Hive Pro

Threat Level

Red

CISA: AA23-320A

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

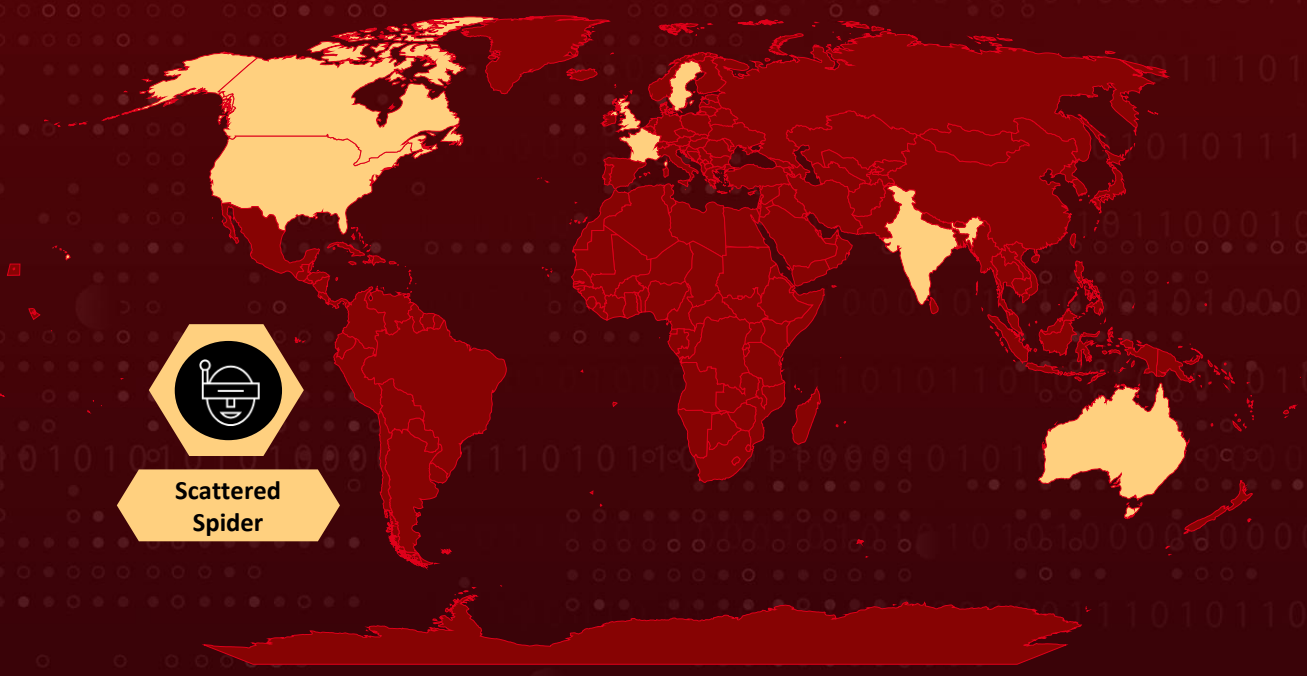
Scattered Spider Cyber Threat Key Findings and Security Measures

Date of Publication	Last updated date	Admiralty code	TA Number
November 17, 2023	June 20, 2025	A1	TA2023466

Summary

First Appearance: May 2022
Attack Region: United States, Canada, United Kingdom, Singapore, India, France, Sweden, and Australia
Malware: BlackCat/ALPHV Ransomware, AveMaria, Raccoon Stealer, VIDAR Stealer, Spectre RAT, DragonForce Ransomware, RansomHub Ransomware, Qilin Ransomware
Threat Actor: Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest and 0ktapus)
Targeted Industries: Commercial facilities, Telecommunications, Technology, Business-Process Outsourcing (BPO), Financial services, Hospitality, Media and entertainment, Healthcare, Retail, Insurance, Managed Service Providers (MSPs), Manufacturing, Cryptocurrency, and Food services
Affected Platform: Windows

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2015-2291	Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2021-35464	ForgeRock Access Management (AM) Core Server Remote Code Execution Vulnerability	ForgeRock Access Management (AM) Core Server	✗	✓	✓
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi	✗	✓	✓

Actor Details

#1 Scattered Spider, a cybercriminal group primarily targets commercial facilities sectors and subsectors, specializing in data theft for extortion and utilizing BlackCat/ALPHV ransomware. Scattered Spider employs social engineering techniques, such as phishing, push bombing, and SIM swap attacks, to obtain credentials.

#2 The threat actors register their own multi-factor authentication (MFA) tokens for persistence, perform privileged escalation, and leverage common endpoint detection and response (EDR) tools for remote access and command execution. They conduct discovery, lateral movement, and exfiltration, targeting specific information like SharePoint sites, credential storage documentation, and code repositories.

