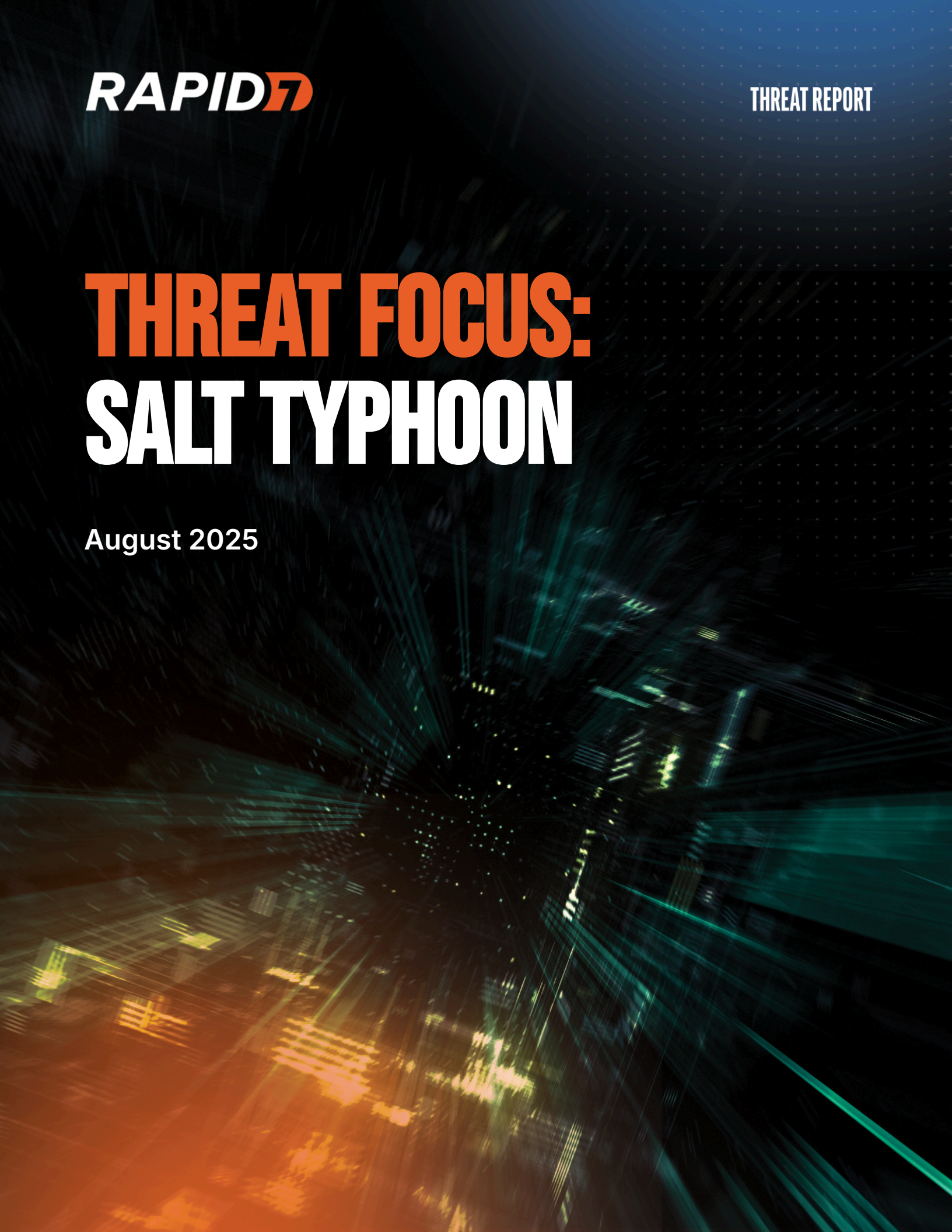
RAPID7

THREAT REPORT

# THREAT FOCUS: SALT TYPHOON

August 2025



# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

This report presents an in-depth investigation into the threat actor known as **Salt Typhoon**. Salt Typhoon is a highly sophisticated Chinese state-sponsored cyber threat actor (APT) known for its stealthy, long-term espionage operations against critical infrastructure. Active since around 2020, Salt Typhoon (also tracked as Earth Estries, GhostEmperor, FamousSparrow, and UNC2286 by various security firms) is linked to China's Ministry of State Security (MSS).

The group has aggressively targeted telecommunications carriers, government networks, and other strategic sectors across the United States, Asia-Pacific, Europe, the Middle East, and Africa. Major intrusions between 2020 and 2025 include breaches of at least eight U.S. telecom companies – enabling the recording of sensitive phone calls – and the extensive compromise of a U.S. state Army National Guard network.

