HC3: Threat Actor Profile

October 24, 2024 TLP:CLEAR Report: 202410241500

Scattered Spider

Executive Summary

Scattered Spider is a financially motivated threat actor active since at least 2022, which has targeted organizations in various industries, including healthcare. The group has leveraged both legitimate, publicly available tools and other malware in its intrusions, including multiple ransomware variants. The group has become known for its advanced social engineering techniques, including voice phishing and leveraging artificial intelligence (AI) to spoof victims' voices for obtaining initial access to targeted organizations. The group will likely continue to evolve its TTPs to evade detection.

Report

Scattered Spider (also known as Octo Tempest, Roasted 0ktapus, Storm-0875, Starfraud, UNC3944, Scatter Swine, and Muddled Libra) is a financially motivated cybercriminal group that engages in data extortion and several other criminal activities. Scattered Spider is a native English-speaking cybercriminal group that has been active since at least 2022. The group is thought to comprise of individuals based in the United States and the United Kingdom. They are believed to be primarily between the ages of 19 and 22, as of September 2023. The group initially targeted customer relationship management (CRM) and business-process outsourcing (BPO) firms, as well as telecommunications and technology companies. Beginning in 2023, Scattered Spider expanded its operations to compromise victims in the gaming, hospitality, retail, MSP, manufacturing, and financial sectors. More recently, the group has expanded its operations to cloud environments. During campaigns, Scattered Spider has leveraged targeted social-engineering techniques, attempted to bypass popular endpoint security tools, and has deployed ransomware for financial gain. The group added RansomHub and Qilin to its cyber arsenal in Q2 2024.

Scattered Spider threat actors are considered experts in social engineering. Previously, on April 3, 2024, HC3 published a Sector Alert titled "Social Engineering Attacks Targeting IT Help Desks in the Health Sector", which detailed activity by threat actors employing advanced social engineering tactics to target IT help desks in the health sector. The threat actors gained initial access to targeted organizations by leveraging spear phishing voice (T1566.004) techniques, with the ultimate goal of leveraging the unauthorized access to modify ACH information for payer accounts to divert legitimate payments to attacker-controlled bank accounts. While this threat activity was not attributed to a specific threat actor, the tactics, techniques, and procedures (TTPs) observed overlap with Scattered Spider. On November 16, 2023, CISA released a joint Cybersecurity Advisory (CSA) on Scattered Spider (Alert Code: AA23-320A) in response to activity by Scattered Spider threat actors against the commercial facilities sectors and subsectors. This report provides updated technical details with IOCs and TTPs.

Scattered Spider has leveraged various malware and tools in its campaigns, including both publicly available and legitimate tools. For example, the group has leveraged various remote monitoring and management (RMM) tools, used multiple information stealers, and deployed ALPHV/BlackCat ransomware to victim environments for financial gain. Additionally, information stealers (infostealers) in general have previously been considered a precursor to ransomware attacks, according to SpyCloud, as they have enabled threat actors to obtain credentials for initial access. According to the researchers, infostealer infections preceded nearly one-third (30%) of ransomware events for North American and European ransomware victim companies in 2023. Scattered Spider threat actors have historically evaded detection on target networks by using living off the land (LOTL) techniques and allowlisted applications to navigate victim networks, as well as frequently modifying their TTPs.

HC3: Threat Actor Profile

October 24, 2024 TLP:CLEAR Report: 202410241500

Scattered Spider's attacks typically begin with SMS phishing, phone calls to victim help desks, and SIM swapping. After compromising credentials via social engineering, the threat actors have impersonated employees in calls to victim organizations' service desks, attempting to secure multifactor authentication (MFA) codes or password resets. During these calls, they provided the verification information requested by help desk employees, including usernames, employee IDs, and other types of personally identifiable information (PII) associated with the employees. The threat actors then utilize legitimate software such as AnyDesk and ScreenConnect to maintain persistence. They later employ malicious tools like Mimikatz and secretdump to escalate privileges. Following this, they move laterally through the network using RDP, SSH, and other services. In the final stages, they disable security and recovery services, exfiltrate data, and conduct ransomware operations. **Table 1** and **Table 2** provide updated information from a previous CISA advisory on the group based on open-source reports. **Table 1** details a list of legitimate tools Scattered Spider has repurposed and used for their criminal activity. Additional tools and software used by the group can be found here.

