1.1.1 *Scattered Spider*

Threat Actor Group	
Name	Scattered Spider, UNC3944, oktapus, Muddled Libra, Scatter Swine, Storm-0875, Octo Tempest, LUCR-3, Star Fraud
Class	Human–operated Ransomware
Active since	2022
Source geography	Unknown
Primary language	English
Associated actors	BlackCat (ALPHV) Gang
Summary	Scattered Spider is a ransomware group known for its use of social engineering, phishing, and exploitation of vulnerabilities to infiltrate target companies. The threat actor group is financially motivated and has been active since May 2022. This group has been linked to several high-profile attacks, including those on MGM Resorts and Caesars Entertainment. Scattered Spider is an affiliate of the BlackCat/ALPHV ransomware gang and has been observed to use their malwares in operation. The threat actor group is suspected to be comprised of teenagers and young adults, and is one of many illicit hacking groups within "the Community", a collection of English-speaking online criminals.[1] The threat actor first identifies administrative users and gather information about the SaaS (software as a service) and cloud service providers (CSPs) used by their targets. Then, they often use lookalike domains for smishing attacks. These domains are short-lived, used only during the initial access phase, and quickly taken down to evade investigation. [2] Their modus operandi involves luring users into providing their login credentials, one-time password (OTP) codes, or two-factor authorization (2FA) codes through phishing and social engineering. The threat actor would then pose as legitimate employees to bypass security measures, effectively circumventing multifactor authentication (MFA). Once inside the network, the threat actor group deploys ransomware, encrypt critical systems, and demand hefty ransoms.[3] The group uses commercial residential proxy services to mask their locations and employs a variety of legitimate remote access tools to maintain backdoor access into the environment.[4] Once they gain a foothold, Scattered Spider spends significant time searching internal documentation, resources, and chat logs to facilitate privilege escalation and maintain their presence. The group favors remote desktop protocol (RDP) connections for lateral movement and often create unmanaged virtual machines within victims' environments for launching further attacks. Their tactics include direct communications with victims, deploying ransomware on business-critical systems, and making enormous extortion demands. In January, June, and July 2024 respectively, an alleged ringleader and two members of Scattered Spider were arrested by the US and UK authorities.[5] Their last known operation was in January 2024.

[1] https://www.cbsnews.com/news/cybersecurity-investigators-worry-ransomware-attacks-may-worsen-as-young-hackers-in-us-work-with-russians-60-minutes-transcript/

[2] https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/

[3] https://therecord.media/scattered-spider-ransomware-attacks-hospitality-retail

[4] https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware/

[5] https://krebsonsecurity.com/2024/06/alleged-boss-of-scattered-spider-hacking-group-arrested/

	Overall, Scattered Spider poses a low to medium threat to CLIENTHK as they are known to mostly target United States organisations but have demonstrated interest in critical infrastructures in the APAC region.

Goal orientation	
Motivation	Given the nature of some of the targets, particularly in terms of organisations the threat actor has targeted in the past, as well as the modus operandi used, we assess with high confidence that Scattered Spider is financially motivated.
Intended effect	The primary intended effect is to conduct data theft and operational disruptions to incite targets to transfer the ransom payment and in exchange they will decrypt and not leak the data.

Intent	
Target geography	Scattered Spider is observed to target various geographies, but around 84% of the known victims are companies located in USA[6]. Based on Scattered Spider's known victim list, we assess Scattered Spider to have a **LOW** intent to target Hong Kong.
Target sector	Given that the group is opportunistic, Scattered Spider is known to target all sectors. The group has been previously observed to target the financial sector and other critical infrastructures, we assess Scattered Spider to have a **HIGH** intent to target the Hong Kong financial sector.
Target areas	Scattered Spider is known to target and exfiltrate data from SaaS (software as a service)/CSP (cloud service provider) environments, such as Windows, Linux, Google Workspace, AzureAD, M365 and AWS environments[7]. Based on this, we assess Scattered Spider to have a **HIGH** intent to target CLIENTHK.
Intent score	Based on the above observations, we assess Scattered Spider to have a **MEDIUM** intent to target CLIENTHK.

