Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Growing Threat of Earth Estries Group Behind Major Telecom Breaches

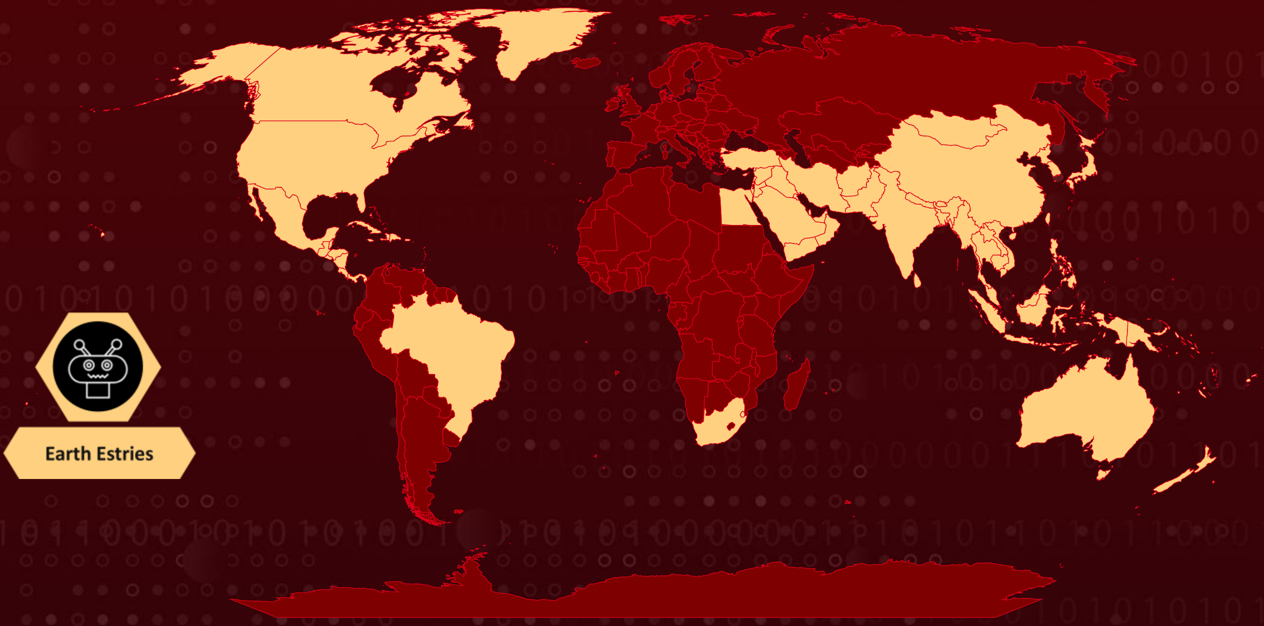
Date of Publication	Admiralty Code	TA Number
November 29, 2024	A1	TA2024447

Summary

Active Since: 2020
Threat Actor: Earth Estries (aka Salt Typhoon, FamousSparrow, GhostEmperor, UNC2286)
Malware: GHOSTSPIDER, SNAPPYBEE (aka Deed RAT), MASOL RAT
Attack Regions: APAC, Middle East, Africa, Parts of the Americas
Targeted Industries: Chemical, Consulting Firms, Government, Military, NGOs, Non-Profit Organizations, Technology, Telecommunications, Transportation

Attack: Earth Estries, also called Salt Typhoon, is a Chinese cyberespionage group that targets key sectors, including telecommunications, government organizations, and ISPs across the U.S., APAC, Middle East, and South Africa. Operating since 2020, the group takes advantage of vulnerabilities in public-facing servers, deploying tools like GhostSpider, SNAPPYBEE, and MASOL RAT for discreet, ongoing espionage campaigns.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 The Chinese cyberespionage group Earth Estries, also known as Salt Typhoon, has been identified utilizing advanced malware tools such as the GhostSpider backdoor, SNAPPYBEE, and MASOL RAT. Active since at least 2020, the group has conducted sustained attacks on governments and internet service providers.

#2 In 2023, its activities expanded to include critical sectors, notably telecommunications and government entities across the United States, the Asia-Pacific region, the Middle East, and South Africa. Earth Estries exploits vulnerabilities in public-facing servers to establish initial access.

#3 These tactics enable the deployment of customized malware for prolonged espionage. The group has reportedly compromised over 20 organizations spanning various industries. A significant focus of Earth Estries has been the deployment of MASOL RAT on Linux systems, with a particular emphasis on Southeast Asian government networks.