Table 1: Legitimate Tools Used by Scattered Spider

Tool	Use
AnyDesk	Enables remote monitoring and management of systems.
ASG Remote Desktop	Enables remote monitoring and management of systems.
ConnectWise Control	Enables remote monitoring and management of systems.
Fleetdeck.io	Enables remote monitoring and management of systems.
GitGuardian	A code security platform that helps developers, security teams, and cloud operations secure software development.
Impacket [S0357]	Scattered Spider has used Impacket for lateral movement.
ITarian	Enables remote monitoring and management of systems.
LaZagne [S0349]	Scattered Spider can obtain credential information using LaZagne.
Level.io	Enables remote monitoring and management of systems.
ManageEngine	Enables remote monitoring and management of systems.
Microburst	An open-source tool used to identify Azure credentials and secrets.
Mimikatz [S0002]	Extracts credentials from a system. Scattered Spider has gathered credentials using Mimikatz.
LogMeIn	Enables remote monitoring and management of systems.
Ngrok [S0508]	Enables remote access to a local web server by tunneling over the internet. Scattered Spider has used ngrok to create secure tunnels to remote web servers.
Pulseway	Enables remote monitoring and management of systems.
RustDesk	Enables remote monitoring and management of systems.
Screenconnect	Enables remote connections to network devices for management.
Splashtop	Enables remote connections to network devices for management.
Tactical.RMM	Enables remote monitoring and management of systems.
Tailscale	Provides virtual private networks (VPNs) to secure network communications.
Teamviewer	Enables remote connections to network devices for management.
Trufflehog	A free open-source application security tool that helps developers find and verify secrets in their code repositories.
Zoho Assist	Enables remote monitoring and management of systems.

In addition to using legitimate tools, Scattered Spider also uses malware as part of its TTPs. See **Table 2** for some of the malware used by Scattered Spider.

Table 2: Malware Used by Scattered Spider

Malware	Use
ATOMIC	A data miner used to obtain credentials.
AveMaria (aka WarZone [S0670])	Enables remote access to a victim's systems. Scattered Spider has utilized WarzoneRAT to remotely access a compromised system.
BlackCat [S1068]	Scattered Spider has deployed BlackCat ransomware to victim environments for financial gain.
EIGHTBAIT	A phishing kit designed to send captured credentials to an actor-controlled Telegram channel. Additionally, EIGHTBAIT can deploy AnyDesk to a victim's system.
Oktapus	The Oktapus phishing kit is a set of tools that attackers use to create fake websites and emails to trick users into giving away sensitive information.
Raccoon Stealer	Steals information including login credentials [TA0006], browser history [T1217], cookies [T1539], and other data.
RansomHub ransomware	Scattered Spider has deployed RansomHub ransomware to victim environments for financial gain.
POORTRY (aka BurntCigar)	A malicious signed driver designed to terminate processes associated with security software and to delete files as part of a Bring Your Own Vulnerable Driver (BYOVD) attack.
STONESTOP	A loader used to install a malicious signed driver dubbed POORTRY.
ULTRAKNOT (aka Meduza stealer)	Steals information including login credentials [TA0006], browser history [T1217], cookies [T1539], and other data.
VIDAR Stealer	Steals information including login credentials [TA0006], browser history [T1217], cookies [T1539], and other data.
Qilin (aka Agenda)	Scattered Spider threat actors have collaborated with Qilin ransomware affiliates.