Salt Typhoon's tactics are advanced and persistent. The group gains initial access by exploiting unpatched internet-facing systems (e.g. VPN appliances, firewalls, email servers), then deploys custom malware (like the Demodex kernel rootkit and backdoors such as SparrowDoor and GhostSpider) alongside "living off the land" tools (PsExec, WMI, PowerShell).

They achieve deep persistence and move laterally through networks while evading detection via anti-forensic techniques and stealthy command-and-control (C2) channels (often over HTTPS).

Their operations focus on intelligence collection – for example, siphoning call records, geolocation data, credentials, and sensitive communications – with an eye toward both espionage and potential prepositioning for disruptive cyberattacks in a future conflict.
This report profiles Salt Typhoon's origin and affiliations, motivations and targets, a timeline of key campaigns (2020–2025), and a detailed breakdown of tactics, techniques, and procedures aligned with the MITRE ATT&CK® framework. Each phase of the adversary lifecycle – Initial Access through Exfiltration – is examined to illustrate how Salt Typhoon operates at every step. We also highlight notable tools and malware in the group's arsenal and summarize insights of leaked Salt Typhoon data. Finally, we assess the threat's impact and provide

practical defense recommendations tailored for telecommunications providers, government networks, and enterprises to counter this persistent threat.

# METHODOLOGY

The research results contained in this report are a combination of several methodologies: Rapid7 proprietary investigation tools, analysts, open-source intelligence (OSINT) search tools, and deep and dark web searches.

# INTRODUCTION

Salt Typhoon is a code name designated by Microsoft for a Chinese advanced persistent threat group as part of Microsoft's weather-themed naming convention for nation-state actors. The group emerged in the early 2020s as a prolific cyber-espionage actor, though evidence suggests it may have operated in some form since at least 2019. Over the past several years, Salt Typhoon has conducted a sweeping campaign of intrusions into high-value targets, primarily in the communications and government sectors. These intrusions were initially discovered and reported under different aliases by various cybersecurity organizations: for example, GhostEmperor (named by Kaspersky in 2021) targeted Southeast Asian government and telecom entities with a novel kernel rootkit, and FamousSparrow (named by ESET in 2021) spied on hotels and governments worldwide by exploiting Microsoft Exchange vulnerabilities. In late 2024, the U.S. government publicly linked these and other operations to a single threat actor "Salt Typhoon," attributing the activity to a Chinese state-sponsored campaign.

# ORIGIN, AFFILIATES AND ALIASSES

Security authorities attribute Salt Typhoon to the People's Republic of China, likely operating under or in close coordination with the Ministry of State Security (MSS), China's civilian intelligence agency. The group's activities and targets align with Chinese state interests, and U.S. officials have described Salt Typhoon as an MSS-linked actor conducting espionage and potential pre-attack reconnaissance on U.S. networks. There is significant evidence that

Salt Typhoon is not a lone hacker crew but a highly organized cluster of multiple teams, possibly operating as or through contractors in China's cybersecurity apparatus.

A January 2025 U.S. Treasury sanction identified a China-based network security company, Sichuan Juxinhe Network Technology, as directly involved in Salt Typhoon's operations. Researchers believe this company and others function as front organizations for MSS hacking activities, indicating Salt Typhoon may be structured as an MSS-directed "hack-for-hire" operation composed of distinct sub-teams.

Indeed, leaked data from a Salt Typhoon contractor in mid-2025 appears to confirm this structure. According to a SpyCloud investigation, a data leak offered on a Dark Web forum included internal files from Salt Typhoon's operators – such as employee rosters, router configuration files from compromised devices, and even spreadsheets of transactions for "hacking services" sold to Chinese government customers. The records pointed to two additional shell companies (Beijing Huanyu Tiangiong Information Technology and Sichuan Zhixin Ruijie Network Technology) involved in Salt Typhoon's campaigns. One leaked contract showed these hackers providing technical services to a state-owned enterprise linked to China's military-industrial complex.