#3 The threat actors pose as IT or helpdesk staff to gain access to networks, often using legitimate tools like Fleetdeck.io and Teamviewer. Additionally, they use malware like AveMaria, Raccoon Stealer, and VIDAR Stealer for remote access and data theft.

#4 Scattered Spider is known to join incident response calls and teleconferences, potentially to identify how security teams are responding to their activities and proactively develop new intrusion avenues. The group may also create new identities in the environment, supported by fake social media profiles. Scattered Spider is known for major breaches like the Twilio/Okta incident and the MGM breach.

#5

In recent campaigns, Scattered Spider has expanded its focus to include large retailers, insurance companies, and telecommunications providers—most notably in the UK and North America. Noteworthy incidents in early 2025 included attacks on prominent UK brands such as Marks & Spencer, Co-op, and others, resulting in operational disruptions and the exfiltration of sensitive data. These attacks involved the use of adversary-in-the-middle (AiTM) phishing kits, ESXi ransomware payloads, and partnerships with newer ransomware groups like DragonForce and RansomHub.

#6

The group's updated toolkit includes remote access tools like Atera Agent, AnyDesk, and Splashtop, alongside modern C2 frameworks. They have also deployed newer malware families like Lumma Stealer, and Spectre RAT, in addition to their legacy tools. Despite multiple arrests of group affiliates in late 2024, Scattered Spider rapidly restructured and resumed operations, now showing signs of increased automation and AI-driven phishing techniques, indicating continued evolution and high operational maturity.

Actor Group

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGET REGIONS</th><th>TARGET INDUSTRIES</th></tr>
<tr><td rowspan="3">Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest and 0ktapus)</td><td>Suspected English speaking US and UK individuals</td><td rowspan="3">United States, Canada, United Kingdom, Singapore, India, France, Sweden, and Australia</td><td rowspan="3">Commercial facilities, Telecommunications, Technology, Business-Process Outsourcing (BPO), Financial services, Hospitality, Media and entertainment, Healthcare, Retail, Insurance, Managed Service Providers (MSPs), Manufacturing, Cryptocurrency, and Food services</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain</td></tr>
</table>

Recommendations

Patch Management: Ensuring that all systems, especially those exposed to the internet are updated promptly with the latest security patches is essential. Regular vulnerability assessments and automated patch deployment can minimize the window of opportunity for adversaries to exploit known vulnerabilities.

Harden Identity and Access Controls: Enforce strong multi-factor authentication (MFA) across all accounts, prioritizing phishing-resistant methods such as FIDO2 tokens or certificate-based smart cards. Monitor for and block rogue MFA registrations, especially following helpdesk interactions or high-privilege access changes. Implement conditional access policies to restrict access based on device posture, IP reputation, and geographic context.

Monitoring and Detection: Enhancing network visibility and monitoring can significantly improve an organization's defensive posture. Deploying advanced security monitoring tools and integrating threat intelligence feeds enable rapid detection of suspicious activities. Continuous logging and real-time analysis of network traffic, combined with periodic security audits, provide a robust mechanism to uncover potential breaches in the early stages.

Network Segmentation: Proper network segmentation limits the damage that can be done if an attacker gains access to one part of the system. By segmenting critical infrastructure from less sensitive data, organizations can better contain breaches and make lateral movement more difficult for attackers.

Enhance Social Engineering Defenses: Conduct regular simulated phishing exercises and user awareness training, particularly focused on helpdesk impersonation and MFA fatigue tactics. Deploy browser isolation or email security solutions with link rewriting and AI-based detection to counter adversary-in-the-middle (AiTM) phishing kits. Verify all internal IT/helpdesk requests through out-of-band verification channels.

Reduce Remote Access Tool Threats: Audit remote access tools on the network to identify currently used and authorized software. Review logs for abnormal use of remote access software running as a portable executable. Use security software to detect instances of remote access software being loaded only in memory.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	TA0040 Impact	T1657 Financial Theft	T1567 Exfiltration Over Web Service
T1585.001 Social Media Accounts	T1585 Establish Accounts	T1566 Phishing	T1660 Phishing
T1566.004 Spearphishing Voice	T1199 Trusted Relationship	T1078.002 Domain Accounts	T1078 Valid Accounts
T1648 Serverless Execution	T1204 User Execution	T1136 Create Account	T1556.006 Multi-Factor Authentication
T1556 Modify Authentication Process	T1484.002 Domain Trust Modification	T1484 Domain Policy Modification	T1578.002 Create Cloud Instance
T1578 Modify Cloud Compute Infrastructure	T1656 Impersonation	T1606 Forge Web Credentials	T1621 Multi-Factor Authentication Request Generation
T1552.001 Credentials In Files	T1552.004 Private Keys	T1552 Unsecured Credentials	T1217 Browser Bookmark Discovery
T1538 Cloud Service Dashboard	T1083 File and Directory Discovery	T1018 Remote System Discovery	T1539 Steal Web Session Cookie