#4 By exploiting N-day vulnerabilities in public-facing servers, the group establishes control and uses LOLBINs to achieve lateral movement within compromised networks. Subsequently, they deploy malware such as SNAPPYBEE, DEMODEX, and GHOSTSPIDER to conduct long-term surveillance and data theft.

#5 GhostSpider, a modular and highly stealthy backdoor, is engineered specifically for prolonged espionage. Operating entirely in memory, it uses encryption to avoid detection. In addition to GhostSpider, Earth Estries employs a diverse toolkit of proprietary tools and shared utilities commonly used by other Chinese threat actors.

#6 This toolset supports sophisticated, multi-stage espionage operations targeting edge devices, on-premise infrastructure, and cloud environments. Recent campaigns have prominently targeted U.S.-based telecommunications companies, including T-Mobile USA, as well as ISPs across North America.

Recommendations

Enhance Server Vulnerability Management: Organizations should prioritize securing public-facing servers by regularly patching N-day vulnerabilities and using advanced threat detection tools to monitor for signs of exploitation. This includes configuring firewalls and implementing web application firewalls (WAF) to block unauthorized access attempts.

Implement Zero Trust Security Architecture: A Zero Trust model can help prevent unauthorized lateral movement within the network. By requiring continuous authentication and validation at every step, organizations can limit the ability of threat actors to move laterally and deploy additional malware once inside the network.

Deploy Integrity Monitoring on Critical Files and Processes: Monitor critical system files, processes, and configurations for unauthorized changes. For example, sudden changes to the regsvr32.exe or unusual DLL hijacking activities can signal the presence of backdoor tools like GhostSpider. File integrity monitoring (FIM) tools can help detect these changes in real time.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1071.001 Web Protocols	T1059.003 Windows Command Shell	T1112 Modify Registry	T1070.004 File Deletion

T1070 Indicator Removal	**T1027** Obfuscated Files or Information	**T1083** File and Directory Discovery	**T1005** Data from Local System
T1041 Exfiltration Over C2 Channel	**T1071** Application Layer Protocol	**T1053** Scheduled Task/Job	**T1047** Windows Management Instrumentation
T1588.002 Tool	**T1588** Obtain Capabilities	**T1105** Ingress Tool Transfer	**T1588.006** Vulnerabilities
T1587 Develop Capabilities	**T1587.001** Malware		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2b5e7b17fc6e684ff026df3241af4a651fc2b55ca62f8f1f7e34ac8303db9a31, 44ea2e85ea6cffba66f5928768c1ee401f3a6d6cd2a04e0d681d695f93cc5a1f, 6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc, 25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b, b63c82fc37f0e9c586d07b96d70ff802d4b707ffb2d59146cf7d7bb922c52e7e, fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5, fba149eb5ef063bc6a2b15bd67132ea798919ed36c5acda46ee9b1118b823098, 2fd4a49338d79f4caee4a60024bcd5ecb5008f1d5219263655ef49c54d9acdec, 16c8afd3b35c76a476851f4994be180f0cd72c7b250e493d3eb8c58619587266, 9ba31dc1e701ce8039a9a272ef3d55aa6df66984a322e0d309614a5655e7a85c, b2b617e62353a672626c13cc7ad81b27f23f91282aad7a3a0db471d84852a9ac,

TYPE	VALUE
SHA256	05840de7fa648c41c60844c4e5d53dbb3bc2a5250dcb158a95b77bc0f68fa870, 1a38303fb392ccc5a88d236b4f97ed404a89c1617f34b96ed826e7bb7257e296
File Name	NortonLog.txt, dbindex.dat, WINMM.dll, onedrived.ps1, DgApi.dll, imfsbDLL.dll
File Path	C:\Windows\System32\drivers\dumpfiskfss.sys, C:\Windows\System32\SstpCfs.dll
Domains	www[.]infraredsen[.]com, imap[.]dateupdata[.]com, materialplies[.]com, news[.]colourtinctem[.]com, api[.]solveblemten[.]com, esh[.]hoovernamosong[.]com, vpn114240349[.]softether[.]net, pulseathermakf[.]com, billing[.]clothworls[.]com, helpdesk[.]stnekpro[.]com, jasmine[.]lhousewares[.]com, private[.]royalnas[.]com, telcom[.]grishamarkovgf8936[.]workers[.]dev, vpn305783366[.]softether[.]net, vpn487875652[.]softether[.]net, vpn943823465[.]softether[.]net
IPv4:Port	141[.]255[.]164[.]98[:]2096
IPv4	23[.]81[.]41[.]166, 165[.]154[.]227[.]192, 158[.]247[.]222[.]165, 103[.]159[.]133[.]251, 27[.]102[.]113[.]240, 103[.]91[.]64[.]214, 172[.]93[.]165[.]14, 91[.]245[.]253[.]27, 103[.]75[.]190[.]73, 45[.]125[.]67[.]144, 43[.]226[.]126[.]164, 172[.]93[.]165[.]10, 193[.]239[.]86[.]168, 146[.]70[.]79[.]18,