Recent Campaigns

The following historical campaigns have been associated with Scattered Spider threat actors:

- **July 2024:** In July 2024, Fireblocks published research regarding an Oktapus campaign against Fireblocks that began with a series of well-crafted phishing SMS messages from U.S.-based phone numbers, mimicking legitimate communications from Fireblocks. The messages urged recipients to visit a link in order to attend a meeting with HR, redirecting them to a counterfeit Okta login page. The attackers used domain spoofing and lookalike URLs to enhance the authenticity of their phishing campaigns, a tactic that has proven effective in past instances.
- **June 2024:** Mandiant, part of Google Cloud, published a blog regarding UNC3944 targeting SaaS applications for data theft to attacker-owned cloud storage objects (using cloud synchronization tools), persistence mechanisms against virtualization platforms, and lateral movement via SaaS permissions abuse.
- **June 2024:** In early 2024, GuidePoint's Digital Forensics and Incident Response (DFIR) team responded to an attempted ransomware event seeking to impact an organization's ESXi environment, an event later attributed to an affiliate of the RansomHub ransomware-as-a-service (RaaS) group. Subsequent threat hunting has led them to assess with high confidence that the

same actor had previously performed successful ransomware attacks under the banner of the now-defunct ALPHV ransomware group, also known as BlackCat or Noberus. Based on the observed threat actor Tactics, Techniques, and Procedures (TTPs), including those presented herein, they assessed with high confidence that the actor was either a present or former member of the Scattered Spider affiliate group, based on observed overlaps with known Scattered Spider tools, TTPs, and infrastructure. Discussion and concurrence from industry peers and law enforcement supported their assessment.

- **April–June 2024:** In the second quarter of 2024, Scattered Spider added both RansomHub and Qilin to its ransomware payloads in campaigns, according to Microsoft.
- **April 2024**: In April 2024, Unit 42 researchers published a report on the Muddled Libra group targeting software-as-a-service (SaaS) applications and cloud service provider (CSP) environments. The threat actors began by performing reconnaissance to identify administrative users to target for their initial access when social engineering the help desk. The attacker then modified permissions to increase their scope of access. By modifying permission sets of compromised users, this escalated their privileges to gain further access to SaaS applications and organization's CSP environments. Muddled Libra also added additional identity providers with impersonation privileges, which allowed them to access additional applications while impersonating other user accounts. The threat actor also targeted SharePoint to gain a better understanding of the network configuration within a target company and which tools they could exploit, such as remote access tools. Within the Microsoft 365 suite, the group targeted email boxes and other email functionality to gain access to sensitive data. The report includes details of AWS and Azure data exfiltration techniques.
- **March 2024**: In March 2024, Unit 42 published a report on the Muddled Libra group using social engineering as their primary modus operandi, targeting a company's IT help support desk from mid-2022 through the beginning of 2024. Initial attacks were highly structured and favored large business process outsourcing firms serving high-value cryptocurrency holders. Unit 42 believes that when the threat actors exhausted those targets, they evolved into a ransomware affiliate model with extortion as their key objective. The report noted that Muddled Libra had also been observed using AI to spoof victims' voices by leveraging social media videos to train AI models.
- **September 2023:** Two of the largest casino and gambling companies in the United States were impacted by an ALPHV/BlackCat ransomware attack in September 2023, after Scattered Spider threat actors gained initial access by calling in to the target organization's IT help desk and impersonating an employee by leveraging information obtained from LinkedIn.
- **January 2023**: On January 23, 2023, the Hawaii Department of Health (DOH) was notified by Mandiant that an unauthorized individual used an account belonging to a former medical certifier at a local Hawaii hospital to access the Electronic Death Registry System (EDRS) at the edr[.]ehawaii[.]gov website after the login credentials were placed for sale on the dark web. According to open-source reports, the intrusion was carried out by Kentucky resident Jesse Kipf, who went by various monikers, including FreeRadical and GhostMarket09. The individual was considered an initial access broker (IAB) linked to the threat actor Scattered Spider.
- **June–December 2022**: Tracked by MITRE as C0027, a financially motivated campaign linked to Scattered Spider targeted telecommunications and business process outsourcing (BPO) companies from at least June through December of 2022. During C0027, Scattered Spider used various forms of social engineering, performed SIM swapping, and attempted to leverage access from victim environments to mobile carrier networks.

