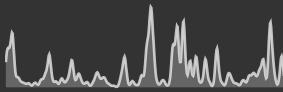



THREAT ACTOR

Scattered Spider

14 mentions in the last 2 weeks



1K articles in the last 12 months

 Using open-source data collected by Feedly AI.

Overview

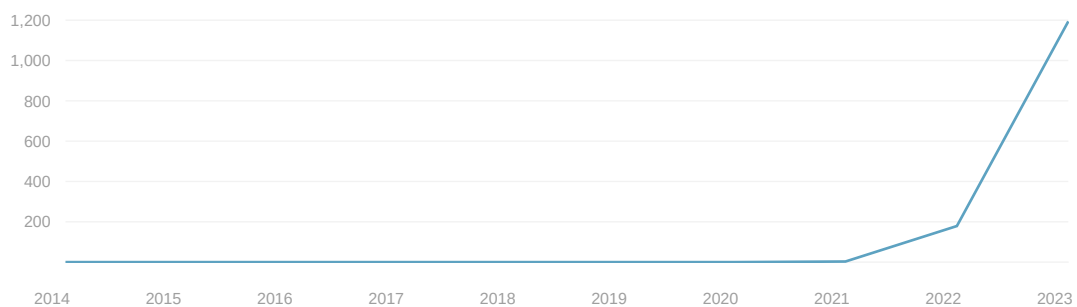
Scattered Spider is a financially motivated cybercriminal group known for its sophisticated and multifaceted cyber attacks, primarily targeting large enterprises and their supply chains. The group operates under various aliases, including UNC3944, Oktapus, Muddled Libra, Octo Tempest, and Scatter Swine. They have gained notoriety for employing advanced social engineering techniques, particularly i... [See More](#)

Aliases

- Oktapus
- DEV-0971
- Muddled Libra
- Octo Tempest

[See 7 more aliases](#)

Article count



Targets

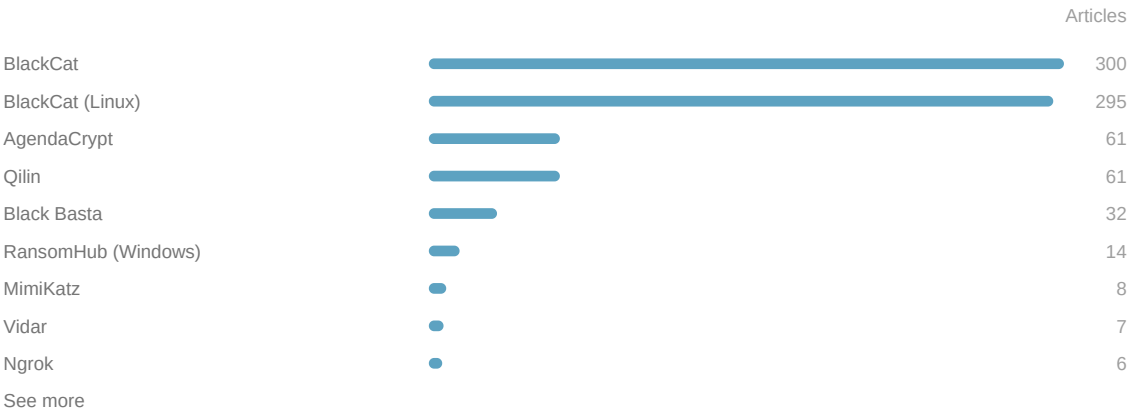
- United States



Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED
Finance 14 articles	<ul style="list-style-type: none">Change HealthcareCoinbase	3 11	4 months ago 21 months ago
Healthcare 5 articles	<ul style="list-style-type: none">Change HealthcareUnitedHealth Group	3 2	4 months ago 7 months ago
Gambling 173 articles	<ul style="list-style-type: none">Caesars EntertainmentMGM Resorts InternationalMandalay Bay	59 113 1	15 months ago 15 months ago 18 days ago
Lodging 113 articles	<ul style="list-style-type: none">MGM Resorts International	113	15 months ago
Travel & Hospitality 113 articles	<ul style="list-style-type: none">MGM Resorts International	113	15 months ago
Tech 27 articles	<ul style="list-style-type: none">OktaTwilioKlaviyoSnowflakeCloudflare	6 16 1 2 2	21 months ago 27 months ago 24 months ago 5 months ago 21 months ago
Telecom 18 articles	<ul style="list-style-type: none">TwilioCloudflare	16 2	27 months ago 21 months ago
Advertising 1 article	<ul style="list-style-type: none">Klaviyo	1	24 months ago
Retail 1 article	<ul style="list-style-type: none">Klaviyo	1	24 months ago
Insurance 3 articles	<ul style="list-style-type: none">UnitedHealth GroupTransamerica Corporation	2 1	7 months ago 7 months ago
Gaming 3 articles	<ul style="list-style-type: none">Riot Games	3	18 days ago
Food 11 articles	<ul style="list-style-type: none">CloroxDoorDash	8 3	14 months ago 27 months ago
Media & Entertainment 2 articles	<ul style="list-style-type: none">Cloudflare	2	21 months ago
Others 2 articles	<ul style="list-style-type: none">VMware vCenter	2	51 days ago

