2024-10-16

HUNTER

EMERGING THREATS

SALT TYPHOON THREAT GROUP

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.

THREAT SUMMARY

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.

Intel 471 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)

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, include the Derusbi DLL backdoor, 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 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

SINGLE CHARACTER BATCH SCRIPT FILE EXECUTED ON ENDPOINT
https://hunter.cyborgsecurity.io/research/hunt-package/73fd8d9a-edb6-4db6-aab8-0dbc916f0fb4

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

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

RELATED LINKS
Sign up for free HUNTER access
Salt Typhoon Threat Group Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Command and Control
  - Persistence
  - Privilege Escalation
  - Initial Access
  - Collection
  - Lateral Movement
  - Execution
  - Defense Evasion
- Technique Names:
  - DLL Side-Loading
  - Local Data Staging
  - Spearphishing Attachment
  - Malicious File
  - Scheduled Task
  - Masquerading
  - DLL Search Order Hijacking
  - Deobfuscate/Decode Files or Information
  - Windows Management Instrumentation
  - Ingress Tool Transfer
  - Rundll32
  - Command and Scripting Interpreter
  - SMB/Windows Admin Shares
- Threat Names:

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