Salt Typhoon targeting telecommunications with new backdoor

Original report published on: 25 November 2024[1]

Executive summary

Earth Estries (aka Salt Typhoon, GhostEmperor, FamousSparrow and UNC2286) is a highly sophisticated Chinese APT group first seen in 2021. The group has conducted cyber-espionage campaigns targeting critical sectors such as telecommunications, government entities, and NGOs across Asia-Pacific, the Middle East, Africa, and the US. Leveraging vulnerabilities in public-facing servers to gain initial access, they employ advanced malware such as GHOSTSPIDER, SNAPPYBEE and MASOL RAT, alongside stealth techniques like living-off-the-land binaries and complex C2 infrastructure. Their evolving toolset, including a new variant of Demodex rootkit, highlights their capability for prolonged intrusions, operational agility, and significant overlaps with other Chinese APT groups, reflecting the use of shared tools and strategies.

Background

Earth Estries achieves initial access by exploiting vulnerabilities in public-facing servers, including Ivanti Connect Secure VPN (CVE-2023-46805 and CVE-2024-21887), Fortinet FortiClient (CVE-2023-48788), Sophos Firewall (CVE-2022-3236) and ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065). These exploits allow them to bypass authentication, execute arbitrary commands, and gain privileged access to target environments.

Once they have obtained a foothold, they employ living-off-the-land binaries (LOLBINs) such as WMI.exe and PSEXEC.exe for lateral movement while deploying custom malware to maintain persistence and control. They execute a multi-stage infection chain involving batch files or PowerShell scripts to deploy encrypted payloads, such as DEMODEX rootkit and GHOSTPSIDER backdoor, and MASOL RAT. Encrypted configurations and shellcode are stored in registry keys, while reflective loaders decrypt and execute these components in memory, evading detection.

GHOSTSPIDER is a multi-modular backdoor that uses TLS-secured communication protocol to connect with the C2 server. It begins with a stager deployed using DLL search order hijacking which then receives and executes additional payloads such as beacon loaders and additional modules. By isolating different capabilities across separate modules, GHOSTSPIDER operates with minimal forensic artifacts makes it challenging to detect.

An updated DEMODEX rootkit[2] was observed where the attacker replaced the first-stage PowerShell script with a CAB file containing the necessary registry data, including the encrypted configuration and shellcode payload. Once the installation is complete, the CAB file is deleted, to hinder forensics.

The researchers have linked an IP with a Linux backdoor associated with MASOL RAT while analysing this campaign. MASOL RAT was first identified in 2020 targeting Southeast Asian governments with evidence suggesting that it was developed in 2019, with Linux variant observed in use after 2021, while the Windows version has not been seen since.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Regularly update and patch public-facing servers to address exploited vulnerabilities such as:
  - ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)
  - Sophos Firewall (CVE-2022-3236)
  - Ivanti Connect Secure VPN (CVE-2023-46805, CVE-2024-21887)
  - Fortinet FortiClient (CVE-2023-48788)
- Implement monitoring for LOLBINs such as the use of `cmd.exe` with `wevutil` to output 4624 events (successful logon) for reconnaissance and `wmic.exe` to create process on another host for lateral movement.
- Deploy Endpoint Detection and Response (EDR) tools that can identify reflective loaders and in-memory malware execution.
- Use network segmentation to limit lateral movement and isolate critical assets.
- Conduct regular threat hunt based on MITRE ATT&CK Tactics and Techniques provided to proactively detect, investigate, and respond to adversarial behaviours.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise

Malware Hashes – SHA256	Remarks
fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5	SNAPPYBEE loader
fba149eb5ef063bc6a2b15bd67132ea798919ed36c5acda46ee9b1118b823098	SNAPPYBEE payload
2fd4a49338d79f4caee4a60024bcd5ecb5008f1d5219263655ef49c54d9acdec	DEMODEX PowerShell dropper
16c8afd3b35c76a476851f4994be180f0cd72c7b250e493d3eb8c58619587266	DEMODEX driver
9ba31dc1e701ce8039a9a272ef3d55aa6df66984a322e0d309614a5655e7a85c	DEMODEX loader
25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b	SNAPPYBEE loader
6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc	SNAPPYBEE loader
b2b617e62353a672626c13cc7ad81b27f23f91282aad7a3a0db471d84852a9ac	SNAPPYBEE loader
05840de7fa648c41c60844c4e5d53dbb3bc2a5250dcb158a95b77bc0f68fa870	SNAPPYBEE loader
1a38303fb392ccc5a88d236b4f97ed404a89c1617f34b96ed826e7bb7257e296	SNAPPYBEE payload

