Salty Much: Darktrace’s take on a recent Salt Typhoon intrusion

By Nathaniel Jones

Published: 2025-10-20 · Archived: 2026-04-05 21:43:28 UTC

What is Salt Typhoon?

Salt Typhoon represents one of the most persistent and sophisticated cyber threats targeting global critical infrastructure today. Believed to be linked to state-sponsored actors from the People’s Republic of China (PRC), this advanced persistent threat (APT) group has executed a series of high-impact campaigns against telecommunications providers, energy networks, and government systems—most notably across the United States.

Active since at least 2019, the group — also tracked as Earth Estries, GhostEmperor, and UNC2286 — has demonstrated advanced capabilities in exploiting edge devices, maintaining deep persistence, and exfiltrating sensitive data across more than 80 countries. While much of the public reporting has focused on U.S. targets, Salt Typhoon’s operations have extended into Europe, the Middle East, and Africa (EMEA) where it has targeted telecoms, government entities, and technology firms. Its use of custom malware and exploitation of high-impact vulnerabilities (e.g., Ivanti, Fortinet, Cisco) underscores the strategic nature of its campaigns, which blend intelligence collection with geopolitical influence [1].

Leveraging zero-day exploits, obfuscation techniques, and lateral movement strategies, Salt Typhoon has demonstrated an alarming ability to evade detection and maintain long-term access to sensitive environments. The group’s operations have exposed lawful intercept systems, compromised metadata for millions of users, and disrupted essential services, prompting coordinated responses from intelligence agencies and private-sector partners worldwide. As organizations reassess their threat models, Salt Typhoon serves as a stark reminder of the evolving nature of nation-state cyber operations and the urgent need for proactive defense strategies.

Darktrace’s coverage

In this case, Darktrace observed activity in a European telecommunications organization consistent with Salt Typhoon’s known tactics, techniques and procedures (TTPs), including dynamic-link library (DLL) sideloading and abuse of legitimate software for stealth and execution.

Initial access

The intrusion began with exploitation of **CVE-2025-5777**, a vulnerability affecting **Citrix NetScaler Gateway** appliances, in the first week of July 2025. From there, the actor pivoted to Citrix Virtual Delivery Agent (VDA) hosts in the client’s **Machine Creation Services (MCS)** subnet. Initial access activities in the intrusion originated from an endpoint potentially associated with the SoftEther VPN service, suggesting infrastructure obfuscation from the outset.

Tooling

Darktrace subsequently observed the threat actor delivering a backdoor assessed with high confidence to be SNAPPYBEE (also known as Deed RAT) [2][3] to multiple Citrix VDA hosts. The backdoor was delivered to these internal endpoints as a DLL alongside legitimate executable files for antivirus software such as Norton Antivirus, Bkav Antivirus, and IObit Malware Fighter. This pattern of activity indicates that the attacker relied on DLL side-loading via legitimate antivirus software to execute their payloads. Salt Typhoon and similar groups have a history of employing this technique [4][5], enabling them to execute payloads under the guise of trusted software and bypassing traditional security controls.

Command-and-Control (C2)

The backdoor delivered by the threat actor leveraged **LightNode VPS endpoints** for C2, communicating over both **HTTP** and an unidentified **TCP-based protocol**. This dual-channel setup is consistent with Salt Typhoon's known use of non-standard and layered protocols to evade detection. The HTTP communications displayed by the backdoor included POST requests with an Internet Explorer User-Agent header and Target URI patterns such as "/17ABE7F017ABE7F0". One of the C2 hosts contacted by compromised endpoints was aar.gandhibludtric[.]com (38.54.63[.]75), a domain recently linked to Salt Typhoon [6].

Detection timeline

Darktrace produced **high confidence detections** in response to the early stages of the intrusion, with both the initial tooling and C2 activities being strongly covered by both investigations by Darktrace Cyber AI Analyst™ investigations and Darktrace models. Despite the sophistication of the threat actor, the intrusion activity identified and **remediated before escalating beyond these early stages of the attack, w**ith Darktrace's timely high-confidence detections likely playing a key role in neutralizing the threat.

Cyber AI Analyst observations

Darktrace's Cyber AI Analyst autonomously investigated the model alerts generated by Darktrace during the early stages of the intrusion. Through its investigations, Cyber AI Analyst discovered the initial tooling and C2 events and pieced them together into unified incidents representing the attacker's progression.