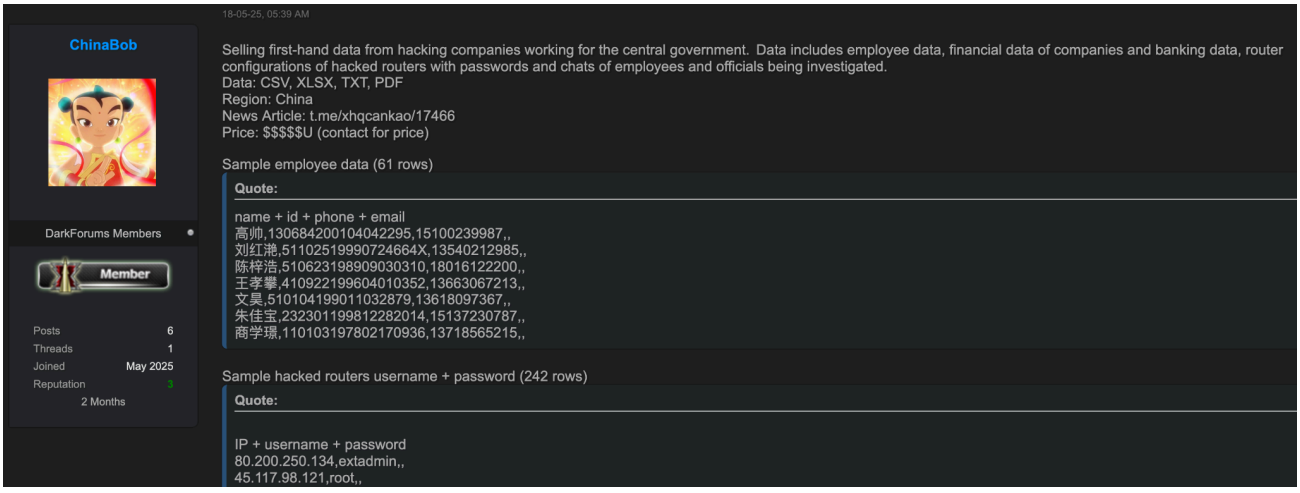



*Figure 1 - ChinaBob's post on DarkForums offering the Salt Typhoon details*

These findings underscore that Salt Typhoon operates within a broader ecosystem of state-sanctioned cyber operators, with close ties to China's intelligence and defense establishment. Salt Typhoon's activities have been tracked under numerous aliases by cybersecurity firms, which initially observed portions of the group's campaign in isolation. GhostEmperor, uncovered by Kaspersky in 2021, described a then-unknown Chinese APT using a Windows kernel rootkit ("Demodex") and advanced techniques to persist on Exchange email servers and other systems.

Earlier, in February 2024, the I-Soon leaks were published on Github with information about customers, similar to what was leaked by "ChinaBob". While comparing them, the I-Soon and Salt Typhoon leaks reveal a deeply interconnected ecosystem of Chinese state cyber operations, involving entities like the MSS, MPS, PLA, and affiliated private contractors. The Institute of Information Engineering (IIE) and PLA Unit 61419 appear in both leaks, illustrating their central roles. Qi'anxin (Legendsec) also bridges both datasets, appearing as a prospective employer in I-Soon's internal chatter and as a data buyer in the Salt Typhoon leak. However, unique entities such as Unit 152, regional government offices, and front companies like Juxinhe and Huanyu Tiangiong appear only in the Salt Typhoon data. This indicates that while I-Soon's leak exposed a single contractor's internal operations, the ChinaBob/Salt Typhoon dump aggregates activity from multiple contractors involved in China's broader hack-for-hire infrastructure.

# MOTIVATIONS, TARGET SECTORS AND GEOGRAPHICAL FOCUS

## Motivations

Salt Typhoon is principally motivated by cyber espionage and strategic intelligence collection. Unlike ransomware gangs or financially driven criminals, Salt Typhoon's operations are aligned with national objectives: stealing sensitive data, monitoring communications, and maintaining covert access in preparation for potential future contingencies. U.S. government officials warn that Salt Typhoon isn't just gathering intelligence but also "prepositioning" itself to disrupt or sabotage critical infrastructure in the event of a conflict involving China.

In other words, beyond spying, the group's long-term persistence in key networks could enable destructive cyber attacks (e.g. disabling communications networks) if geopolitical tensions escalate.

## Target Sectors

Salt Typhoon has predominantly targeted organizations that handle high-value communications and data. Foremost among these are telecommunications providers – especially major mobile carriers and internet backbone firms in the United States. By late 2024, at least eight large U.S. telecom companies were identified as victims.

These intrusions gave Salt Typhoon access to telephone infrastructure and lawful-intercept systems, allowing them to surreptitiously collect call detail records and even record the phone calls of senior U.S. officials and politicians.