Capability	
Resources	Considering that Scattered Spider's targets are most often large companies, they are expected to have a large budget from their ransom revenue. As an ex-affiliate of ALPHV/BlackCat, the threat actor is known to leverage ALPHV/BlackCat's ransomware. Based on the modus operandi of this threat actor and the scale of operation in comparison with other threat actors we have observed, we assess it is likely to have a **MEDIUM** level of resources.
Skills	Scattered Spider started as a SIM swapping group, but they have since upgraded their operations. Since 2023, they have been observed to leverage malwares, exploit vulnerabilities, and exfiltrate VPN and MFA enrollment data. Nevertheless, the threat actor's use of open-source tools and scripts are not highly innovative within the cyberattack space. Most notably, Scattered Spider is skilled in their social engineering skills. Unlike LockBit, BlackCat, and other ransomware groups, the group is comprised of English-speakers, so the threat actor group has been known to be skillful in conducting social engineering operations against employees in the United States, their most targeted geography. Based on this, we assess the threat actor group to have a **MEDIUM** level skillset.
Resolve	Given the extensive reconnaissance conducted to tailor their intrusion and subsequent activities, the group are assessed to be proactive in their approach to maximise their likelihood of success, evade detection and maintain persistent

[6] https://www.group-ib.com/blog/0ktapus/

[7] https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

	access. However, it is known that the threat actor group immediately changes their target when their operations are disrupted before the extortion phase.[8] Based on this, we assess a **MEDIUM** degree of resolve against disruption and detection efforts.
Access to target	The threat actor group have a **HIGH** level of ability to access targeted critical systems such as business-critical virtual machines, and other critical systems through the deployment of tools to conduct remote desktop protocols (RDP). The threat actors operate with a rapid speed, accessing critical systems and exfiltrating significant amounts of data within a few days.
Risk sensitivity	Taking into consideration the criminal nature of this activity, we assess this threat actor is likely to have a **LOW** risk appetite and operations are predominantly carried out over the internet.
Capability score	Given the above observations and our understanding of the capability of other threat actors in this category, we assess that this threat actor has a **MEDIUM** level capability.

Modus Operandi	
Reconnaissance	Scattered Spider first collects information on open-source intelligence such as LinkedIn and previously compromised data to identify administrative users of the organization and uncover information on the SaaS and CSP that the organization uses.[9] The threat actor is also known to sometimes purchase employees' credentials and/or session tokens in criminal underground markets.[10]
Preparation	The threat actor prepares their infiltration by generating phishing sites with lookalike domains. These malicious domain names commonly uses the format of [organization name]-[service].com, where services include SSO, helpdesk and HR. Scattered Spider has been observed to register their domains via Porkbun, Namecheap, Metaregistrar, and Hosting Concepts, and host the domains on Digital Ocean infrastructure and a large content delivery network (CDN) service. These domains are short-lived for the purpose of the initial access phase, so they are very quickly taken down before defenders can investigate.[11] ***Develop malicious code:*** • POORTRY[12] – malware that can be used to terminate a security software running on a Windows device • STONESTOP[13]– Windows userland utility that acts as a loader and installer for POORTRY and also instructs POORTRY on what actions to perform. ***Tools commonly deployed:*** • ADRecon[14] – obtain victim domain account credentials

[8] https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

[9] https://www.cbsnews.com/news/cybersecurity-investigators-worry-ransomware-attacks-may-worsen-as-young-hackers-in-us-work-with-russians-60-minutes-transcript/

[10] https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

[11] https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/

[12] https://www.bleepingcomputer.com/news/security/malicious-windows-kernel-drivers-used-in-blackcat-ransomware-attacks/

[13] https://www.sentinelone.com/labs/driving-through-defenses-targeted-attacks-leverage-signed-malicious-microsoft-drivers/