Top malware families associated with this threat actor



Tactics, Techniques, and Procedures

Last mentioned ▾

TECHNIQUE	MITRE ID	PROCEDURES	MITIGATION	ARTICLES
Phishing ↑	T1566	<u>1380</u>	<u>5</u>	<u>255</u>
Valid Accounts ↑	T1078	<u>221</u>	<u>7</u>	<u>66</u>
Financial Theft ↑	T1657	<u>511</u>	<u>2</u>	<u>132</u>
Impersonation	T1656	<u>183</u>	<u>2</u>	<u>62</u>
Multi-Factor Authentication Request Generation	T1621	<u>174</u>	<u>3</u>	<u>43</u>
Phishing for Information	T1598	<u>35</u>	<u>2</u>	<u>13</u>
Cloud Service Hijacking	T1496.004	<u>3</u>	0	<u>2</u>
Malicious Link	T1204.001	<u>30</u>	<u>3</u>	<u>6</u>
Obfuscated Files or Information	T1027	<u>28</u>	<u>4</u>	<u>9</u>

Exploited vulnerabilities

CVE ID	CVSS SCORE ⬇	EPSS SCORE ⬇	VENDOR	PRODUCT	TREND	EXPLOITED ⬇
CVE-2024-37085 VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions...	CVSS 7.2	0%	Vmware	esxi		Sep 25, 2024
CVE-2015-2291 The Intel Ethernet diagnostics driver (IQVW32.sys and IQVW64.sys) for Windows before version 1.3.1.0 has an improper input...	High	0%	Intel	ethernet_diagnostics_driver_iqvw32.sys		Apr 6, 2022

Detection Rules

RULE	ARTICLES	COUNT	ACTION
Sigma rules	<u>1</u>	1	<div>Download</div>

Threat intelligence reports



Investigating Oktapus: Phishing Analysis & Detection
by jnazario / 13d
submitted by /u/jnazario [link] [comments]



Scattered Spider x RansomHub: A New Partnership
 • by netbiosX / 31d
submitted by /u/netbiosX [link] [comments]

News



⚡ THN Recap: Top Cybersecurity Threats, Tools and Tips (Dec 2 - 8)
 New Malware > DroidBot •
27 The Hacker News by info@thehackernews.com (The Hacker News) / 11h •
 18 CVEs • 22 TTPs
"This phase is crucial for attackers to achieve their ultimate objectives, which might include data exfiltration, persistence or further system compromise." The disclosure comes as new research has revealed how the legitimate Windows...



Alleged Scattered Spider hacker arrested, indicted

↗ [Scattered Spider hacker arrested again](#) •

SCM feed for Latest by SC Staff / 14h

Nearly 150 employees of the financial entity have been compromised by Ogletree in a phishing campaign between October and November 2023 that sought to exfiltrate account credentials via company-spoofing phishing sites, the complain...

Also in GamblingNews, Factiva / Kryptot, +6 feeds



Another teenage hacker charged as feds continue Scattered Spider crackdown | The Record from Recorded Future News

55 1d

submitted by /u/anynamewillbegood [link] [comments]



Texas Teen Arrested for Scattered Spider Telecom Hacks

↗ [California teen linked to Scattered Spider](#) •

darkreading by Becky Bracken, Senior Editor, Dark Reading / 3d

An FBI operation nabbed a member of the infamous cybercrime group, who is spilling the tea on "key Scattered Spider members" and their tactics.

Also in darkreading, Bloomberg Law Privac..., +27 feeds



Recently Charged Scattered Spider Suspect Did Poor Job at Covering Tracks

🕸 10 TTPs • SecurityWeek by Eduard Kovacs / 3d •

↗ [California teen linked to Scattered Spider](#)

A California teen suspected of being a Scattered Spider member left a long trail of evidence and even used an FBI service to launder money.

Also in The Record from Reco..., RSS reader not yet w..., +33 feeds



US arrests Scattered Spider suspect linked to telecom hacks

🕸 loC > 2 domains • 3d • 🕸 9 TTPs •

↗ [California teen linked to Scattered Spider](#)

submitted by /u/arqf_ [link] [comments]

[See 43 more articles and social media posts](#)