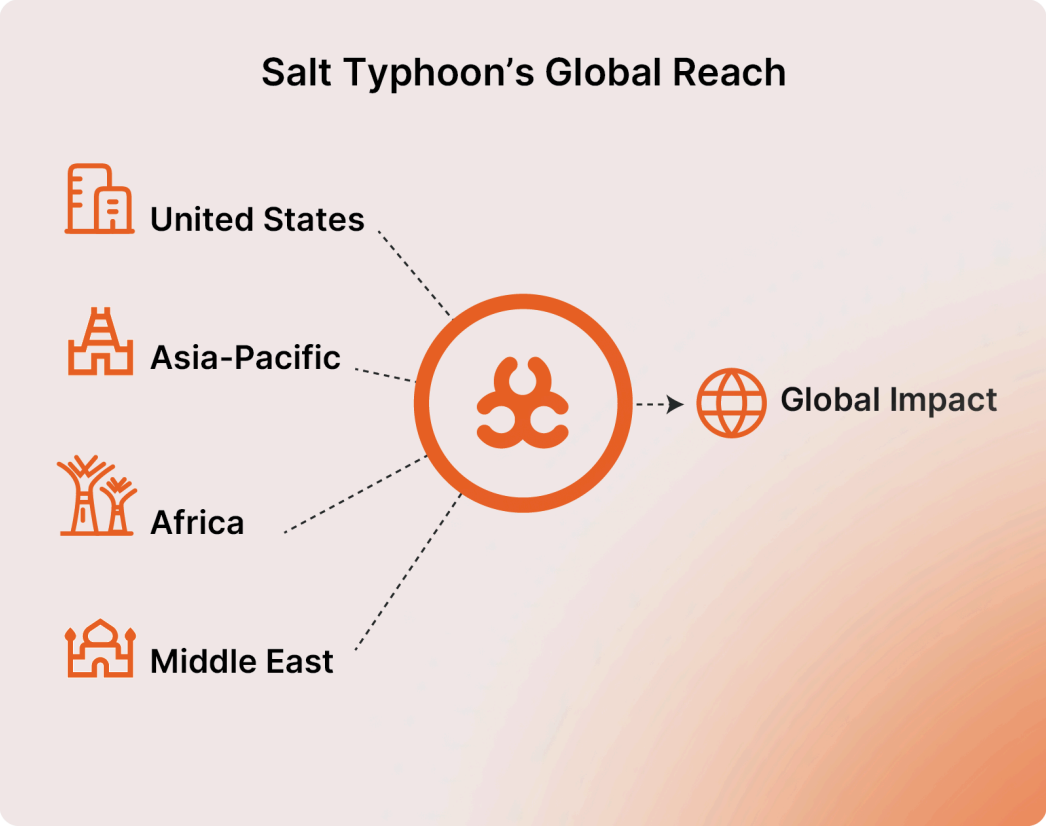
The group has also compromised telecom operators or IT service providers abroad – for example, researchers and news reports have tied Salt Typhoon to breaches in Southeast Asian telecoms, a Canadian satellite internet operator (Viasat) in 2025, and other global communication networks.

Beyond telecoms, Salt Typhoon aggressively targets government and defense networks. This includes military organizations; A notable case is the hack of a U.S. state's Army National Guard network from March to December 2024, where the adversaries obtained administrator credentials, network maps, and data exchanges with Guard units in every U.S. state and several territories. Government agencies (both civil and defense), intelligence and law enforcement units, and even third-party contractors serving government (consulting firms, telecom vendors, etc.) have been breached as part of Salt Typhoon's efforts to gather U.S. intelligence.

Other sectors tied to high-value information have been hit as well. Salt Typhoon compromised organizations across industries such as technology, consulting, chemical, transportation, and even NGOs involved in government work.

Essentially, any sector that could yield strategic intelligence – whether it's travel data on diplomats (hotels), infrastructure schematics (engineering firms), or policy deliberations (think tanks and NGOs) – may fall within Salt Typhoon's scope.

## Geographical Focus




Salt Typhoon's campaign is global but with a concentration on the United States and allied nations. Its operations since 2020 have been observed in at least 13 countries across North America, Asia, Africa, and the Middle East. The United States is a primary target with dozens of U.S. organizations affected, reflecting the group's focus on U.S. governmental and commercial networks.

In Asia-Pacific, victims have appeared in Taiwan, Vietnam, the Philippines, Malaysia, Indonesia, India, Pakistan, and Afghanistan indicating interest in regional governments and telecoms. Several African and Middle Eastern entities (e.g. in South Africa and Eswatini) were also compromised.

This wide reach underscores Salt Typhoon's global espionage mission, though the unifying theme is targeting countries and sectors of strategic relevance to Chinese interests.

# TIMELINE OF ACTIVITIES

| Time Period | Activity |
|---|---|
| **2019-2020** | Early activity, targeting U.S. political figures |
| **2021** | Exploiting Exchange ProxyLogon vulnerabilities |
| **2022** | Maintained persistence, broadened targeting |
| **Early-Mid 2023** | Global espionage campaign, new malware |
| **Late 2024** | U.S. telecom breaches, National Guard compromise |
| **January 2025** | Sanctions and public alerts |
| **April 2025** | FBI bulletin, expanded investigation |
| **May 2025** | Leak of Salt Typhoon data |
| **June-July 2025** | Ongoing intrusions, revelations |

# TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) OVERVIEW

Salt Typhoon employs a broad range of sophisticated tactics and techniques throughout the attack lifecycle, combining custom malware with "living-off-the-land" abuse of legitimate tools. The group is adept at using exploits for initial compromise, stealthy malware for persistence, and built-in network administration tools for lateral movement – all while working to avoid detection. Table 1 provides a high-level alignment of Salt Typhoon's known TTPs with the MITRE ATT&CK framework tactics:

| MITRE ATT&CK Tactic | Techniques Used by Salt Typhoon |
|---|---|
| **Initial Access** | Exploit vulnerable public-facing systems (e.g. VPNs, firewalls, Exchange servers); compromise network edge devices (routers) via zero-day or N-day exploits. |
| **Execution** | In-memory malware execution via multi-stage loaders; use of scripting (PowerShell) and batch scripts for payload deployment; execution through Windows utilities and scheduled tasks. |
| **Persistence** | Install kernel-mode rootkits to maintain stealthy persistence; deploy custom backdoors that start on boot or as services; create new local accounts or maintain stolen VPN credentials for recurrent access. |
| **Privilege Escalation** | Exploit system vulnerabilities for privilege gain (e.g. via DLL sideloading or known Windows privilege escalation flaws); abuse access tokens or credential material to assume higher privileges; use rootkits and driver exploits to gain kernel-level privileges. |
| **Defense Evasion** | Delete or alter logs to cover tracks; employ heavy obfuscation and encryption in malware (Demodex and other implants have multiple layers of encryption/packing); use valid code-signing or known |

| | |
|---|---|
| | benign binaries (LOLBins) to execute malicious payloads; disable security tools or use kernel hooks to blind endpoint defenses. |
| **Credential Access** | Dump credentials from memory using tools like Mimikatz (LSASS process dumping); harvest password hashes/tokens for later reuse (pass-the-hash); steal password files or router config credentials (Salt Typhoon's leaked data showed hundreds of router passwords obtained); keylogging or input capture on compromised servers (as needed to obtain specific credentials). |
| **Discovery** | Reconnaissance of domain trusts and accounts; network scanning and mapping of connected networks and devices; enumerate running services, processes, and security software on penetrated systems; gather info on data repositories (database listings, file shares). |
| **Lateral Movement** | Use of PsExec and SMB/WMI for remote command execution on other hosts; pivot through VPN or RDP using stolen credentials to access additional systems; leverage compromised routers and networking equipment to hop between network segments; deploy malware to multiple systems using enterprise software deployment tools or domain admin access. |
| **Collection** | Identify and collect sensitive data: e.g. database dumps, email archives, telecom call detail records and voice intercepts; copy configuration files, network diagrams, and communications (as seen in the National Guard breach); use utilities like robocopy or custom scripts to gather files of interest; monitor network traffic in real-time via implanted packet capture tools (Salt Typhoon deployed a sniffer backdoor called *"JumbledPath"* to capture data at network choke points). |
| **Command & Control** | Establish encrypted C2 channels using HTTP/HTTPS or custom protocols (e.g. the GhostSpider backdoor uses TLS-encrypted communications); utilize compromised servers or cloud services as relay nodes; employ C2 frameworks like Cobalt Strike with customized beacons; frequently rotate C2 infrastructure and domains to avoid tracking, sometimes using legitimate hosting providers to blend in. |

| | |
|---|---|
| **Exfiltration** | Exfiltrate data over encrypted channels camouflaged as normal traffic (often over HTTPS or DNS); stage collected files in password-protected archives for exfil; upload stolen data to cloud storage services or attacker-controlled servers; in telecom hacks, exfiltrated call recordings and metadata were likely transmitted gradually to avoid detection. |

# TOOLS AND MALWARE USED

Salt Typhoon employs a mix of proprietary malware and repurposed administrative tools to achieve its objectives. Below are some of the notable tools and malware associated with the group:

**Demodex Rootkit:** A kernel-mode rootkit identified with the GhostEmperor activity, used by Salt Typhoon for stealth and persistence. Demodex lodges itself in the Windows kernel to hide processes and files and to help the attackers maintain SYSTEM-level control undetected. It's loaded via an exploit that bypasses driver signature enforcement, indicating the attackers' low-level prowess.

**SparrowDoor Backdoor:** A custom backdoor first publicly linked to the FamousSparrow APT (now considered Salt Typhoon). SparrowDoor provides remote access to infected systems and is typically installed as a Windows service for persistence. It was used to spy on hotel Wi-Fi networks and government systems, supporting capabilities like file transfer, command execution, and surveillance of the target machine.

**GhostSpider Malware:** A multi-module backdoor discovered by Trend Micro in 2024 during Earth Estries (Salt Typhoon) operations. GhostSpider is designed for long-term espionage with a flexible plugin system. It communicates over TLS (HTTPS) to C2, making detection hard. Its presence in Southeast Asian telco attacks shows Salt Typhoon continuously develops new bespoke malware.