[14] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=ADRecon

	• AnyDesk[15] – legitimate system for remote control, file transfer, and VPN functionality that can be used as a backdoor tool • DCSync[16] – malware that mimics the behaviour of Domain Controller (DC) to act as a credential stealer • FiveTran[17] – legitimate system for transfering data that can be used as a information stealer • FleetDeck[18] – legitimate system for managing computers remotely that can be used as a backdoor tool • gosecretsdump[19] – open-source module that can be used as a credential stealer • Govmomi[20] – library that interacts with VMware vSphere APIs (ESXi and/or vCenter Server) and can be used to obtain victim account credentials • Hekatomb[21] – python script that connects to Lightweight Directory Access Protocol (LDAP) directory that can be used to steal credentials • Impacket[22] – open-source collection of modules for constructing and manipulating network protocols that can be used as a credential and information stealer • LaZagne[23] – post-exploitation, open-source tool that can be used to steal stored passwords on a system • LummaC2[24] – subscription-based information stealer focused on cryptocurrency wallets and sensitive information such as login credentials • Mimikatz[25] – credential stealer, keylogger tool for Windows • ngrok[26] – legitimate reverse proxy tool that reveals local servers behind Network Address Translations (NATs) and firewalls to the public internet; can be used as a backdoor and tunneling tool • PingCastle[27] – obtain victim domain account credentials • ProcDump[28] – free Microsoft tool that can be used as a credential stealer • PsExec[29] – free Microsoft tool that can be used for remote code execution • Pulseway[30] – remote monitoring and management (RMM) software that can be used as a backdoor tool • Pure Storage FlashArray[31] – legitimate Windows PowerShell SDK that can be used to obtain victim account credentials

[15] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=AnyDesk

[16] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=DCSync

[17] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=FiveTran

[18] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=FleetDeck

[19] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=gosecretsdump

[20] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Govmomi

[21] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Hekatomb

[22] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Impacket

[23] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=LaZagne

[24] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=LummaC2

[25] https://apt.etda.or.th/cgi–bin/listgroups.cgi?t=Mimikatz&n=1

[26] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Ngrok

[27] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=PingCastle

[28] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=ProcDump

[29] https://apt.etda.or.th/cgi–bin/listgroups.cgi?t=PsExec&n=1

[30] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Pulseway

[31] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Pure%20Storage%20FlashArray

	• RedLine[32] – malware that collects credentials stored in browsers, email applications, and cryptocurrency wallet data[33] • Rsocx[34] – Socks5 proxy server that can be used as a tunneling tool • RustDesk[35] – open-source remote control for self-hosting that can be used as a backdoor tool • ScreenConnect[36] – legitimate remote administration tool that can be used to connect to and conduct lateral movement in target environments[37] • SharpHound[38] – malware used to identify different attack paths and obtain victim credentials and informations • Socat[39] – command line based utility that can be used as a tunneling tool on Linux • Spidey Bot[40] – credential and information stealer that collects stored passwords and other data from VPN, internet browsers, email clients, gaming software, and cryptocurrency • Splashtop[41] – legitimate remote access and support software that can be used as a backdoor tool • Stealc[42] – malware that steals information from web browsers, browser extensions, cryptocurrency applications, and email messaging softwares • TacticalRMM[43] – RMM software that can be used as a backdoor tool • Tailscale[44] – legitimate software that connects devices and development environments, can be used as a backdoor tool • TightVNC[45] – legitimate, free, and open source remote desktop software for accessing and controlling computers over a network that can be used as a backdoor tool • VIDAR[46] – malware that steals information and credentials on 2FA Software and Tor Browser • WinRAR[47] – legitimate data compression tool for Windows • WsTunnel[48] – tunneling tool that bypass firewalls and proxies • Living off the Land[49] – collection of binaries, scripts, and libraries for attackers to share.
Infiltration	The group collects admin credentials to the company's SaaS and CSP by sending lure messages targeting employees' cellphones, urging them to update account

