Hive Pro®

Threat Level

Red

CISA: AA23-320A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

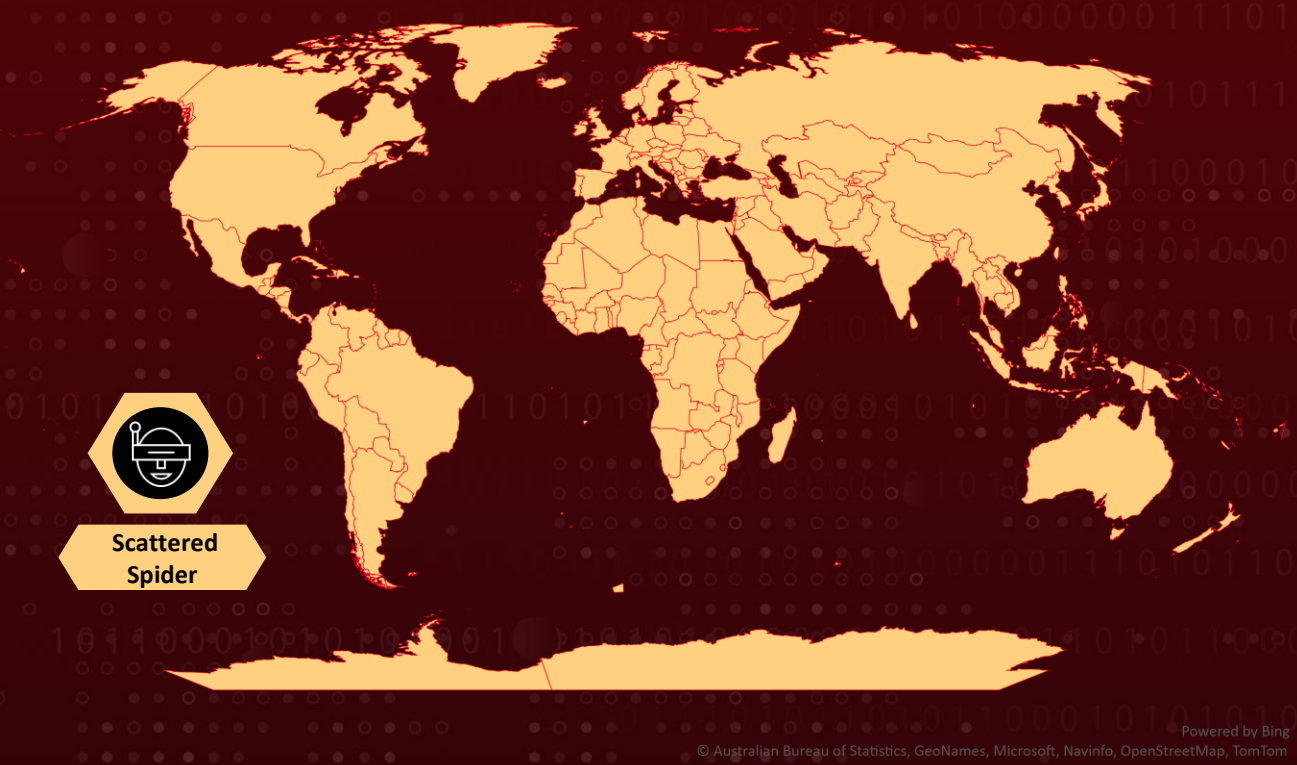
Scattered Spider Cyber Threat Key Findings and Security Measures

Date of Publication	Last Updated Date	Admiralty Code	TA Number
November 17, 2023	December 15, 2023	A1	TA2023466

Summary

First Appearance: June 2022
Attack Region: Worldwide
Malware: BlackCat/ALPHV Ransomware, AveMaria, Raccoon Stealer, and VIDAR Stealer
Threat Actor: Scattered Spider (Starfraud, UNC3944, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, and Muddled Libra)
Targeted Industries: Commercial facilities, Telecommunications, Technology, Business-Process Outsourcing (BPO), Financial, Insurance, Investment, Retail, Entertainment, Food ordering and delivery
Attack: A cybercriminal group, Scattered Spider, known for targeting commercial facilities, highlighting their evolving tactics, social engineering expertise, phishing, and SIM swap attacks, evolving techniques like file encryption post-exfiltration to maintain persistence and adapt to security measures.

Attack Regions



Attack 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 and has been expanding its infrastructure and launching new phishing attacks.

#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 such as 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.

Recommendations

Multi-Factor Authentication (MFA) Best Practices: Implement and enforce multi-factor authentication across all systems and applications.

Phishing and Smishing Protections: Deploy advanced email filtering solutions to detect and block phishing attempts. Implement SMS filtering and awareness programs to minimize the success of smishing attacks.

