August 7, 2025

EMERGING THREATS

SALT TYPHOON THREAT GROUP

UPDATE 08/07/2025: During the last year, **Salt Typhoon** operations have prominently featured the exploitation of vulnerabilities in Cisco's IOS XE software, notably CVE-2023-20198 and CVE-2023-20273, to gain unauthorized access to network devices. These attacks have led to the compromise of a number of entities including major telecommunications providers in the United States, Canada, and South Africa, with the group breaching the satellite communications firm Viasat in early 2025 for instance. Beyond exploiting known vulnerabilities, **Salt Typhoon** also has a history of employing sophisticated techniques tied to malware that include deploying trojanized payloads for downloading additional tools, exfiltrating data or executing remote commands on a victim's system. Furthermore, techniques that have been observed also involve the capture and exfiltration of data that can range from sensitive credentials, session tokens and information pertaining to the victim or the victim's system. With these tactics, attackers are able to laterally move across networks, and leverage existing network tools and protocols to conduct malicious activities without triggering security alarms. The group's strategic focus on telecommunications infrastructure allows for extensive intelligence collection, including the interception of communications and monitoring of law enforcement activities, posing significant risks to national security.

THREAT SUMMARY

UPDATE 08/05/2025: During the last year, **Salt Typhoon** operations have prominently featured the exploitation of vulnerabilities in Cisco's IOS XE software, notably CVE-2023-20198 and CVE-2023-20273, to gain unauthorized access to network devices. These attacks have led to the compromise of a number of entities including major telecommunications providers in the United States, Canada, and South Africa, with the group breaching the satellite communications firm Viasat in early 2025 for instance. Beyond exploiting known vulnerabilities, **Salt Typhoon** also has a history of employing sophisticated techniques tied to malware that include deploying trojanized payloads for downloading additional tools, exfiltrating data or executing remote commands on a victim's system. Furthermore, techniques that have been observed also involve the capture and exfiltration of data that can range from sensitive credentials, session tokens and information pertaining to the victim or the victim's system. With these tactics, attackers are able to laterally move across networks, and leverage existing network tools and protocols to conduct malicious activities without triggering security alarms. The group's strategic focus on telecommunications infrastructure allows for extensive intelligence collection, including the interception of communications and monitoring of law enforcement activities, posing significant risks to national security.

Salt Typhoon is an APT threat actor that has most recently and publicly breached the systems of major United States based telecommunication providers (specifically ISPs) in September/October of 2023 - the networks affected by the breach included Verizon Communications, AT&T and Lumen Technologies. Considered to be an extremely damaging cyber espionage campaign, the threat actors claimed to have been entrenched in their systems for 'months'. The intrusion gave attackers access to proprietary intelligence and law enforcement data, exploiting systems used for what is understood as lawful wiretapping. The threat actor **Salt Typhoon** (also known as GhostEmperor, Famous Sparrow or UNC2286), has been active since 2020 and is operated by the Chinese Government to conduct cyber espionage campaigns against targets in North America, Southeast Asia, and Europe. It is also worthy to note that the industries that the threat actor has been observed to attack include telecommunications, government and information technology.

With the evolving cyber threat from entities based in China, this highly damaging attack on U.S. wiretap systems by **Salt Typhoon**, and the likely impending release of the

techniques, tactics and procedures involved in the intrusion, it is important to ascertain and keep track of any information involving this threat group as more data is released.

TITAN References:

TITAN Spot Report: September 26, 2024
https://titan.intel471.com/report/geopol/spotrep/afcfcbde35a6f778dd370b74b36af856)

TITAN Spot Report: October 5, 2024
https://titan.intel471.com/report/geopol/spotrep/80670f23ecdd935f74837e8b33d64ee2

TITAN Intelligence Bulletin: July 3, 2025
http://titan.intel471.com/report/geopol/intelligence_bulletin/21208d0707eea6ffeaf110c96cd9a918)

TITAN Finished Intelligence Report: July 23, 2025
https://titan.intel471.com/report/fintel/f55079c7c862a1d002f5d7ce6516b421

SYNOPSIS

The **Salt Typhoon** threat group is a China based APT group known for their highly effective cyber espionage attacks on infrastructure across the world. They have been observed to employ a variety of malicious tooling that includes malware such as backdoor remote access trojans and rootkits in their sophisticated and targeted campaigns. Initial access has been observed by researchers to involve vulnerable internet-facing applications, as well as spear-phishing campaigns.

