ORION FORUM

APT Profile: Salt Typhoon

SEPTEMBER 25, 2026

The ROCCA project examines significant cyber incidents and the actors behind them to identify patterns in cyber threats, their targets, and their broader security implications. These APT profiles provide background on the groups responsible for major incidents documented in the ROCCA dataset.

Country of Origin	China
Threat Actor Type	State-sponsored cyber espionage group
Other Names	RedMike, Earth Estries, GhostEmperor, UNC5807, and FamousSparrow
Year Identified	2020; related activity assessed by U.S. officials to date back to at least 2019
Target Countries	United States, Canada, United Kingdom, Germany, France, Japan, South Korea, Singapore, Taiwan, India, Saudi Arabia, Mexico, and other countries worldwide

Profile Summary

Salt Typhoon is a Chinese state-sponsored cyber espionage group that conducts long-term intrusions into telecommunications providers, government networks, internet service providers, and other organizations connected to critical communications infrastructure. The group is primarily focused on intelligence collection, rather than financial gain or disruption.

Salt Typhoon has received significant attention because of its ability to compromise telecommunications infrastructure and use that access to collect sensitive communications data. In the United States, investigators found that the 2024 campaign resulted in the theft of customer call-record information and access to information associated with U.S. law-enforcement requests. Major telecommunications companies identified as affected included AT&T, Verizon, and Lumen Technologies.

The group's importance comes from the strategic position provided by telecommunications networks. Compromising a telecommunications provider can give an intelligence service access to information about large numbers of users without compromising each device. Salt Typhoon has also demonstrated the ability to identify and target specific high-value individuals, including people associated with the 2024 U.S. presidential campaigns. By 2025, U.S. officials described the activity as a global campaign affecting organizations in approximately 80 countries, underscoring that the group's operations extend beyond isolated intrusions into individual telecommunications companies.

This map, drawn directly from the ROCCA database, shows cyberattacks conducted by Chinese actors against countries worldwide. Darker shading indicates countries that experienced a higher number of attacks

Background & Development

Salt Typhoon has been publicly documented since at least 2020, although the FBI assessed that related PRC-affiliated activity dates back to at least 2019. The group initially became associated with intrusions against telecommunications providers and communications infrastructure, where access could support long-term intelligence collection. Beginning in the early 2020s, researchers observed the group expanding its activity across telecommunications providers and other organizations connected to critical communications networks. By 2023, activity targeting telecommunications providers had increased across multiple countries. The major turning point came in 2024, when investigators discovered that Salt Typhoon had also compromised multiple major U.S. telecommunications providers. The campaign became particularly significant because the attackers were able to use telecommunications infrastructure to target individuals connected to U.S. political campaigns and collect sensitive communications information.

Salt Typhoon gained access to telecommunications networks used by individuals associated with the campaigns of Donald Trump, JD Vance, and Kamala Harris. The compromise did not involve directly hacking the candidates' phones; instead, the actors exploited telecommunications infrastructure to obtain information about targeted communications. The broader campaign allowed the actors to steal customer call-record data, compromise a limited number of private communications, and copy information associated with U.S. law-enforcement requests. The FBI later described the campaign as "broad and significant," emphasizing that the actors leveraged access to telecommunications networks to target victims on a global scale. The U.S. government continued to investigate the campaign throughout 2025, identifying additional victims and publishing guidance on PRC-affiliated actors' methods of compromising telecommunications and other critical infrastructure.

Organizational Structure

Salt Typhoon is assessed to be a highly sophisticated cyber espionage operation with access to significant technical resources and a coordinated operational structure designed to support long-term intelligence collection. Although the group's internal organization remains unknown,

similar to other Chinese threat actors like APT41, its activities suggest the involvement of specialized teams responsible for initial access, network exploitation, credential theft, privilege escalation, persistence, lateral movement, and data collection. The group demonstrates advanced operational security practices by prioritizing stealth and maintaining prolonged access within compromised environments. A February 2025 compromise of three network devices at an unnamed Canadian telecommunications company illustrates these techniques (the incident is examined in greater detail within the “Target Profile” section).

Rather than relying on easily identifiable malware, Salt Typhoon frequently uses stolen credentials and legitimate administrative tools, including “living-off-the-land” techniques that use existing system utilities to blend malicious activity with normal network operations. Common tactics, techniques, and procedures (TTPs) include exploiting internet-facing applications and network devices, compromising VPN infrastructure, modifying routers, deploying web shells, conducting network reconnaissance, abusing legitimate system tools, and establishing persistent access mechanisms. These techniques significantly complicate detection and attribution because the group’s activities often resemble legitimate administrative behavior, allowing operators to remain undetected within targeted networks for extended periods.