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.

Enhance Endpoint Security: Utilize advanced endpoint protection solutions, such as antivirus and endpoint detection and response (EDR) tools, to detect and prevent malware infections. Ensure that security software is regularly updated and configured to provide optimal protection.

Network Monitoring and Anomaly Detection: Implement continuous network monitoring to detect unusual activities, especially the use of legitimate tools for malicious purposes. Utilize anomaly detection systems to identify deviations from normal network behavior.

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
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
SHA1	0272b018518fef86767b01a73213716708acbb80, 10b9da621a7f38a02fea26256db60364d600df85, d8cb0d5bbeb20e08df8d2e75d7f4e326961f1bf5, ec37d483c3c880fadc8d048c05777a91654e41d3,
SHA256	4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93, 443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58,

TYPE	VALUE
SHA256	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, 185[.]123[.]143[.]201, 185[.]123[.]143[.]205, 185[.]123[.]143[.]217, 185[.]156[.]46[.]141,

TYPE	VALUE
IPv4	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
CIDR	18[.]206[.]107[.]24/29
Domains	victimname-okta[.]com, 53help[.]org, workatbbt[.]com, bbtplus[.]com, dashsso[.]com,

TYPE	VALUE
Domains	telnyx-sso[.]com, bbt-hr[.]com, grayscale-sso[.]com, ssopodium[.]com, telnyxsso[.]com, trustsso[.]com, freshworks-sso[.]net, bbtemps[.]com, freshworksso[.]com, grayscalesso[.]com, freshworks-sso[.]com, postmarksso[.]com, ssotelnyx[.]com, cashsso[.]com, hubsso[.]net, intercomsso[.]net, podiumsso[.]com, klaviyocorp[.]net, graysso[.]com, att-my[.]com, bbtvpn[.]com, telesignsso[.]com, aitice-usa[.]com, att-networks[.]net, connect-cox[.]com, asurionsso[.]com, fedsso[.]net, victrasso[.]net, activesso[.]comassurionsso[.]net, actlvecampaign[.]net, gryscale-ox0d[.]com, workbbt[.]com, victrasso[.]com, bbt-work[.]com, my-twilio[.]com, bbthour[.]com

References

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

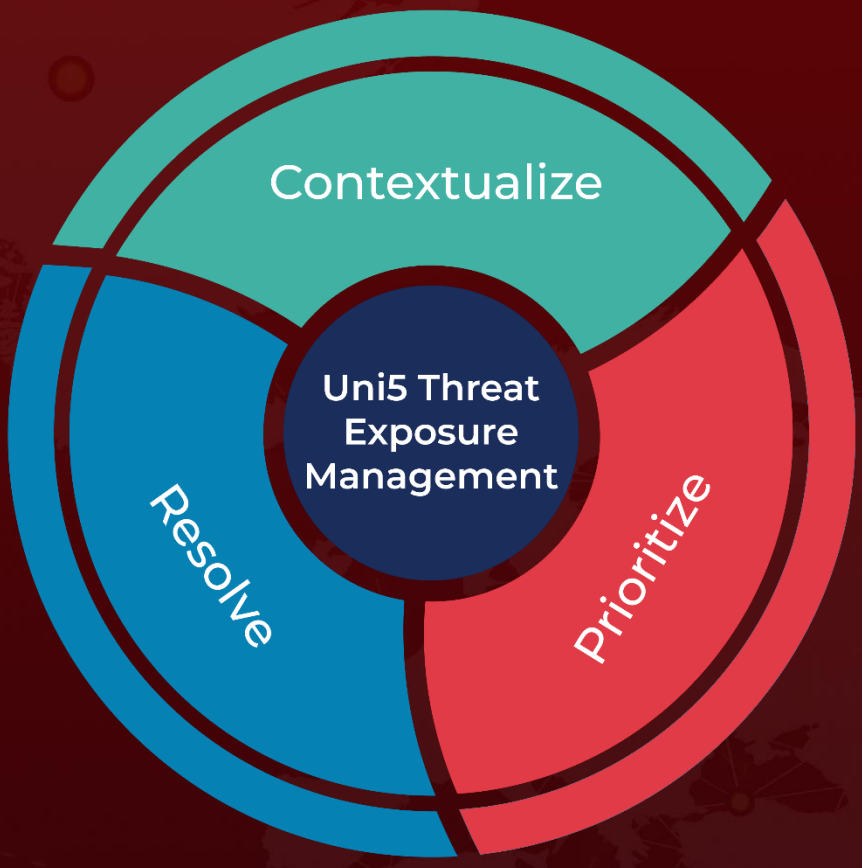
https://www.hivepro.com/threat-advisory/attackers-target-telecommunications-sector-to-gain-network-access/

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

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