HC3: Threat Actor Profile

October 24, 2024 TLP:CLEAR Report: 202410241500

Aliases or Threat Actor Names

- Scattered Spider (CrowdStrike)
- Octo Tempest (Microsoft)
- Roasted 0ktapus (Group-IB)
- Storm-0875 (Microsoft)
- Starfraud
- UNC3944 (Mandiant)
- Scatter Swine (Okta)
- Muddled Libra (Palo Alto Networks Unit 42)
- Dev0671 (Microsoft)
- Dev0875 (Microsoft)
- Dev0971 (Microsoft)
- White Dev 146
- LUCR-3 (Permiso Security)

Exploited Vulnerabilities

- CVE-2015-2291: Intel Ethernet Diagnostics Driver for Windows Denial-of-Service Vulnerability
- CVE-2021-35464: ForgeRock Access Management (AM) Core Server Remote Code Execution Vulnerability
- CVE-2022-21882: Microsoft Win32k Privilege Escalation Vulnerability
- CVE-2022-41328: Fortinet FortiOS Path Traversal Vulnerability

Associated Individuals (Arrested Members)

- Noah Michael Urban (aka Sosa, Elijah, King Bob, and Antony Ramirez) of Florida, U.S. (19 years old)
- Tyler Buchanan (aka tylerb) of Dundee, Scotland, United Kingdom (22 years old)
- Jesse Kipf (aka FreeRadical, GhostMarket09, Theelephantshow, Yelichanter, and ayohulk) of Kentucky, U.S. (39 years old)
- Male suspect from Walsall, United Kingdom (17 years old)

Affiliated Threat Actors or Groups

- The Community (The Com)
- ALPHV/BlackCat ransomware-as-a-service (RaaS) operator(s)
- RansomHub ransomware-as-a-service (RaaS) operator(s)
- Qilin ransomware-as-a-service (RaaS) operator(s)

Threat Actor Communications

- Telegram
- Discord
- TOR
- Tox
- Email
- Encrypted applications
- Hacker forums

HC3: Threat Actor Profile

October 24, 2024 TLP:CLEAR Report: 202410241500

Indicators of Compromise

A sample of indicators of compromise (IOCs) associated with Scattered Spider and malware used by the group from multiple sources can be found below:

- IOCs associated with Scattered Spider from Sekoia can be found here on GitHub.
- IOCs associated with Scattered Spider from EclecticIQ can be found here.
- IOCs associated with Scattered Spider from OccamSec can be found here.
- IOCs associated with Qilin ransomware from HC3 can be found here and here from DarkTrace.
- IOCs associated with RansomHub ransomware can be found here.

Mitigations

The FBI and CISA recommended the below mitigations in September 2023 to defend against Scattered Spider:

- Implementing application controls.
- Implementing FIDO/WebAuth authentication or Public Key Infrastructure (PKI)-based MFA.
- Strictly limiting the use of Remote Desktop Protocol (RDP) and other remote desktop services.

Additional mitigations can be found below:

- Mitigations for Scattered Spider and BlackCat Ransomware from FS-ISAC can be found here.
- Mitigations for Qilin ransomware from HC3 can be found here.
- Mitigations for RansomHub ransomware from CISA can be found here and from TrendMicro here.
- Guidance for identifying and mitigating Living Off the Land Techniques can be found here.

Analyst Comment

While Scattered Spider is comprised of young individuals, they have successfully executed high-profile breaches largely due to their advanced social engineering capabilities. Despite this, the group appears to have poor operational security, as multiple key members have been arrested. Nonetheless, the group continues to conduct successful attacks while evolving its TTPs to evade detection in victim environments. HC3 assesses with moderate confidence that the group will likely continue to target various industries, including healthcare, for financial gain.