Demodex rootkit is one of the malware variants that Salt Typhoon employs in their attacks. This rootkit leverages sophisticated stealth and persistence in their multi-stage deployments of the malware - the methods used to stay obfuscated include EDR evasion techniques (such as preventing user-mode hooking with DLL files) and encrypted Powershell scripts. The malware loads the core-implant DLL loading it directly into memory, and the core-implant abuses an open-source tool utilized for video game hacking (Cheat Engine) in order to execute in kernel space. Other malware variants that **Salt Typhoon** has been seen to employ, including the Derusbi DLL backdoor, are efficient in techniques such as information stealing, creating a reverse shell, and modifying system processes, files and registry. As well as other lesser known malware such as 'Scandi' and 'Underaxe'. Additionally, **Salt Typhoon** is proficient in abusing legitimate software, with observed techniques seen to abuse tools such as Certutil, PsExec, ProcDump, WinRaR and Impacket.

With the TTPs(Tactics, Techniques and Procedures) of the United States based telecommunication intrusion assumed to be released in the near future, Intel471 will be updating this collection with new data and information as research becomes available.

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('c7d3ba73-f2f1-42c6-8f9b-39d768ad551e'),touched:!t)

RELATED HUNT PACKAGES

SUSPICIOUS SCHEDULED TASK CREATED - EXECUTION DETAILS CONTAINS SCRIPTING REFERENCE

https://hunter.cyborgsecurity.io/research/hunt-package/9a4fa42f-57dd-4449-b0c0-a1dd0976b17a

SINGLE-CHARACTER NAMED FILES USED FOR EXECUTION

https://hunter.cyborgsecurity.io/research/hunt-package/f20c5f61-c68a-446d-95c4-e227d3ac1078

CURL/WGET DOWNLOAD AND EXECUTE - POTENTIAL PAYLOAD DOWNLOAD FOLLOWED BY EXECUTION

https://hunter.cyborgsecurity.io/research/hunt-package/b585a013-e56d-4c3f-ac29-f2a610ac0ce8

WINRAR USED TO EXTRACT FROM AN ARCHIVE

https://hunter.cyborgsecurity.io/research/hunt-package/994d2cf1-4500-42f9-b6c4-ce2c04aaf084

SUSPICIOUS BITS ACTIVITY

https://hunter.cyborgsecurity.io/research/hunt-package/a96fd1ad-53c7-4125-9dfd-1dffa2f68f2d

SINGLE CHARACTER BATCH SCRIPT FILE EXECUTED ON ENDPOINT

https://hunter.cyborgsecurity.io/research/hunt-package/73fd8d9a-edb6-4db6-aab8-0dbc916f0fb4

USER ACCOUNT CREATION IN CISCO IOS

https://hunter.cyborgsecurity.io/research/hunt-package/f96170fb-93bd-4f44-b998-a0827287655d

EXECUTION BAT SCRIPT TO UNPACK PAYLOAD

https://hunter.cyborgsecurity.io/research/hunt-package/606cd1ac-622d-4645-9553-2b04df7407d8

CERTUTIL FILE DOWNLOAD

https://hunter.cyborgsecurity.io/research/hunt-package/f7b279bf-f1f9-4506-b636-e66f1834a278

DLL AND EXE FILE WRITTEN IN SAME DIRECTORY IN SHORT PERIOD - POTENTIAL DLL WRITE FOR DLL SIDE LOADING

https://hunter.cyborgsecurity.io/research/hunt-package/c3b32d06-aad2-425c-87a9-dcf085ad7da8

BASE64 ENCODED COMMAND EXECUTION

https://hunter.cyborgsecurity.io/research/hunt-package/2c6de808-b4c2-4f49-a496-ce4c25e1202d

DUMP LSASS VIA COMSVCS DLL

https://hunter.cyborgsecurity.io/research/hunt-package/f68b340c-0148-458f-913d-344a39509632