T1021 Remote Services	T1021.007 Cloud Services	T1213.003 Code Repositories	T1213.002 Sharepoint
T1526 Cloud Service Discovery	T1218 System Binary Proxy Execution	T1562 Impair Defenses	T1568 Dynamic Resolution
T1003 OS Credential Dumping	T1036 Masquerading	T1041 Exfiltration Over C2 Channel	T1071 Application Layer Protocol
T1213 Data from Information Repositories	T1074 Data Staged	T1114 Email Collection	T1530 Data from Cloud Storage
T1219 Remote Access Software	T1486 Data Encrypted for Impact	T1567.002 Exfiltration to Cloud Storage	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1e5ad5c2ffffac9d3ab7d179566a7844, 56fd7145224989b92494a32e8fc6f6b6, 6639433341fd787762826b2f5a9cb202, 828699b4133acb69d34216dcd0a8376e, 9a218d69ecafe65eae264d2fdb52f1aa, d44071f255785c73909d64f824331ebf, b97812a2e6be54e725defbab88357fa2
SHA1	0272b018518fef86767b01a73213716708acbb80, 10b9da621a7f38a02fea26256db60364d600df85, d8cb0d5bbeb20e08df8d2e75d7f4e326961f1bf5, ec37d483c3c880fadc8d048c05777a91654e41d3,

TYPE	VALUE
SHA256	4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93, 443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58, 982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46dada624af0316044e, acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918, cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005
IPv4	159[.]223[.]213[.]174, 169[.]150[.]203[.]51, 37[.]19[.]200[.]142, 37[.]19[.]200[.]155, 144[.]76[.]136[.]153, 119[.]93[.]5[.]239, 146[.]70[.]103[.]228, 185[.]195[.]19[.]206, 198[.]54[.]133[.]45, 198[.]54[.]133[.]52, 37[.]19[.]200[.]151, 45[.]134[.]140[.]177, 45[.]86[.]200[.]81, 89[.]46[.]114[.]66, 100[.]35[.]70[.]106, 136[.]144[.]19[.]51, 136[.]144[.]43[.]81, 142[.]93[.]229[.]86, 143[.]244[.]214[.]243, 146[.]70[.]107[.]71, 146[.]70[.]112[.]126, 146[.]70[.]127[.]42, 146[.]70[.]45[.]166, 146[.]70[.]45[.]182, 152[.]89[.]196[.]111, 162[.]118[.]200[.]173, 172[.]98[.]33[.]195, 173[.]239[.]204[.]129, 173[.]239[.]204[.]130, 173[.]239[.]204[.]131, 173[.]239[.]204[.]132, 173[.]239[.]204[.]133, 173[.]239[.]204[.]134, 180[.]190[.]113[.]87, 185[.]120[.]144[.]101, 185[.]123[.]143[.]197,

TYPE	VALUE
IPv4	185[.]123[.]143[.]201, 185[.]123[.]143[.]205, 185[.]123[.]143[.]217, 185[.]156[.]46[.]141, 185[.]163[.]109[.]66, 185[.]181[.]102[.]18, 185[.]195[.]19[.]207, 185[.]202[.]220[.]239, 185[.]202[.]220[.]65, 185[.]240[.]244[.]3, 185[.]247[.]70[.]229, 185[.]45[.]15[.]217, 185[.]56[.]80[.]28, 188[.]166[.]101[.]65, 188[.]166[.]117[.]31, 188[.]214[.]129[.]7, 192[.]166[.]244[.]248, 193[.]27[.]13[.]184, 193[.]37[.]255[.]114, 194[.]37[.]96[.]188, 195[.]206[.]105[.]118, 198[.]44[.]136[.]180, 217[.]138[.]198[.]196, 217[.]138[.]222[.]94, 23[.]106[.]248[.]251, 31[.]222[.]238[.]70, 45[.]132[.]227[.]211, 45[.]132[.]227[.]213, 45[.]91[.]21[.]61, 5[.]182[.]37[.]59, 51[.]210[.]161[.]12, 51[.]89[.]138[.]221, 62[.]182[.]98[.]170, 64[.]190[.]113[.]28, 67[.]43[.]235[.]122, 68[.]235[.]43[.]20, 68[.]235[.]43[.]21, 82[.]180[.]146[.]31, 89[.]46[.]114[.]164, 91[.]242[.]237[.]100, 93[.]115[.]7[.]238, 98[.]100[.]141[.]70