Relevant HC3 Products

- HC3 Sector Alert: Social Engineering Attacks Targeting IT Help Desks in the Health Sector (April 3, 2024) TLP:CLEAR. https://www.hhs.gov/sites/default/files/help-desk-social-engineering-sector-alert-tlpclear.pdf
- HC3 Threat BRief: Social Engineering Attacks Targeting the HPH Sector (April 11, 2024) TLP:CLEAR. https://www.hhs.gov/sites/default/files/social-engineering-targeting-the-hph-sector-tlpclear.pdf
- HC3 Threat Profile: Qilin, aka Agenda Ransomware (June 18, 2024) TLP:CLEAR. https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf
- HC3 Analyst Note: Vishing Attacks on the Rise (August 19, 2022) TLP:CLEAR. https://www.hhs.gov/sites/default/files/vishing-attacks-on-the-hph-sector-analyst-note.pdf
- HC3 Sector Alert: Possible Threat of Unauthorized Access to HPH Organizations from Remote Access Tool (January 22, 2024) TLP:CLEAR. https://www.hhs.gov/sites/default/files/threat-unauthorized-access-hph-orgs-sector-alert.pdf
- HC3 Threat Brief: Artificial Inteligence, Cybersecurity and the Health Sector (July 13, 2023).

https://www.hhs.gov/sites/default/files/ai-cybersecurity-health-sector-tlpclear.pdf

References

Ahl, Ian. "LUCR-3: Scattered Spider Getting SaaS-y in the Cloud." Permiso Security. September 20, 2023. https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud

Baker, Jason. "Worldwide Web: An Analysis of Tactics and Techniques Attributed to Scattered Spider" GuidePoint Security. June 12, 2024. https://www.guidepointsecurity.com/blog/worldwide-web-an-analysis-of-tactics-and-techniques-attributed-to-scattered-spider/

Barishev, Yossi. "Understanding an 0ktapus Phishing Campaign." Fireblocks. July 8, 2024. https://www.fireblocks.com/blog/understanding-an-0ktapus-phishing-campaign/

Black Arrow Cyber Consulting Limited. "Black Arrow Cyber Threat Briefing 03 May 2024." May 3, 2024. https://www.blackarrowcyber.com/blog/threat-briefing-03-may-2024

Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security of Germany). "Active crime groups in Germany." August 8, 2024. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive-Crime-Gruppen/aktive-crime-gruppen_node.html

Büyükkaya, Arda. "Ransomware in the Cloud: Scattered Spider Targeting Insurance and Financial Industries." EclecticIQ. September 10, 2024. Updated October 2, 2024. https://blog.eclecticiq.com/ransomware-in-the-cloud-scattered-spider-targeting-insurance-and-financial-industries

CISA. "Cybersecurity Advisory: Scattered Spider (Alert Code: AA23-320A)." November 16, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

CrowdStrike. "Adversaries: Scattered Spider." Accessed October 8, 2024. https://www.crowdstrike.com/adversaries/scattered-spider/

CrowdStrike Intelligence Team. "SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security." January 10, 2023. https://www.crowdstrike.com/en-us/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/

CrowdStrike. "Cybersecurity 101: What Are Living off the Land (LOTL) Attacks?" February 22, 2023. https://www.crowdstrike.com/cybersecurity-101/living-off-the-land-attacks-lotl/

Curtis, Abby. "What is Scattered Spider?" Splunk. https://www.splunk.com/en_us/blog/learn/scattered-spider.html

Cyble. "Threat Actor Profile: Scattered Spider." https://cyble.com/threat-actor-profiles/scattered-spider/

DarkNet Diaries. "Ep 112: Dirty Coms." March 8, 2022. https://darknetdiaries.com/episode/112/

DarkOwl. "Scattered Spider: Update on Arrests." June 27, 2024. https://www.darkowl.com/blog-content/scattered-spider-update-on-arrests/