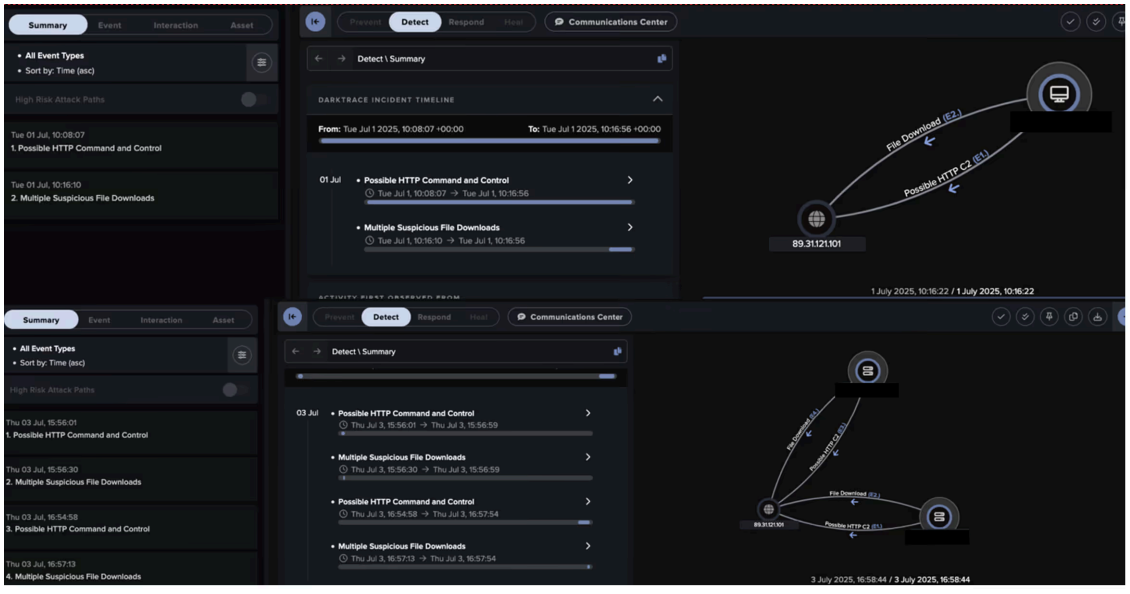

Figure 1: Cyber AI Analyst weaved together separate events from the intrusion into broader incidents summarizing the attacker's progression.

Conclusion

Based on overlaps in TTPs, staging patterns, infrastructure, and malware, Darktrace assesses with moderate confidence that the observed activity was consistent with Salt Typhoon/Earth Estries (ALA GhostEmperor/UNC2286). Salt Typhoon continues to challenge defenders with its stealth, persistence, and abuse of legitimate tools. As attackers increasingly blend into normal operations, detecting **behavioral anomalies** becomes essential for identifying subtle deviations and correlating disparate signals. The evolving nature of Salt Typhoon's tradecraft, and its ability to repurpose trusted software and infrastructure, ensures it will remain difficult to detect using conventional methods alone. This intrusion highlights the importance of **proactive defense**, where anomaly-based detections, not just signature matching, play a critical role in surfacing early-stage activity.

Credit to Nathaniel Jones (VP, Security & AI Strategy, FCISO), Sam Lister (Specialist Security Researcher), Emma Foulger (Global Threat Research Operations Lead), Adam Potter (Senior Cyber Analyst)

Edited by Ryan Traill (Analyst Content Lead)

Appendices

Indicators of Compromise (IoCs)

IoC-Type-Description + Confidence

89.31.121[.]101 – IP Address – Possible C2 server

hxxp://89.31.121[.]101:443/WINMM.dll - URI – Likely SNAPPYBEE download

b5367820cd32640a2d5e4c3a3c1ceedbbb715be2 - SHA1 – Likely SNAPPYBEE download

hxxp://89.31.121[.]101:443/NortonLog.txt - URI - Likely DLL side-loading activity

hxxp://89.31.121[.]101:443/123.txt - URI - Possible DLL side-loading activity

hxxp://89.31.121[.]101:443/123.tar - URI - Possible DLL side-loading activity

hxxp://89.31.121[.]101:443/pdc.exe - URI - Possible DLL side-loading activity

hxxp://89.31.121[.]101:443//Dialog.dat - URI - Possible DLL side-loading activity

hxxp://89.31.121[.]101:443/fltLib.dll - URI - Possible DLL side-loading activity

hxxp://89.31.121[.]101:443/DisplayDialog.exe - URI - Possible DLL side-loading activity

hxxp://89.31.121[.]101:443/DgApi.dll - URI - Likely DLL side-loading activity

hxxp://89.31.121[.]101:443/dbindex.dat - URI - Likely DLL side-loading activity

hxxp://89.31.121[.]101:443/1.txt - URI - Possible DLL side-loading activity

hxxp://89.31.121[.]101:443/imfsbDll.dll – Likely DLL side-loading activity

hxxp://89.31.121[.]101:443/imfsbSvc.exe - URI – Likely DLL side-loading activity

aar.gandhibludtric[.]com – Hostname – Likely C2 server

38.54.63[.]75 – IP – Likely C2 server

156.244.28[.]153 – IP – Possible C2 server

hxxp://156.244.28[.]153/17ABE7F017ABE7F0 - URI – Possible C2 activity

MITRE TTPs

Technique | Description

T1190 | Exploit Public-Facing Application - Citrix NetScaler Gateway compromise

T1105 | Ingress Tool Transfer – Delivery of backdoor to internal hosts

T1665 | Hide Infrastructure – Use of SoftEther VPN for C2

T1574.001 | Hijack Execution Flow: DLL – Execution of backdoor through DLL side-loading

T1095 | Non-Application Layer Protocol – Unidentified application-layer protocol for C2 traffic

T1071.001| Web Protocols – HTTP-based C2 traffic

T1571| Non-Standard Port – Port 443 for unencrypted HTTP traffic

Darktrace Model Alerts during intrusion

Anomalous File::Internal::Script from Rare Internal Location

Anomalous File::EXE from Rare External Location

Anomalous File::Multiple EXE from Rare External Locations

Anomalous Connection::Possible Callback URL

Antigena::Network::External Threat::Antigena Suspicious File Block

Antigena::Network::Significant Anomaly::Antigena Significant Server Anomaly Block

Antigena::Network::Significant Anomaly::Antigena Controlled and Model Alert

Antigena::Network::Significant Anomaly::Antigena Alerts Over Time Block

Antigena::Network::External Threat::Antigena File then New Outbound Block

References

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[2] https://www.trendmicro.com/en_gb/research/24/k/earth-estries.html

[3] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/k/earth-estries/IOC_list-EarthEstries.txt

[4] https://www.trendmicro.com/en_gb/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html

[5] https://lab52.io/blog/deedrat-backdoor-enhanced-by-chinese-apts-with-advanced-capabilities/

[6] https://www.silentpush.com/blog/salt-typhoon-2025/