State and Non-State Relations & Strategic Objectives

Salt Typhoon is widely attributed to the Chinese government, with links to China’s Ministry of State Security (MSS), and is assessed to conduct cyber operations in support of national intelligence objectives. The group’s activities align with broader Chinese state-sponsored cyber campaigns focused on strategic information collection rather than financial gain or ideological objectives. Politically, Salt Typhoon seeks to collect intelligence on foreign governments, policymakers, diplomats, and other high-value decision-makers to support Chinese foreign policy and national security priorities. Access to communications networks provides valuable intelligence that can enhance Chinese military planning, counterintelligence efforts, and strategic awareness of foreign activities. Although the group is primarily focused on espionage, the intelligence collected may also contribute to China’s broader economic and technological competitiveness by providing insight into strategic industries and emerging developments.

There are no publicly identified ideological or social motivations associated with Salt Typhoon; instead, its operations appear driven by state intelligence priorities and long-term strategic objectives.

Target Profile

Salt Typhoon primarily targets organizations that provide access to valuable communications data, strategic intelligence, and critical network infrastructure. The group's victims include government agencies, defense organizations, technology companies, telecommunications providers, internet service providers, and other critical infrastructure operators. Its geographic targeting is global, with identified victims across the United States, Europe, the Indo-Pacific region, and Southeast Asia. Unlike opportunistic cybercriminal groups, Salt Typhoon appears to select targets based on their strategic value and their ability to provide access to sensitive communications, government information, or large-scale infrastructure networks. Telecommunications infrastructure remains a primary operational focus, although Salt Typhoon-related activity has also targeted government, military, transportation, lodging, and other critical infrastructure networks.

Target Type	Strategic Value	Reason
Telecommunications	★★★★★	Access to communications data
Government	★★★★★	Political and intelligence value
Technology	★★★★☆	Supply chain and technical access
Critical Infrastructure	★★★★☆	Strategic resilience information
Private Organizations	★★★☆☆	Economic intelligence

Canadian reporting provides a particularly detailed example of how this targeting operates outside the United States. In mid-February 2025, Salt Typhoon actors compromised three network devices registered to an unnamed Canadian telecommunications company. According to the Canadian Centre for Cyber Security, the actors exploited CVE-2023-20198 to retrieve the running configuration files from all three devices and modified at least one configuration to establish a Generic Routing Encapsulation (GRE) tunnel, allowing them to collect network traffic. The Cyber Centre assessed that the actors were “almost certainly” PRC state-sponsored actors, specifically Salt Typhoon. The agency also warned that compromising telecommunications devices could allow the actors to collect information from the victim’s internal network or use the compromised device to facilitate attacks against additional victims.

Assessment of Impact

Salt Typhoon poses an extremely significant national security threat due to its demonstrated ability to compromise telecommunications infrastructure and access sensitive government and private communications. Successful intrusions into telecommunications providers create risks of widespread intelligence collection, including potential access to communications involving government officials, policymakers, and other high-value targets. Economically, Salt Typhoon operations may result in increased cybersecurity costs, remediation efforts, operational disruptions, and potential exposure of sensitive corporate or technological information. The compromise of critical communications infrastructure also creates public safety concerns, as disruptions or unauthorized access could affect emergency communications and crisis response capabilities. Politically, these operations undermine trust in global communications systems, increase diplomatic tensions, and raise concerns regarding foreign surveillance capabilities. The targeting of individuals connected to the 2024 U.S. presidential campaigns illustrates this concern, as Salt Typhoon used telecommunications access to collect intelligence on high-value political targets rather than directly disrupt election infrastructure. Over the long term, Salt Typhoon demonstrates China’s growing ability to conduct sustained cyber espionage within critical infrastructure environments, highlighting challenges related to cyber deterrence, infrastructure resilience, and national cybersecurity strategy.

Attribution and Evidence

Salt Typhoon has been attributed to Chinese state-sponsored cyber operations based on assessments from multiple government agencies, cybersecurity organizations, and threat intelligence researchers, including the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Canadian Centre for Cyber Security, and major cybersecurity vendors. Attribution is supported by several indicators, including the group's consistent targeting of telecommunications providers, overlap in infrastructure and malware characteristics, similarities across operational campaigns, prolonged persistence within compromised networks, and the use of TTPs associated with Chinese state-sponsored cyber activity. However, attribution and detection remain challenging due to Salt Typhoon's sophisticated operational security practices, including legitimate administrative tools.