[32] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=RedLine

[33] https://cofense.com/blog/luxury-hotels-remain-target-of-social-engineering-attack/

[34] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Rsocx

[35] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=RustDesk

[36] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=ScreenConnect

[37] https://attack.mitre.org/software/S0591/

[38] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=SharpHound

[39] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Socat

[40] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Spidey%20Bot

[41] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Splashtop

[42] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Stealc

[43] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=TacticalRMM

[44] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Tailscale

[45] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=TightVNC

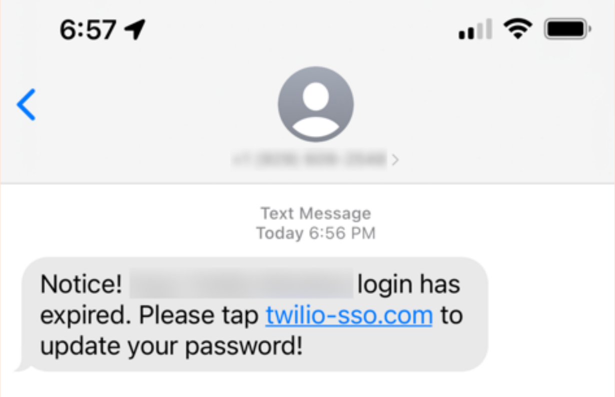
[46] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=VIDAR

[47] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=WinRAR

[48] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=WsTunnel

[49] https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Living%20off%20the%20Land

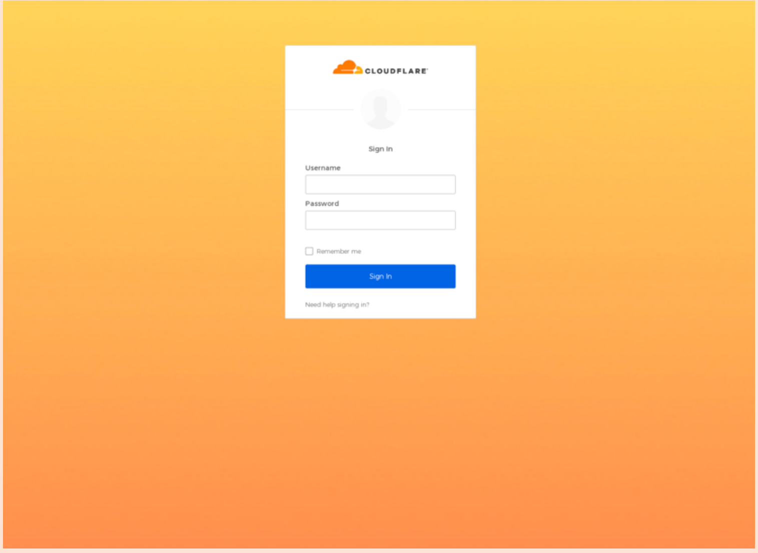
information or reauthenticate to corporate applications through links to spoofed corporate domains. The group uses numerous phishing sites that emulate familiar login pages designed to capture credentials and OTP/2FA codes before they expire. These credentials and OTP/2FA codes are then immediately sent to the threat actors via the messaging service Telegram.[50] Since OTP/2FA codes expire very quickly, the threat actor most likely continuously monitors Telegram and uses the credentials as soon as they received them.[51]



Text Message
Today 6:56 PM

Notice! [redacted] login has expired. Please tap twilio-sso.com to update your password!

