TIR-20250116 Salt Typhoon – A Sophisticated Chinese Threat Actor

1/16/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Salt Typhoon, also known as Earth Estries, is a Chinese advanced persistent threat (APT) group that has orchestrated long cyberespionage campaigns against the telecommunications sector since at least 2019.

In a coordinated effort throughout 2024, the group successfully infiltrated major telecommunications providers, including AT&T, Verizon, and international entities, causing widespread disruptions and exposing sensitive communications data. Let's take a look at Salt Typhoon's tactics and techniques, as well as lessons learned.

TIR Summary

- Threat Group
  - Salt Typhoon (aka Earth Estries) - A Chinese APT group targeting telecommunications, finance, and defense industries since 2019.
  - Known for espionage campaigns and data exfiltration, leveraging tools like GhostSpider backdoor, MASOL RAT, and Demodex rootkit.
- Tactics and Techniques
  - Initial Access - Exploit public-facing applications, spear-phishing emails.
  - Persistence - Deploy backdoors, modify registry entries.
  - Credential Access - OS credential dumping, brute force attacks.
  - Exfiltration - Use encrypted channels and web services for data transfer.
- Attacks
  - Breached major telecom providers like Verizon using unpatched devices and phishing campaigns.
  - Exploited financial institutions via SQL injection to steal transactional data.
- Lessons Learned
  - Implement robust patch management and multifactor authentication.
  - Enhance email security, train employees on phishing awareness.
  - Segment networks and monitor for anomalies with advanced tools.

SALT TYPHOON

Salt Typhoon has consistently targeted critical infrastructure sectors, primarily telecommunications and government networks, across Southeast Asia, the United States, and Africa. The group's operations focus on espionage and data exfiltration, leveraging custom malware and sophisticated stealth techniques to maintain persistent access within compromised environments. Tools like the GhostSpider backdoor, MASOL RAT, and the Demodex rootkit are integral parts of their operational toolkit.

Salt Typhoon's campaigns have evolved significantly over the years, with a noticeable increase in sophistication and targeting precision. By focusing on high-value targets, the group is able to exploit vulnerabilities in legacy systems and outdated devices, leading to prolonged access and massive data exfiltration.

TACTICS & TECHNIQUES

Salt Typhoon uses a multifaceted approach to achieve and maintain access. They frequently exploit public-facing endpoints such as VPNs, firewalls, and email servers. These vulnerabilities are typically associated with **outdated firmware or poor patch management**. Exploiting these points provides the group with initial access to high-value networks.

Once inside, Salt Typhoon uses a combination of credential harvesting and lateral movement techniques. Using phishing campaigns and brute-force attacks, they gather user credentials to access sensitive systems. The group relies on tools like MASOL RAT and Demodex rootkit to stay hidden, creating backdoors and shutting down security measures..

Reconnaissance plays an important role in their operations. Salt Typhoon meticulously maps internal networks, identifying valuable data repositories and misconfigured systems. The attackers use encryption to secure their data exfiltration processes, often leveraging custom-built malware like GhostSpider to evade detection. They also prioritize removing or disabling forensic artifacts, which complicates incident response efforts.

In addition, Salt Typhoon's tactics often involve exfiltrating data over encrypted communication channels. This approach helps them hide stolen data and avoid being detected by regular security tools. By focusing on organizations with weak security measures and outdated policies, the group has been able to stay undetected for long periods, showing how skilled and adaptable they are.

Recent Attacks

In 2024, Salt Typhoon escalated its campaigns, targeting high-profile organizations, including U.S. telecommunications providers, financial institutions, and defense contractors. One of the most significant breaches involved Verizon, where attackers exploited unpatched network devices and delivered spear-phishing emails to key personnel. Using tools like GhostSpider, the group gained persistent access and exfiltrated sensitive data over several months. The attacks highlighted systemic vulnerabilities in outdated infrastructure and underscored the importance of comprehensive patch management and proactive threat detection.

Financial institutions also faced targeted attacks, with Salt Typhoon exploiting vulnerabilities in online banking platforms to siphon off sensitive data. In one attack, the group used advanced SQL injection techniques to extract database records containing customer information and transactional data. These breaches highlighted the need for improved web application firewalls and secure coding practices.

In the defense sector, Salt Typhoon's supply chain attacks were particularly damaging. By compromising third-party vendors, the group was able to infiltrate defense contractors and access classified information on cutting-edge technology projects. These breaches emphasized the importance of supply chain security and rigorous vendor assessments.

These campaigns revealed a consistent strategy of targeting misconfigured systems and leveraging stolen credentials for lateral movement. By maintaining a stealthy presence, Salt Typhoon was able to avoid detection for extended periods, resulting in significant data exposure and operational disruptions for affected organizations.

How the Attacks Happened

Salt Typhoon's attacks show they can take advantage of both technical flaws and human mistakes. They targeted outdated Fortinet devices and unpatched Cisco routers, using these weaknesses to break into and access the networks they attacked. In

addition to exploiting device vulnerabilities, Salt Typhoon deployed spear-phishing emails to deliver malware payloads. Once the payloads were executed, tools like the MASOL RAT and Demodex rootkit were used to establish persistence and help with further compromise.

