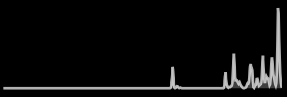
THREAT ACTOR FROM CHINA 🇨🇳

GhostEmperor

50+ mentions in the last 2 weeks



766 articles in the last 12 months

ⓘ Using open-source data collected by Feedly AI.

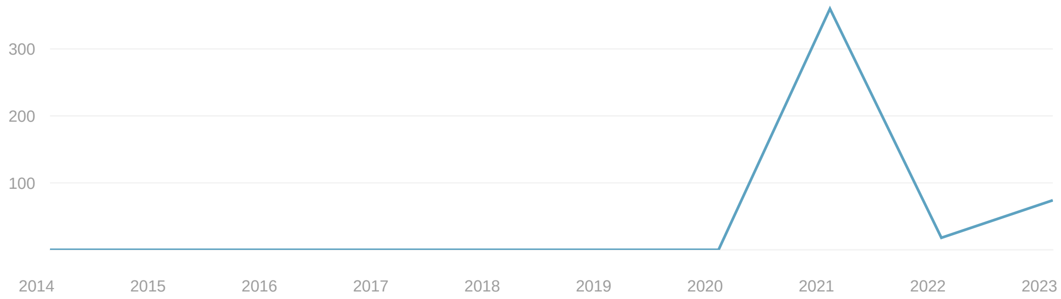
Overview

GhostEmperor is a notorious threat group known for its sophisticated Demodex rootkit. The group has recently resurfaced with an updated version of this rootkit, which features enhancements such as EDR evasion techniques and a reflective loader for executing the core implant. Their operations involve a multi-stage infection chain that starts with a seemingly innocuous batch file, ultimately leading... See More

Aliases

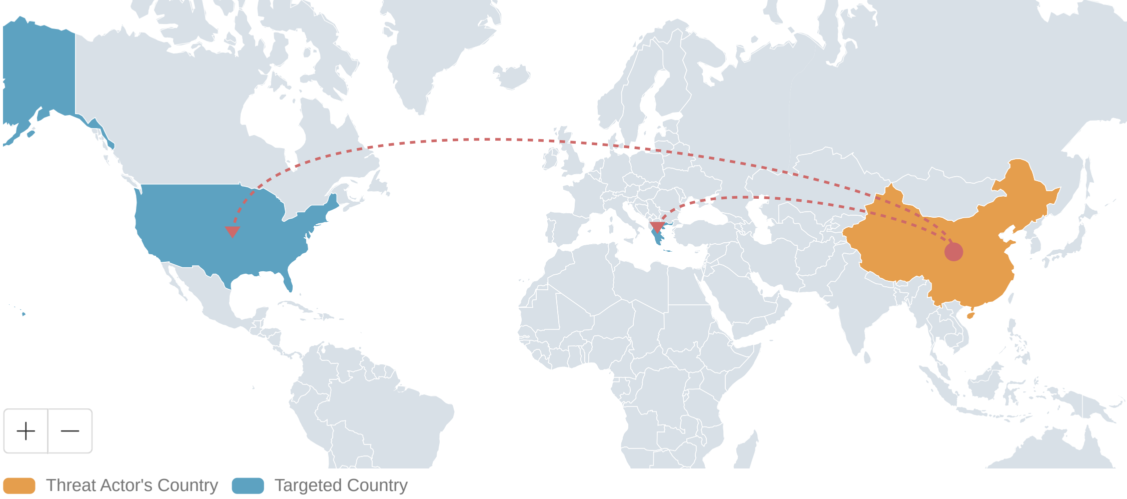
- Famous Sparrow
- Ghost Emperor
- Salt Typhoon
- UNC2286

Article count



Targets

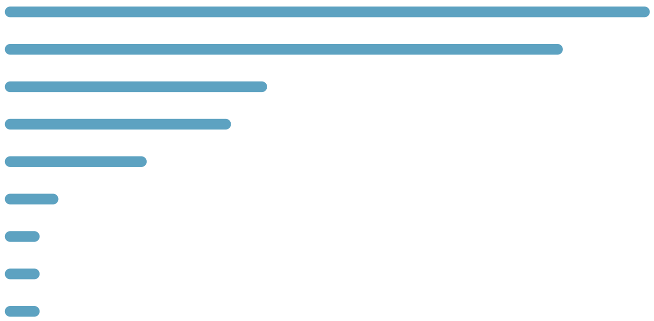
- Greece
- United States



Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED
Telecom 171 articles	Lumen Technologies	47	2 months ago
	Cisco	4	2 months ago
	On Telecoms	1	6 days ago
	Verizon	38	2 months ago
	AT&T	15	2 months ago
	T-Mobile US	66	20 days ago
Others 8 articles	US Telecommunications	8	59 days ago

Top malware families associated with this threat actor



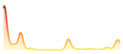
	Articles
Demodex	37
GhostSpider	32
MimiKatz	15
MASOL	13
SparrowDoor	8
Crowdoor	3
Cobalt Strike	2
Deed	2
ShadowPad	2

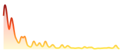
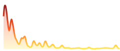
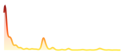
Tactics, Techniques, and Procedures

Last mentioned

TECHNIQUE	MITRE ID	PROCEDURES	MITIGATION	ARTICLES
Phishing ↑	T1566	29	5	14
Network Service Discovery	T1046	4	3	2
Local Accounts	T1078.003	1	2	1
Encrypted Channel ↑	T1573	21	2	15
Rootkit ↑	T1014	101	0	33
Command and Scripting Interpreter ↑	T1059	44	7	16
Ingress Tool Transfer	T1105	19	1	10
Asymmetric Cryptography	T1573.002	10	2	4
Reflective Code Loading	T1620	9	0	3

Exploited vulnerabilities

CVE ID	CVSS SCORE	EPSS SCORE	VENDOR	PRODUCT	TREND	EXPLOITED
CVE-2023-48788 A SQL injection vulnerability exists in Fortinet FortiClientEMS versions 7.2.0 through 7.2.2 and 7.0.1 through 7.0.10. This vulnerability…	CVSS 9.8	0%	Fortinet	forticlient_enterprise_management_server		Mar 13, 2024
CVE-2022-3236 A code injection vulnerability in the User Portal and Webadmin of Sophos Firewall version v19.0 MR1 and older allows a remote attack…	CVSS 9.8	12%	Sophos	firewall		-
CVE-2021-26855	CVSS 9.1	97%	Microsoft	exchange_server		Apr 6, 2022

This is a Server-Side Request Forgery (SSRF) vulnerability in Microsoft Exchange Server. It allows an unauthenticated attacker to send…						
CVE-2024-21887 A command injection vulnerability exists in web components of Ivanti Connect Secure (versions 9.x, 22.x) and Ivanti Policy Secure…	CVSS 9.1	97%	Ivanti	policy_secure		Jun 10, 2024
CVE-2023-46805 An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacke…	CVSS 8.2	96%	Ivanti	policy_secure		Jun 10, 2024
CVE-2021-26857 Microsoft Exchange Server Remote Code Execution Vulnerability. This vulnerability is related to deserialization of untrusted data…	CVSS 7.8	72%	Microsoft	exchange_server		May 5, 2022
CVE-2021-26858 Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854,…	CVSS 7.8	35%	Microsoft	exchange_server		May 5, 2022
CVE-2021-27065 This is a remote code execution vulnerability in Microsoft Exchange Server. It allows an attacker to execute arbitrary code on the…	CVSS 7.8	97%	Microsoft	exchange_server		Apr 6, 2022
CVE-2024-20399 A vulnerability in the CLI of Cisco NX-OS Software allows an authenticated, local attacker with Administrator credentials to…	CVSS 6.7	0%	Cisco	nx-os		-

Threat intelligence reports

Salt Typhoon Threat Group

Threat Actors • Intel471 / 5d • Threat Intelligence Reports •

18 TTPs

The provided logic looks for single character batch script (.bat) file names found in the command line arguments of a process execution. This Hunt Package aims to identify potential DLL side-loading activity by searching for when an executable…

News

Checklist 403: The FBI, Salt Typhoon, and Encryption

Use encrypted apps against hackers • SecureMac by SecureMac Team / 5h

In a striking reversal of past positions, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) are now advising Americans to use end-to-end encrypted apps such as iMessage and FaceTime to safeguard against…

Also in NBC News Technology, NCSC, +46 feeds

China's Salt Typhoon recorded top American officials' calls, says White House

China-linked hackers target US officials •

The Register – Security by Jessica Lyons / 6h

the actual number of calls that they took, recorded and took, was really more focused on very senior political individuals," Neuberger said, according to media reports. During the Bahrain event, she told reporters that the Salt Typhoon…

Also in The Register, Techmeme, +38 feeds

Trump’s pick to run FCC deeply concerned about Salt Typhoon

FCC proposes cybersecurity rules after hack •

Cybersecurity Dive - Latest News by Matt Kapko / 8h

President-elect Donald Trump’s pick to chair the Federal Communications Commission, Brendan Carr, said he is deeply concerned about the recently uncovered swarm of attacks on U.S. telecom companies . Carr’s comments ab…

Also in Bug bounty programs, lightreading, +85 feeds

Salt Typhoon hack targeted senior US politicians, says Neuberger

↗ China-linked hackers target US officials •

SCM feed for Latest by SC Staff / 8h

Despite the intrusions believed to have resulted in the exfiltration of Americans' metadata, such an operation was highly targeted against senior political players, noted Neuberger during the Manama Dialogue security conference in Bahrain.

Also in The Register, Techmeme, +92 feeds

U.S. Officials Sound Alarm Over Salt Typhoon Hack as Cybersecurity Becomes Political Flashpoint

↗ Chinese hackers breach US telecom networks •

CySecurity News - Latest Information Sec... by Shivani Tiwari / 9h

U.S. Officials Urge Encryption Adoption Amid "Salt Typhoon" Cyberattack In an unprecedented response to the "Salt Typhoon" cyber intrusion, top cybersecurity and law enforcement officials in the U.S. are urging citizens to adopt encrypted…

Also in WTOP News, Morphisec Press Rele..., +22 feeds

9th December – Threat Intelligence Report

3 CVEs • Check Point Research by hagarb / 11h • 12 TTPs

Stoli Group USA has filed for Chapter 11 bankruptcy after an August 2024 ransomware attack severely disrupted its IT infrastructure, forcing manual operations and hindering financial reporting. ENGlobal Corporation, an energy…

See 44 more articles and social media posts

Made with feedly