TYPE	VALUE
IPv4	146[.]70[.]79[.]105, 205[.]189[.]160[.]3, 96[.]9[.]211[.]27, 43[.]226[.]126[.]165, 139[.]59[.]108[.]43, 185[.]105[.]1[.]243, 143[.]198[.]92[.]175, 139[.]99[.]114[.]108, 139[.]59[.]236[.]31, 104[.]194[.]153[.]65

CVEs

The Earth Estries threat actor strategically leveraged the following vulnerabilities to broaden its impact and target victims via compromised devices. For quick access, patch links for each exploited CVE are hyperlinked via the checkmarks labeled ‘Patch Link.’

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH LINK
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	✓	✓	✓
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClientEMS	✗	✓	✓
CVE-2022-3236	Sophos Firewall Code Injection Vulnerability	Sophos Firewall	✓	✓	✓
CVE-2021-26855	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH LINK
CVE-2021-26857	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-26858	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2021-27065	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓

References

https://www.trendmicro.com/en_us/research/24/k/earth-estries.html

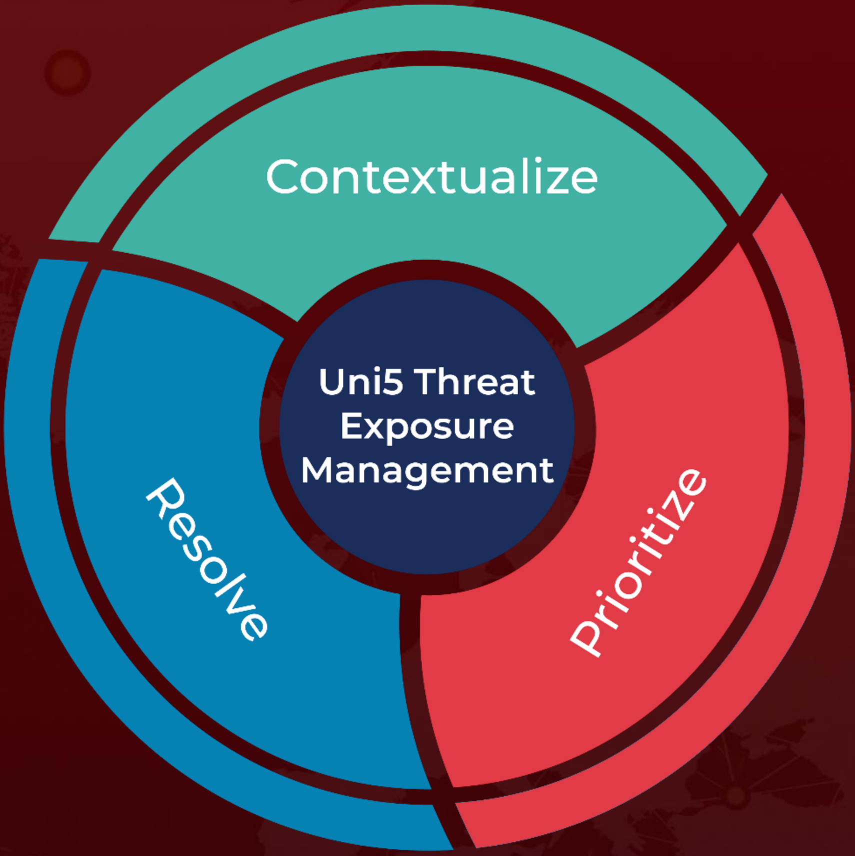
https://hivepro.com/threat-advisory/tropic-trooper-targets-middle-east-with-new-web-shell/

https://hivepro.com/threat-advisory/ghostemperor-the-threat-actor-who-outwits-security-measures/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 29, 2024 • 5:50 AM

More at www.hivepro.com