**SNAPPYBEE (Deed RAT):** A modular remote access trojan that Salt Typhoon has deployed in some campaigns. SNAPPYBEE can run on multiple systems and is shared among certain Chinese threat groups, indicating a malware-as-a-service origin. It provides spying

functions (like keylogging, screen capture) and has been observed with Salt Typhoon alongside GhostSpider.

**MASOL RAT:** A cross-platform backdoor (Windows/Linux) used by Earth Estries since around 2020. MASOL RAT was seen on Linux servers of Southeast Asian governments, showing Salt Typhoon's ability to also target non-Windows systems. It likely enables command execution and data theft on Linux, giving the group coverage across different OS in a network.

Some of the following tools are what we call "dual usage tools". They can be both used for malicious or legitimate purposes, however the context of how these tools are used in combination with alerts/data is important to decide to investigate or not:

**PsExec:** Not malware per se, but a Microsoft Sysinternals tool heavily used by Salt Typhoon for lateral movement. PsExec allows executing processes on remote Windows machines and is co-opted by the attackers to spread their payloads (earning it a mention in their TTPs). It often appears in their operations to run commands or launch malware on multiple servers from a single controller host.

**WMIC** (Windows Management Instrumentation Command-line): Another legitimate tool abused by Salt Typhoon. WMIC lets administrators (and attackers) execute system management commands on local or remote machines. Salt Typhoon uses WMIC for things like spawning processes remotely, enumerating system info, or even dumping user accounts – all via a native Windows interface that tends not to raise alarms.

**Mimikatz:** A well-known post-exploitation tool for credential dumping, explicitly observed in Salt Typhoon incidents. Mimikatz enables the extraction of plaintext passwords, hashes, Kerberos tickets, etc., from Windows memory. Salt Typhoon uses it to escalate privileges and facilitate lateral movement by acquiring credentials (Domain Admins, etc.) once they have a foothold.

**Cobalt Strike Beacon:** Salt Typhoon has been noted to use Cobalt Strike, a commercial red team framework, to maintain access and control hosts. The Beacon component of Cobalt Strike provides an encrypted C2 channel with flexible configuration (e.g., can mimic web traffic). Using Cobalt Strike allows Salt Typhoon to tap into a powerful toolset (keylogging, credential harvesting, privilege escalation scripts) within one platform.

These tools together illustrate Salt Typhoon's dual approach of custom malware and living-off-the-land. The custom malware (Demodex, GhostSpider, SparrowDoor, etc.) provides deep stealth and tailored capabilities, while the use of common tools (PsExec, WMIC, Mimikatz) allows them to operate within the bounds of normal sysadmin behavior. The presence of widely-used frameworks like Cobalt Strike also suggests Salt Typhoon is not above using publicly available offensive tools to expedite their mission – and to potentially confuse attribution, since many actors use Cobalt Strike.

Salt Typhoon is like any other APT group, continuously evolving its toolset. As of 2025, new malware can emerge (for example, if some of their tools are exposed, they may adopt replacements or upgrades). But the fundamental pattern remains: combine stealthy implants with the target's own system tools to maximize effectiveness.

# THREAT IMPACT AND LONG-TERM RISK

Salt Typhoon's activities pose severe national security and infrastructure risks due to the sensitive nature of the targets and data involved. The immediate impact of the group's cyber-espionage has been the compromise of confidential communications at the highest levels of government and industry. By extracting phone call recordings and metadata of senior officials, Salt Typhoon has potentially given Chinese intelligence deep insight into U.S. leadership's plans, personal communications, and strategies. Such counterintelligence gains can undermine diplomatic, military, and economic positions of the targeted country. U.S. authorities have characterized Salt Typhoon's telecom espionage as a "serious national intelligence risk," effectively a breach of the nation's strategic communications backbone.

In addition to espionage, the access maintained by Salt Typhoon translates to a latent sabotage threat. The group's presence in critical telecom networks and even military communication systems suggests an ability to disrupt or degrade those systems at will. U.S. officials warn that the Salt Typhoon group is "prepositioning itself to paralyze U.S. critical infrastructure" in the event of conflict.

For example, should tensions with China escalate to open hostilities, Salt Typhoon could leverage its implanted accesses to shut down or corrupt telecommunication services (impacting military command and control, emergency services, and civilian communication).

The pre-positioning idea is like having sleeper agents in cyberspace: they are already inside the infrastructure, needing only an instruction to cause damage. Given that the Salt Typhoon group had reached into networks connecting state National Guards and fusion centers, one can imagine the potential to sow chaos during a national crisis by cutting off lines of communication or feeding false information. The breaches also highlight a supply chain and third-party risk. Salt Typhoon's compromise of not just primary targets but their partners (e.g., telecom vendors, consulting firms) means that any organization even peripherally connected to a strategic target could be at risk. This widens the threat landscape considerably. It also means traditional security perimeters are insufficient – even if a critical organization is locked down, Salt Typhoon might infiltrate via a less secure partner.