Major Cyber Operations

Date	Operation / Target	Attack Type	Sector
2019-2022	Early telecommunications intrusions in Southeast Asia	Exploitation, credential theft, persistence	Telecommunicati
2023	Telecommunications providers worldwide	Credential theft, network exploitation	Telecommunicati
2024	U.S. law-enforcement systems	Unauthorized access	Telecommunicati / Law Enforcemer
Oct. 2024	Trump, JD Vance & Harris campaign-related communications	Targeted collection through compromised telecom networks	Political / Telecommunicati

Oct.-Dec. 2024	AT&T, Verizon, Lumen Technologies & other U.S. telecom providers	Network compromise, credential abuse, data collection	Telecommunicati
Feb. 2025	Unnamed Canadian telecommunications company	Exploitation of network devices; configuration modification; traffic collection	Telecommunicati
2026	Global telecommunications and network infrastructure	Router exploitation, credential abuse, persistent access	Telecommunicati / Critical Infrastructure

See CSIS Database and Canadian Centre for Cyber Security for more detailed descriptions.

Critical Attack Profile: Salt Typhoon's 2025 Canadian Telecommunications Compromise

In February 2025, actors associated with Salt Typhoon compromised three network devices belonging to an unnamed Canadian telecommunications company. The Canadian Centre for Cyber Security assessed that the actors were almost certainly PRC state-sponsored actors, specifically Salt Typhoon. Rather than targeting individual computers, the attackers targeted the infrastructure connecting them, potentially giving them visibility into communications and network activity across a much broader environment.

Canadian authorities identified the activity during an investigation and compared the observed indicators with known Salt Typhoon activity. Salt Typhoon operations generally emphasize long-term intelligence collection and persistent access rather than financial gain or immediate disruption. The Canadian incident fits this strategy: compromising telecommunications infrastructure potentially allowed the attackers to collect information from the victim's network and potentially use the compromised devices to facilitate further intrusions.

The attackers exploited CVE-2023-20198, a critical vulnerability affecting Cisco IOS XE devices. According to Cisco's security advisory, the vulnerability received a CVSS score of 10.0 and could allow attackers to gain privileged access to affected devices. Cisco released fixes for the vulnerability in 2023, making its exploitation 16 months later particularly significant. After gaining access, the attackers retrieved the running configuration files from all three devices. They then modified at least one configuration to establish a Generic Routing Encapsulation (GRE) tunnel, enabling traffic collection from the network. The attack can therefore be summarized as: exploit vulnerability → access network devices → retrieve configurations → modify device → establish GRE tunnel → collect traffic. This illustrates why network-edge devices are particularly valuable intelligence targets. A compromised router can provide visibility into information moving through a network without requiring attackers to compromise every individual endpoint.

The immediate financial impact has not been publicly quantified, but the telecommunications provider likely faced costs associated with investigation, remediation, reconfiguration, and strengthening network defenses. The potential societal impact is broader: telecommunications infrastructure carries information belonging to large numbers of users, meaning that compromising only three devices could potentially affect communications beyond those devices themselves. From a national-security perspective, the incident gave a foreign intelligence actor access to Canadian telecommunications infrastructure. Such access can provide information about communications patterns, organizational relationships, network architecture, and other intelligence of value to a state actor. The Cyber Centre also found indicators suggesting that related PRC cyber activity in Canada extended beyond telecommunications, demonstrating that the campaign was broader than a single sector.

The incident exposed several important security weaknesses. First, a known critical vulnerability remained exploitable after its disclosure and patching. Second, network devices contained configuration information valuable to an adversary. Third, attackers were able to manipulate legitimate network functionality to facilitate traffic collection. Finally, endpoint-focused security measures may fail to detect compromises occurring directly on routers and other network infrastructure. The incident also presents challenges for cyber investigations and attribution. Investigators must correlate technical indicators, network configurations, device logs, authentication records, and traffic data with known threat-actor activity. Because Salt Typhoon operates across national borders, information sharing between governments and private-sector telecommunications providers is particularly important for connecting individual compromises to broader campaigns. The compromise occurred in mid-February 2025 but was publicly disclosed by Canadian authorities in June 2025, illustrating the potential gap between compromise, investigation, attribution, and public notification.

The most important lesson is simple: the infrastructure carrying information can be just as valuable to an adversary as the information itself. Salt Typhoon did not need an elaborate zero-day to achieve this access. Instead, the group exploited a known vulnerability and then used legitimate network functionality to turn compromised infrastructure into a potential intelligence-collection platform. The Canadian case therefore demonstrates why critical-

infrastructure defense must extend beyond traditional endpoint security. Governments and telecommunications providers should treat network-edge devices as national-security assets, prioritize rapid remediation of critical vulnerabilities, restrict administrative interfaces, monitor configuration changes, and maintain sufficient logging to reconstruct suspicious activity. Ultimately, a seemingly small technical compromise can create a much larger strategic intelligence opportunity.