DarkOwl. "StarFraud Chat – Telegram Channel Analysis using A.I." June 19, 2024. https://www.darkowl.com/blog-content/starfraud-chat-telegram-channel-analysis-using-a-i/

DarkOwl. "Threat Actor Spotlight: SCATTERED SPIDER." March 19, 2024. https://www.darkowl.com/blog-content/threat-actor-spotlight-scattered-spider/

DefendEdge. "The Community That Spawned Notorious Threat Actors." April 29, 2024. https://www.defendedge.com/the-community-that-spawned-notorious-threat-actors/

Foresiet. "Meduza Stealer: Detailed Analysis of its Features, Capabilities, and Recent Updates on Active C2." August 30, 2024. https://foresiet.com/blog/meduza-stealer-detailed-analysis-of-its-features-capabilities-and-recent-updates-on-active-c2

Franceschi-Bicchierai, Lorenzo. "How the FBI and Mandiant caught a 'serial hacker' who tried to fake his own death." TechCrunch. October 1, 2024. https://techcrunch.com/2024/10/01/how-the-fbi-and-mandiant-caught-a-serial-hacker-who-tried-to-fake-his-own-death/

FS-ISAC. "Scattered Spider & BlackCat Ransomware: Mitigation Guidance." November 2023. https://www.fsisac.com/hubfs/Knowledge/ScatteredSpider&BlackCatRansomware-MitigationGuidance.pdf

Gatlan, Sergiu. "Microsoft links Scattered Spider hackers to Qilin ransomware attacks." BleepingComputer. July 16, 2024. https://www.bleepingcomputer.com/news/security/microsoft-links-scattered-spider-hackers-to-qilin-ransomware-attacks/

Hawaii Department of Health. "Department of Health to send notifications regarding unauthorized access to Electronic Death Registry System." March 9, 2023. https://health.hawaii.gov/news/newsroom/department-of-health-to-send-notifications-regarding-unauthorized-access-to-electronic-death-registry-system/

Kelley, Margaret. "Muddled Libra's Evolution to the Cloud." Palo Alto Networks Unit 42. April 9, 2024. https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/

Klopsch, Andreas. "Attack tool update impairs Windows computers." Sophos. August 27, 2024. https://news.sophos.com/en-us/2024/08/27/burnt-cigar-2/

Krebs, Brian. "Alleged Boss of 'Scattered Spider' Hacking Group Arrested." KrebsonSecurity. June 15, 2024. https://krebsonsecurity.com/2024/06/alleged-boss-of-scattered-spider-hacking-group-arrested/

Krebs, Brian. "Fla. Man Charged in SIM-Swapping Spree is Key Suspect in Hacker Groups Oktapus, Scattered Spider." KrebsonSecurity. January 30, 2024. https://krebsonsecurity.com/2024/01/fla-man-charged-in-sim-swapping-spree-is-key-suspect-in-hacker-groups-oktapus-scattered-spider/

Mandiant. "UNC3944 Targets SaaS Applications." June 13, 2024. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications

Mandiant. "Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety." September 14, 2023. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware/

Microsoft. "How Microsoft names threat actors." August 21, 2024. https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming?view=o365-worldwide

Microsoft. "Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction." October 25, 2023. https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

Microsoft Threat Intelligence @MsftSecIntel. July 15, 2024. https://x.com/MsftSecIntel/status/1812932749314978191

Mirkasymov, Rustam. "Roasting 0ktapus: The phishing campaign going after Okta identity credentials." Group-IB. August 25, 2022. https://www.group-ib.com/blog/0ktapus/

MITRE. "Groups: Scattered Spider." Last Modified April 4, 2024. Created July 5, 2023. https://attack.mitre.org/groups/G1015/

Morrison, Sara. "The chaotic and cinematic MGM casino hack, explained." Vox. October 6, 2023. https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware

NIST. "CVE-2015-2291 Detail." Last Modified August 24, 2017. https://nvd.nist.gov/vuln/detail/CVE-2015-2291

Okta Defensive Cyber Operations. "Detecting Scatter Swine: Insights into a Relentless Phishing Campaign." August 25, 2022. https://sec.okta.com/scatterswine

Palo Alto Networks Unit 42. "Muddled Libra's Evolution to the Cloud." April 9, 2024. https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/

Palo Alto Networks Unit 42. "Threat Group Assessment: Muddled Libra (Updated)." March 8, 2024. https://unit42.paloaltonetworks.com/muddled-libra/

Parisi, Tim. "Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies." CrowdStrike. December 2, 2022. https://www.crowdstrike.com/en-us/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

Pierre-Antoine D., Quentin Bourgue, Livia Tibirna and Sekoia TDR. "Scattered Spider laying new eggs." Sekoia. February 22, 2024. https://blog.sekoia.io/scattered-spider-laying-new-eggs/

Quorum Cyber. “Scattered Spider Threat Actor Profile.” https://www.quorumcyber.com/threat-actors/scattered-spider-threat-actor-profile/

SOCRadar. “Dark Web Profile: Scattered Spider.” January 18, 2024. Updated July 17, 2024. https://socradar.io/dark-web-profile-scattered-spider/

SpyCloud. “SpyCloud Report: Infostealer Malware is a Precursor to Ransomware Attacks.” September 20, 2023. https://spycloud.com/newsroom/spycloud-report-infostealer-malware-precursor-to-ransomware-attacks/

The Record from Recorded Future. “CLICK HERE: Throwing Bricks for $$$: Violence-as-a-Service Comes of Age.” September 20, 2022. https://www.youtube.com/watch?v=vetDHP0VKHE

Thomas, Will. “Defending Against SCATTERED SPIDER and The Com with Cybercrime Intelligence.” SANS Institute. July 15, 2024. https://www.sans.org/blog/defending-against-scattered-spider-and-the-com-with-cybercrime-intelligence/

Trellix. “Scattered Spider: The Modus Operandi.” August 17, 2023. https://www.trellix.com/blogs/research/scattered-spider-the-modus-operandi/

Uptucs Threat Research. “Meduza Stealer Malware: What is it & How Does it Work?” June 30, 2023. https://www.uptycs.com/blog/threat-research-report-team/what-is-meduza-stealer-and-how-does-it-work

U.S. Attorney's Office, Eastern District of Kentucky. “Pulaski County Man Sentenced for Cyber Intrusion and Aggravated Identity Theft.” August 20, 2024. https://www.justice.gov/usao-edky/pr/pulaski-county-man-sentenced-cyber-intrusion-and-aggravated-identity-theft

U.S. Attorney's Office, Middle District of Florida, “Palm Coast Man Arrested For Wire Fraud And Aggravated Identity Theft Charges.” January 11, 2024. https://www.justice.gov/usao-mdfl/pr/palm-coast-man-arrested-wire-fraud-and-aggravated-identity-theft-charges

Vectra AI. “Understanding Scattered Spider, and how they perform cloud-centric identity attacks.” SC Media. May 2, 2024. https://www.scworld.com/native/understanding-scattered-spider-and-how-they-perform-cloud-centric-identity-attacks

Vicens, AJ. “Potent youth cybercrime ring made up of 1,000 people, FBI official says.” May 24, 2024. CyberScoop. https://cyberscoop.com/potent-youth-cybercrime-ring-made-up-of-1000-people-fbi-official-says/

West Midlands Police. “Walsall teenager arrested in joint West Midlands Police and FBI operation.” July 19, 2024. https://www.westmidlands.police.uk/news/west-midlands/news/news/2024/july/walsall-teenager-arrested-in-joint-west-midlands-police-and-fbi-operation/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

HC3: Threat Actor Profile

October 24, 2024 TLP:CLEAR Report: 202410241500

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback