutions across 42 countries was reported. Distinctive feature: a novel concealment technique that hides C2 traffic behind Google Sheets APIs.

SEP 2025

Operation CYBER GUARDIAN

Singapore's CSA disclosed that all four major telecom operators had been compromised. The 11-month remediation operation became the largest cyber defense operation in Singapore's history.

SEP 2025

NYT, Nearly Every American

The New York Times published an in-depth investigation: nearly every American's communications data may have been affected. The operation is not targeted but national in scale.

AUG 2025

Five Eyes Joint Advisory

The joint advisory published under the code AA25-239A was co-signed by the United Kingdom, Canada, Australia, and New Zealand alongside the United States. It explicitly named three Chinese companies.

APR 2025

FBI USD 10M Bounty

A bounty of up to USD 10 million was announced for information on individuals linked to Salt Typhoon, one of the highest FBI bounties ever announced for state-sponsored APT operators.

CHAPTER 08

08 Regional Impact: Türkiye and the MENA Region

This section addresses a gap left unfilled in the existing Salt Typhoon literature. All major published vendor reports adopt a U.S.-centric perspective; no comprehensive analysis exists that assesses the group's strategic significance for Türkiye, NATO's southeastern flank, and the MENA region.

8.1 Documented Attacks Against NATO Members

Country	Date	Target Hit
USA	Oct 2024+	9 major telecoms, National Guard, Congress, Treasury
Canada	Feb 2025+	Multiple telecom operators (via Cisco IOS XE)
Netherlands	2025	Government networks
Norway	Feb 2026	Government networks (first formal EU confirmation)
Italy	Apr 2026	Sistemi Informativi (IBM subsidiary), suspected
UK	2024-2025	British telecom subsidiaries

8.2 Türkiye Exposure Matrix

Critical Asset Category	Counterpart in Türkiye	Exposure
Telecom backbone	Türk Telekom, Turkcell, Vodafone Türkiye	HIGH
Cisco IOS XE fleet	Telecom and ISP infrastructure	HIGH
BTK lawful intercept	CALEA-equivalent lawful intercept infrastructure	HIGH
Public-sector IT	e-Government, public cloud, defense contractors	MEDIUM-HIGH
Military / Diplomatic	Ministry of Defense, MFA, NATO task forces	HIGH
Hospitality / Transport	Turkish Airlines, hotels, logistics	MEDIUM

> ***Central proposition:*** There is no concrete open-source evidence that Salt Typhoon has yet targeted Türkiye. However, when the group's geopolitical motivations, target profile, and the structural characteristics of Turkish telecom infrastructure are considered together, it is unlikely that Türkiye is absent from its medium-term target matrix.

CHAPTER 09

09 Typhoon Family Comparison

Microsoft's "Typhoon" surname taxonomy for China linked APTs has become a de facto industry standard. Understanding Salt Typhoon correctly requires a comparative review of this family.

Attribute	Salt Typhoon	Volt Typhoon	Flax Typhoon
Primary Target	Telecom backbone, ISPs	Critical infrastructure	Taiwan,government,academia
Main Objective	Espionage, wiretap access	Pre-positioning	Intelligence, operational network
Primary Vector	Cisco/Ivanti/PAN-OS edge	SOHO router botnet, LotL	Public facing VPN, servers
Signature Technique	JumbledPath, backbone sniffing	KV-Botnet (SOHO devices)	China Chopper, SoftEther
Dwell Time	3+ years documented	Years (silent access)	Years (Taiwanese institutions)
Attributed Unit	MSS (intelligence)	MSS / PLA (military)	MSS / Integrity Tech
Official Sanctions	Jan 2025 (USA)	None (yet)	Sep 2024 (FBI takedown)

9.1 Typological Positioning

Salt Typhoon, Espionage Arm

Access to lawful intercept systems · Targeting of senior political figures · Multi-year dwell time · First Typhoon subjected to formal sanctions.

Volt Typhoon, Operational Preparation

Not espionage, but pre-positioning the capability to cause disruption in the event of a future conflict. Uses thousands of SOHO devices as proxies via the KV-Botnet.

Flax Typhoon, Regional Intelligence

A more regionally focused actor targeting the Taiwanese government, academia, and private sector. In September 2024, the FBI dismantled its Raptor Train botnet (260K+ devices).

CHAPTER 10

10 Future Forecasts

10.1 Geographic Expansion Forecasts

HIGH	Eastern Mediterranean and Black Sea basin (Türkiye, Greece, Romania, Bulgaria), a natural continuation of the NATO expansion pattern
HIGH	Gulf states (UAE, Saudi Arabia), intelligence demand paralleling China's economic footprint in the Middle East
MEDIUM	Latin America (Brazil, Mexico), expansion into a new operational geography
LOW	Decline of U.S. focus, sanctions are not a deterrent; on the contrary, motivation to entrench further may increase

10.2 Tactical Evolution Forecasts

- **AI-assisted Evasion:** LLM-generated legitimate-looking content used to disguise C2 traffic
- **Cloud-based C2 Expansion:** Google Sheets was successful, OneDrive, Discord, and GitHub will also be targeted
- **New Edge Device Targets:** 5G core network, OT/ICS gateways, IoT/IIoT management platforms
- **Supply-chain Attacks:** MSP/MSSP targeting will increase (Sistemi Informativi model)
- **"Harvest now, decrypt later":** Stockpiling encrypted communications for future quantum-assisted decryption

10.3 Conclusion

As of 2026, Salt Typhoon is positioned as one of the most structurally entrenched, strategically impactful, and long-lived actors in the global cyber threat landscape. Effective defense requires a combination of threat intelligence, digital risk protection, active patch management, edge device visibility, NDR deployment, Zero Trust architecture, and supply chain security.

> Critical observation areas for the next 12-24 months: ***(a)*** how far European government breaches will spread through the door Norway opened, ***(b)*** in which MENA countries the density of Chinese APT activity will be documented, ***(c)*** whether the exposure of Eastern Mediterranean countries, including Türkiye, will become public, ***(d)*** assessment of the effectiveness of sanctions regimes.

CHAPTER 11

11 Our Solution

Cyberthint provides a layered defense model for organizations exposed to Salt Typhoon and similar state-aligned APT campaigns:

1. Continuous threat intelligence feed covering Salt Typhoon infrastructure rotation, fresh IOCs, and CISA grade advisories delivered in real time.

2. External attack surface monitoring against Cisco IOS XE, Ivanti, PAN-OS, Fortinet, and BeyondTrust exposures, mapped to the CVE list in Section 3.1.

3. Dark web tracking of telecom credentials, leaked operator data, and underground forum mentions tied to your industry and region.

4. Ready-to-deploy detection rules mapped to MITRE ATT&CK G1045, covering JumbledPath, loopback IP anomalies, and Google Sheets C2 abuse.

5. Tabletop exercises and Atomic Red Team simulations modeling Salt Typhoon scenarios for telecom operators, ISPs, and IT service providers.

6. Regional intelligence context for Türkiye, MENA, and the Eastern Mediterranean, including ongoing assessment of geopolitical exposure factors.