IP Address	Remarks

103[.]91[.]64[.]214	Campaign Alpha (DEMODEX)
165[.]154[.]227[.]192	Campaign Alpha (frpc)
23[.]81[.]41[.]166	Campaign Alpha (Open directory C&C)
158[.]247[.]222[.]165	Campaign Alpha (SNAPPYBEE)
172[.]93[.]165[.]14	Campaign Alpha (related C&C)
91[.]245[.]253[.]27	Campaign Alpha (SNAPPYBEE)
103[.]75[.]190[.]73	Campaign Alpha (related C&C)
45[.]125[.]67[.]144	Campaign Beta (DEMODEX)
43[.]226[.]126[.]164	Campaign Beta (DEMODEX)
172[.]93[.]165[.]10	Campaign Beta (DEMODEX)
193[.]239[.]86[.]168	Campaign Beta (DEMODEX)
146[.]70[.]79[.]18	Campaign Beta (DEMODEX)
146[.]70[.]79[.]105	Campaign Beta (DEMODEX)
205[.]189[.]160[.]3	Campaign Beta (DEMODEX)
96[.]9[.]211[.]27	Campaign Beta (DEMODEX)
43[.]226[.]126[.]165	Campaign Beta (DEMODEX)
139[.]59[.]108[.]43	Campaign Beta (GHOSTSPIDER)
185[.]105[.]1[.]243	Campaign Beta (GHOSTSPIDER)
143[.]198[.]92[.]175	Campaign Beta (GHOSTSPIDER)
139[.]99[.]114[.]108	Campaign Beta (GHOSTSPIDER)
139[.]59[.]236[.]31	Campaign Beta (GHOSTSPIDER)
104[.]194[.]153[.]65	Campaign Beta (GHOSTSPIDER)

Domain	**Remarks**
materialplies[.]com	Campaign Alpha (related C&C)
news[.]colourtinctem[.]com	Campaign Alpha (related C&C)
api[.]solveblemten[.]com	Campaign Alpha (SNAPPYBEE)
esh[.]hoovernamosong[.]com	Campaign Alpha (SNAPPYBEE)
vpn114240349[.]softether[.]net	Campaign Alpha (SoftEther VPN)
imap[.]dateupdata[.]com	Campaign Beta (DEMODEX)
pulseathermakf[.]com	Campaign Beta (DEMODEX)
www[.]infraredsen[.]com	Campaign Beta (DEMODEX)
billing[.]clothworls[.]com	Campaign Beta (GHOSTSPIDER)
helpdesk[.]stnekpro[.]com	Campaign Beta (GHOSTSPIDER)
jasmine[.]lhousewares[.]com	Campaign Beta (GHOSTSPIDER)
private[.]royalnas[.]com	Campaign Beta (GHOSTSPIDER)
telcom[.]grishamarkovgf8936[.]workers[.]dev	Campaign Beta (GHOSTSPIDER)
vpn305783366[.]softether[.]net	Campaign Beta (SoftEther VPN)
vpn487875652[.]softether[.]net	Campaign Beta (SoftEther VPN)
vpn943823465[.]softether[.]net	Campaign Beta (SoftEther VPN)

MITRE ATT&CK Tactics and Techniques

Tactics	**Technique ID**	**Technique Name**

Initial Access	T1190	Exploiting Public-Facing Application
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1047	Windows Management Instrumentation
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Defense Evasion	T1027	Obfuscated Files or Information
	T1574.001	DLL Search Order Hijacking
	T1014	Rootkit
	T1620	Reflective Code Loading
Lateral Movement	T1021.006	Remote Services: Windows Remote Management
Exfiltration	T1041	Exfiltration Over C2 Channel

References

1. **^** “Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions”
2. **^** “The Return of GhostEmperor’s Demodex”