The long-term risk is that Salt Typhoon (and similar groups) will continue to exploit the weakest link in the chain unless systemic changes are made in how organizations do vendor security and network segmentation. There is also a data integrity risk. While Salt Typhoon has been focused on espionage (which is mostly theft of data), their deep access means they could also subtly manipulate data. For instance, in telco environments, beyond stealing data, they might alter databases – e.g., modify call records or insert false records, potentially to mislead investigators or frame individuals.

In military networks, they could alter readiness data or equipment configurations. Such subtle tampering could have pernicious effects and be very hard to detect, especially if defenders are only looking for theft, not changes. Another dimension of impact is the erosion of trust in critical systems. Knowing that an adversary was quietly siphoning data from fundamental institutions (like phone networks or Guard units) can have a chilling effect. Citizens and officials may lose confidence in the security of their communications. This has prompted significant responses: the FBI's $10M reward and public alerts indicate an urgent need to rally information and support to deal with the threat.

Internationally, it may spur changes such as excluding certain equipment vendors (to reduce potential backdoors), increasing cybersecurity requirements for telcos, and even diplomatic confrontation over these cyber activities. From a long-term perspective, Salt Typhoon's success might encourage them (and others) to continue or expand such operations. It took years for these breaches to come to light; thus, Salt Typhoon may still have unknown persistence in additional networks that haven't been discovered yet. The Wall Street Journal

in mid-2025 quoted U.S. officials expressing concern that Chinese cyber presence is only partially known and likely far more extensive. This ongoing uncertainty is itself a risk – defenders may be operating under false assumptions of security in some networks that are in fact compromised.

In summary, Salt Typhoon's campaigns impacts:

- **Intelligence Loss:** Confidential information in adversary hands (diplomatic, military, economic intel).
- **Infrastructure Vulnerability:** The latent ability for an adversary to disrupt communications and other critical services from within.
- **Financial Costs:** Remediation of these widespread breaches will cost carriers and agencies significant resources (incident response, replacing hardware, etc.).
- **Policy & Diplomatic Fallout:** It has triggered high-level responses – e.g., U.S. government openly attributing and sanctioning Chinese entities, which affects international relations.
- **Psychological Impact:** The revelation that even sensitive, supposedly secure networks (like military) were not secure can reduce public confidence and raise paranoia about technology trustworthiness.

# DEFENSIVE RECOMMENDATIONS

Defending against a threat actor as advanced as Salt Typhoon requires a multi-layered security strategy and a shift in mindset towards proactive defense. Below are practical recommendations tailored to the sectors most targeted by Salt Typhoon – telecommunications providers, government/military networks, and enterprises – with an emphasis on countering the group's known tactics:

**Adopt a zero-trust architecture:** All organizations, especially telecoms and government agencies, should operate under the assumption that an intruder may already be in the network. Zero Trust means continuously verifying user and device identity, limiting access

privileges, and segmenting networks so that compromise of one node does not grant wide access. For telcos, this might mean separating critical network management systems from corporate IT and requiring strict authentication even for internal connections. Government networks should treat even “internal” traffic with scrutiny and use micro-segmentation to contain breaches.

**Strict patch management & vulnerability reduction:** Close the initial access paths that Salt Typhoon favors. Telecom operators and enterprises must aggressively patch internet-facing systems – VPN gateways, firewalls, email servers (Exchange), etc. – on a tight timeline. Any known critical vulnerabilities (e.g., those in Ivanti, Fortinet, Sophos devices, or ProxyLogon in Exchange) should be treated as emergency fixes. Where possible, implement virtual patching or workarounds if a full patch isn’t available. Conduct regular external surface scans to ensure no forgotten or unpatched service is exposed. Telecom infrastructure often involves proprietary hardware; coordinate with vendors for prompt security updates on routers, MSCs, etc., and consider retiring or isolating legacy systems that cannot be adequately secured.

**Robust network segmentation and monitoring:** Telecommunication networks should be segmented such that systems like lawful intercept servers and CDR databases are on isolated segments accessible only by a small number of authenticated management stations. Government networks should ensure operational systems (e.g., fusion center databases, mission-critical servers) are on separate enclaves with limited access paths. Implement internal firewalls or software-defined networks to tightly control which host can talk to which. Then, deploy network monitoring (IDS/IPS) at key junctions – monitor east-west traffic for unusual patterns, like a user machine querying domain controllers or an admin tool being used irregularly. Given Salt Typhoon’s penchant for using common ports (443, etc.), incorporate deep packet inspection that can detect anomalies in protocol usage (e.g., an internal machine acting as a web client at odd hours to an IP that’s not a known business partner).