POTENTIAL IMPACKET WMIEXEC MODULE COMMAND EXECUTION

https://hunter.cyborgsecurity.io/research/hunt-package/5b4c793a-260a-4d43-bbc7-ad4547eeacda

SUSPICIOUS EXECUTABLE OR SCRIPTS LAUNCHED IN COMMON CONFIGURATION OR SYSTEM RELATED FOLDERS

https://hunter.cyborgsecurity.io/research/hunt-package/F2DD3A46-1C5D-42D3-B3FA-5BEC58D75E0B

POTENTIALLY ABNORMAL PARENT PROCESS FOR CMD.EXE OR REGEDIT.EXE

https://hunter.cyborgsecurity.io/research/hunt-package/332e1055-ae60-4e27-853b-b0b9ee02dcc0

DLL DROPPED IN PROGRAMDATA DIRECTORY - POSSIBLE COBALT STRIKE ACTIVITY

https://hunter.cyborgsecurity.io/research/hunt-package/58810576-0820-4ea9-a467-415659801dbc

BITSADMIN DOWNLOADING PAYLOADS FROM GITHUB

https://hunter.cyborgsecurity.io/research/hunt-package/df748f44-97e4-4c6e-bc86-43bc697fb198

EXCESSIVE WINDOWS DISCOVERY COMMANDLINE ARGUMENTS - POTENTIAL MALWARE INSTALLATION

https://hunter.cyborgsecurity.io/research/hunt-package/8bb5819f-06a4-4e5d-9099-e43115601999

WDIGEST DOWNGRADE ATTACK - REGISTRY KEY MODIFICATION

https://hunter.cyborgsecurity.io/research/hunt-package/61eece5f-432b-45ad-ab6a-ff1e5e783396

MITRE CONTEXT

- Exploits Vulnerabilities:
  - CVE-2024-1708
  - CVE-2025-31324
  - CVE-2024-1709
  - CVE-2023-20198
  - CVE-2024-3400
  - CVE-2023-20273
- MITRE Tactic Names:
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Execution
  - Command and Control
  - Collection
  - Persistence
  - Initial Access
  - Privilege Escalation
- MITRE Technique Names:
  - Malicious File
  - Deobfuscate/Decode Files or Information
  - Windows Management Instrumentation
  - Ingress Tool Transfer
  - OS Credential Dumping
  - Obfuscated Files or Information
  - Archive via Utility
  - Remote System Discovery
  - Rundll32
  - Create Account
  - Scheduled Task
  - DLL Search Order Hijacking
  - Modify Registry
  - Command and Scripting Interpreter
  - PowerShell

    - Masquerading
    - SMB/Windows Admin Shares
    - DLL Side-Loading
    - Registry Run Keys / Startup Folder
    - BITS Jobs
    - Spearphishing Attachment
    - Local Data Staging
- MITRE Technique IDs:
    - T1574.002
    - T1112
    - T1021.002
    - T1105
    - T1027
    - T1218.011
    - T1140
    - T1047
    - T1136
    - T1204.002
    - T1074.001
    - T1053.005
    - T1574.001
    - T1059.001
    - T1566.001
    - T1547.001
    - T1036
    - T1560.001
    - T1003
    - T1059
    - T1197
    - T1018

REFERENCES

1. https://www.washingtonpost.com/national-security/2024/10/06/salt-typhoon-china-espionage-telecom/
2. https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b
3. https://www.sygnia.co/blog/ghost-emperor-demodex-rootkit/
4. https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/
5. https://titan.intel471.com/report/geopol/spotrep/80670f23ecdd935f74837e8b33d64ee2
6. https://titan.intel471.com/report/geopol/spotrep/afcfcbde35a6f778dd370b74b36af856
7. https://www.varonis.com/blog/salt-typhoon
8. https://eclypsium.com/blog/cve-2023-20198-cisco-salt-typhoon-viasat-canadian-telcos/
9. https://www.authentic8.com/blog/cyber-intel-brief-salt-typhoon-breach-chrome-zero-day-pay2key-ransomware
10. https://censys.com/blog/the-persistent-threat-of-salt-typhoon-tracking-exposures-of-potentially-targeted-devices
11. http://titan.intel471.com/report/geopol/intelligence_bulletin/21208d0707eea6ffeaf110c96cd9a918