TYPE	VALUE
IPv4	98[.]100[.]141[.]70, 138[.]68[.]27[.]0, 195[.]206[.]107[.]147, 193[.]149[.]129[.]177, 188[.]166[.]92[.]55, 188[.]166[.]101[.]65
CIDR	18[.]206[.]107[.]24/29
Domains	victimname-sso[.]com, victimname-servicedesk[.]com, victimname-okta[.]com, 7-eleven-hr[.]com, activecampiagn[.]net, acwa-apple[.]com, bbtplus[.]com, bell-hr[.]com, bestbuy-cdn[.]com, birdsso[.]com, citrix-okta[.]com, commonspiritcorp-okta[.]com, consensys-okta[.]com, corp-hubspot[.]com, cts-comcast[.]com, doordash-support[.]com, duelbits-cdn[.]com, freshworks-hr[.]com , gemini-sso[.]com, gucci-cdn[.]com, itbit-okta[.]com, iyft[.]net, klaviyo-hr[.]com , login[.]freshworks-hr[.]com, login[.]hr-intercom[.]com, morningstar-okta[.]com, mytsl[.]net, okta-ziffdavis[.]com, pfchangs-support[.]com, prntsrc[.]net, pure-okta[.]com, signin-nydig[.]com, simpletexting-cdn[.]com, squarespacehr[.]com, sytemstern[.]net, sso-instacart[.]com, sts-vodafone[.]com,

TYPE	VALUE
Domains	twitter-okta[.]com, xn--gryscale-ox0d[.]com, x-sso[.]com

Patch Links

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html

https://backstage.forgerock.com/knowledge/advisories/article/a47894244

https://support.broadcom.com/

https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/release-notes/esxi-update-and-patch-release-notes/vsphere-esxi-803-release-notes.html

https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/5-2/vcf-release-notes/vmware-cloud-foundation-52-release-notes.html

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

https://www.hivepro.com/threat-advisory/attackers-target-telecommunications-sector-to-gain-network-access/

https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations?e=48754805

https://www.silentpush.com/blog/scattered-spider-2025/

https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-insights-history-and-mitigations-for-scattered-spider/

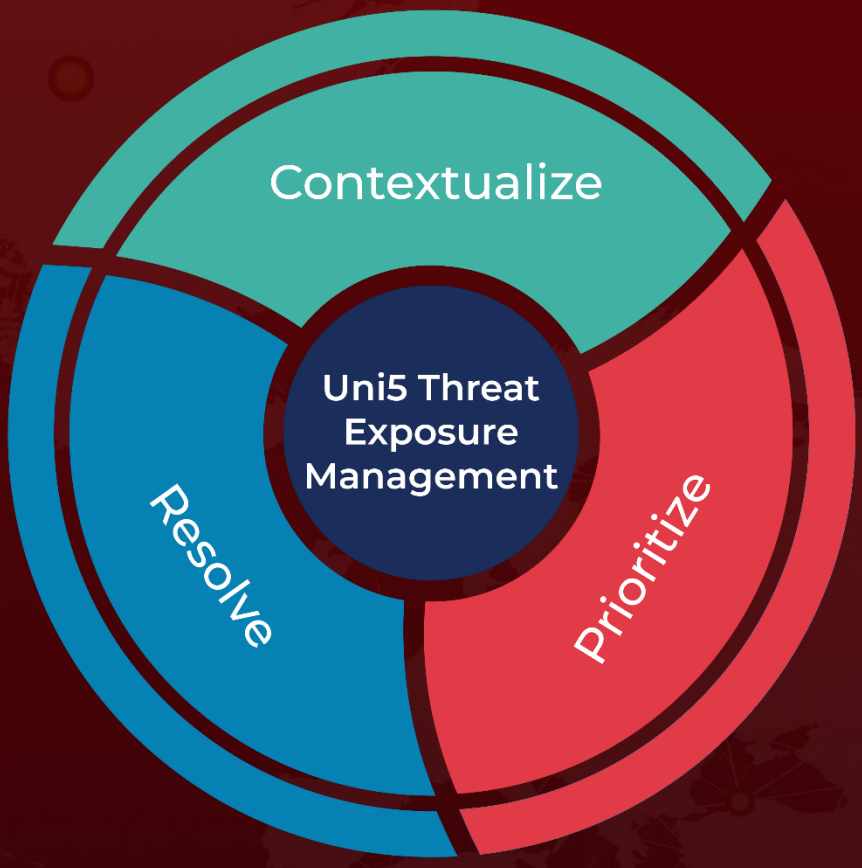
https://www.quorumcyber.com/threat-intelligence/scattered-spider-targets-us-insurance-sector-in-new-ransomware-wave/

https://cyberint.com/blog/dark-web/meet-scattered-spider-the-group-currently-scattering-uk-retail-organizations/#CVEs

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 17, 2023 . 5:00 AM

More at www.hivepro.com