**Credential hygiene and privileged access management:** Since Salt Typhoon thrives on stolen credentials, organizations must harden identity security. Enforce multi-factor authentication (MFA) everywhere, especially for VPNs, administrator accounts, and remote access into critical systems.

Telecommunication providers should require MFA for any access to network management systems or customer data stores. Use privileged access management (PAM) solutions to control admin account usage – e.g., one-time credentials, monitored admin sessions, and no standing administrative rights for user accounts. Regularly audit accounts for any unauthorized creation or privilege escalation (as Salt Typhoon sometimes creates new accounts) and remove stale or unnecessary privileged accounts.

**Enhanced endpoint detection and response (EDR):** Deploy advanced EDR or XDR (Extended Detection and Response) tools across servers and endpoints to catch the subtle behaviors Salt Typhoon exhibits. Specifically, monitor for:

- Use of LOLBINs like wmic.exe, powershell.exe, bitsadmin.exe spawning unusual processes or making outbound connections
- Loading of unsigned drivers or unusual kernel modules (to potentially catch rootkit activity). Kernel monitoring that can alert on attempts to tamper with the OS (e.g., hooking system calls) is crucial – consider tools that compare kernel modules against a known-good list.
- Mimikatz or similar credential dumping patterns (like suspicious access to LSASS memory). Some EDRs have canaries or hooks to detect this behavior.
- Unexpected creation of new services or scheduled tasks (especially with random or suspicious names).

For government and military systems, which may have stricter device policies, ensure all endpoints including servers are covered by EDR and that analysts are actively triaging alerts.

**Incident response readiness and hunting:** Given the threat's stealth, assume compromise and actively hunt for dormant Salt Typhoon implants. This includes:

- Scanning for known indicators (file hashes, C2 domains/IPs) shared via threat intelligence from agencies and vendors.
- Conducting periodic network sweeps for unusual open ports or listening services on routers and servers (they may install backdoor listeners).

- Memory forensics on critical servers to look for in-memory only malware (since Salt Typhoon often resides in memory). Our open-source forensic suite Velociraptor could help here.
- Hunt for anomalies like processes running from temp directories, or auto-start extensibility points in the registry that aren't standard – these could reveal Salt Typhoon persistence.

**Secure configuration of telecom systems:** For telecom providers specifically, implement recommendations from industry standards (like NIST and 3GPP) for hardening. Change default credentials on all network equipment – Salt Typhoon has exploited weak router passwords.

**Collaboration and information sharing:** Given the national security implications, telecoms and government agencies should actively collaborate via information sharing programs (like ISACs – Information Sharing and Analysis Centers for telecom and IT sectors). Share any suspicious activity or partial breach indicators immediately with relevant authorities (FBI, CISA) so that patterns can be correlated. The Salt Typhoon case underscored that dozens of companies were hit – better sharing might have surfaced sooner. Intelligence feeds from the government can also provide updated indicators (e.g., new C2 domains or malware signatures) that organizations can plug into their defenses.

## Sector-specific emphasis:

**Telecom providers:** Enforce rigorous controls around intercept systems and customer data stores – treat them as crown jewels with separate monitoring. Implement telecom-specific anomaly detection (e.g., alerts if anyone exports large volumes of CDRs). Work closely with government agencies on threat intel and consider joint exercises to test network resilience against nation-state attacks.

**Government and military networks:** Assume any network touching the internet is compromised; use classified networks or air-gapped systems for truly sensitive comms. Regularly audit all state-level and partner connections, so ensure that trust is minimized and monitored). Implement "double authentication" for highly sensitive actions (like accessing intelligence databases – require two separate authorizations).

**Enterprises:** Prioritize monitoring of any system that could be a stepping stone to a bigger target (if you do business with government or critical industries, you could be the next supply-chain target). Incorporate threat hunting for signs of long-term quiet intruders, not just noisy malware.

## Conclusion: Be as Persistent as They Are

In closing, the campaign by Salt Typhoon is a wake-up call that advanced persistent threats can silently burrow into the foundational infrastructure of our society. Defenders must respond with equal persistence – continuously hardening systems, watching for subtle clues, and being ready to contain and eradicate these threats at the earliest hint of their presence. With a vigilant, zero-trust approach and strong collaboration between industry and government, the opportunities for groups like Salt Typhoon to succeed can be dramatically reduced.

## About Rapid7 Labs

Rapid7 Labs actively tracks advanced persistent threat (APT) groups such as Salt Typhoon, providing timely curated intelligence, behavioral indicators, and hunting logic to enhance detection and response capabilities across the Rapid7 platform. This intelligence directly fuels our products, including the Intelligence Hub, Managed Detection and Response (MDR), and InsightIDR (IDR), ensuring customers are equipped with actionable insights to identify and mitigate sophisticated nation-state threats.

### ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.