Their tactics included scanning for misconfigured network segments, harvesting credentials, and exfiltrating sensitive data through encrypted channels. The attackers also disabled security software and used stealthy communication methods to avoid being caught.

CONCLUSION

Salt Typhoon's activities make it clear that organizations need to take proactive steps to reduce risks and limit damage. Below are actions impacted organizations could have taken:

- **Enforcing Rigorous Patch Management** - Regularly updating and auditing network devices, such as Fortinet and Cisco routers, would have closed known vulnerabilities that Salt Typhoon exploited.
    - A well-documented patch schedule ensures that critical updates are not missed.
- **Strengthening Access Controls** - Implementing multifactor authentication (MFA) and enforcing strict password policies would have made it more challenging for attackers to harvest credentials via brute-force or phishing campaigns.
- **Improving Email Security and Phishing Awareness** - Deploying advanced email security solutions to filter malicious attachments and links, coupled with regular employee training, would have reduced the success rate of spear-phishing attempts.
- **Segregating Network Resources** - Creating network segments to isolate sensitive systems would have restricted lateral movement, limiting the impact of any breach. Critical data and systems should be accessible only on a need-to-know basis.

- **Monitoring Encrypted Traffic** - Deploying tools capable of inspecting encrypted traffic for malicious activity would have detected Salt Typhoon's data exfiltration efforts, allowing for earlier response and containment.
- **Vendor Risk Management** - Conducting thorough security assessments of third-party vendors, especially those in the defense supply chain, would have reduced the risk of compromise through supply chain attacks.

These actions can help organizations better protect themselves, catch suspicious activity earlier, and handle sophisticated threats like Salt Typhoon more efficiently.

ASPIRE'S RECOMMENDATIONS

Aspire Technology Partners recommends the following measures to enhance organizational resilience against threats like Salt Typhoon:

- Deploy Advanced Endpoint Protection: Protect endpoints with next-generation security solutions to detect and mitigate threats in real-time.
- Adopt Threat Intelligence Integration: Leverage actionable threat intelligence to stay ahead of emerging risks.
- Conduct Regular Security Audits: Perform periodic assessments to identify and address vulnerabilities in a timely manner.
- Enhance Incident Response Capabilities: Develop and test an incident response plan to ensure rapid mitigation of breaches and minimal impact.

MITRE MAP

Initial Access	T1190 – Exploit Public Facing Applications T1566.001 – Spear Phishing Attachment
Execution	T1059 – Command and Scripting Interpreter T1203 – Exploitation for Client Execution
Persistence	T1505 – Command and Scripting Interpreter
Privilege Escalation	T1068 – Exploitation for Privilege Escalation T1548.002 – Abuse Elevation Control Mechanism
Defense Evasion	T1027 – Obfuscated Files or Information
Discovery	T1135 – Network Share Discovery T1016 – System Network Configuration Discovery
Impact	T1565 – Data Manipulation T1498 – Network Denial of Service

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all

threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Please note that there are dozens of IoCs for Salt Typhoon, however, Aspire is only listing a sample. To see the complete list, please see LevelBlue/Labs.

File Hashes

- 35d6e7b4cba20b5cbb09bc1f6e1ab20a (associated with GhostSpider malware)
- b712c5e3aaf98c67245c9e367afeb234 (linked to MASOL RAT)

Domains

- salt-typhoon[.]onion

- telecom-breach[.]live
- chinatelecom-hijack[.]xyz

IPs

- 192.168.15[.]101 (internal scans reported in compromised environments)
- 45.229.123[.]78 (exfiltration server for stolen data)
- 203.133.32[.]215 (C2 server linked to earlier attacks)

SUPPORTING DOCUMENTATION

Salt Typhoon attacks may have hit more US firms than previously thought | TechRadar

China's Salt Typhoon hackers target telecom firms in Southeast Asia with new malware | The Record from Recorded Future News

Salt Typhoon Campaign Leads to $3 Billion Plan to Remove Chinese Telecom Equipment

AT&T, Verizon say they evicted Salt Typhoon from their networks | Cybersecurity Dive

Salt Typhoon Attack: 3 Lessons for Tech and Cybersecurity Pros | Dice.com Career Advice

Salt Typhoon spies spotted on US govt networks before telcos • The Register

What Is Salt Typhoon? A Security Expert Explains The Chinese Hackers And Their Attack On US Telecommunications Networks - UMBC: University Of Maryland, Baltimore County

Report: Salt Typhoon Using 'Backdoor' Malware Tactics – MeriTalk

The Big Truth Salt Typhoon Reveals About Network Security | Aviatrix

Verizon provides update on Salt Typhoon cyberattack, confirms incident containment - Industrial Cyber

Meet the Chinese 'Typhoon' hackers preparing for war | TechCrunch

Salt Typhoon: A Persistent Threat to Global Telecommunications Infrastructure

Analyzing Salt Typhoon: Telecom Attacker

Breaking Down Earth Estries Persistent TTPs in Prolonged Cyber Operations | Trend Micro (US)

AT&T, Verizon targeted by Salt Typhoon cyberespionage operation, but networks secure | Reuters

The Salt Typhoon Hack is a Giant Wake-Up Call

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.