Scattered Spider's messages towards Twilio employees. Note that the threat actor matches employee's names with their numbers and uses domains related to their company's name.[52]



Scattered Spider's phishing site for Cloudfare

Scattered Spider is known to use the acquired usernames, passwords, and personally identifiable information (PII) to conduct SIM swaps on compromised users.[53]

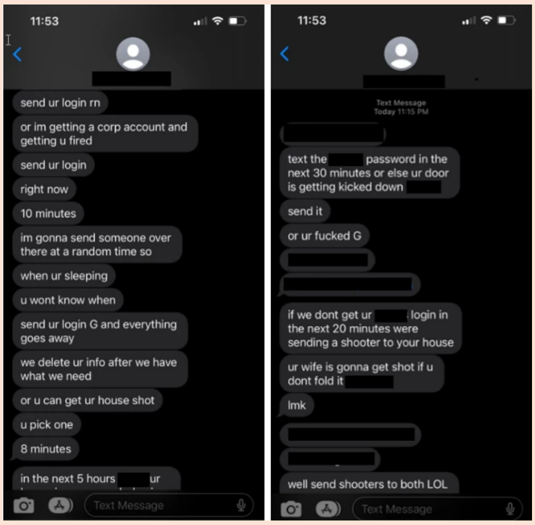
Scattered Spider uses the information they have on the adminstrative users and SaaS/CSP environments to manipulate help desk agents into resetting both passwords and MFA on the same call. Their attacks are persistent, aiming to wear

[50] https://blog.cloudflare.com/2022-07-sms-phishing-attacks/

[51] https://www.group-ib.com/blog/0ktapus/

[52] https://www.twilio.com/en-us/blog/august-2022-social-engineering-attack

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

	down the defenses of help desk agents over extended call durations.[54] The group is also known to call employees to socially engineer them to install a Remote Monitoring and Management (RMM) utility, navigate to the phishing sites, or remove their FIDO2 token.[55] Scattered Spider has once relied on using personal information, such as home addresses and family names, along with physical threats to force individual employees to share corporate credentials, as seen in the screenshots below.  11:53 [redacted] send ur login rn or im getting a corp account and getting u fired send ur login right now 10 minutes im gonna send someone over there at a random time so when ur sleeping u wont know when send ur login G and everything goes away we delete ur info after we have what we need or u can get ur house shot u pick one 8 minutes in the next 5 hours [redacted] ur Text Message 11:53 [redacted] Text Message Today 11:15 PM [redacted] text the [redacted] password in the next 30 minutes or else ur door is getting kicked down [redacted] send it or ur fucked G [redacted] [redacted] if we dont get ur [redacted] login in the next 20 minutes were sending a shooter to your house ur wife is gonna get shot if u dont fold it [redacted] lmk [redacted] [redacted] well send shooters to both LOL Text Message Screenshot of Scattered Spider contacting an employee.
Entrenchment	Once Scattered Spider obtains initial access, they often spend significant time searching through internal documentation, resources, and chat logs to find information that could help them escalate privileges and maintain presence within the victim environments.[56] The threat actor has been observed to add a federated identity provider to the victim's SSO system and activate automatic account linking. This allowed them to sign into any account with a matching SSO attribute. This privilege escalation technique maintains their access even when passwords changed. The threat actor group also exploited already installed endpoint detection and response (EDR) tools, leveraging their remote-shell and command execution capabilities to further elevate access. [57] Scattered Spider has been observed to exploit known vulnerabilities to elevate privileges. This suggests the group leverages publicly released Proof–of–Concepts (PoC) or acquires vulnerability exploits via dark web hacking forums. ***Vulnerability exploits:*** The vulnerabilities known to have been used by this threat actor include: • CVE–2015–2291[58] – Intel Ethernet diagnostics driver for Windows (iqvw64.sys) has a vulnerability that allows local users to cause a denial of service or possibly execute arbitrary code with kernel privileges.

[54] https://unit42.paloaltonetworks.com/muddled-libra/

[55] https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

[56] https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware/

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

[58] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2291

	• CVE–2021–35464[59] – ForgeRock AM server before version 7.0 has a vulnerability in its jato.pageSession parameter that allows remote code execution without authentication. The threat actor is known to use various tactics to evade security monitoring. They accessed victims from the same local area by leveraging commercial residential proxy services. The threat actors also consistently used legitimate software, including a variety of remote access tools downloaded directly from vendor websites. [60] Additionally, the threat actors often installed multiple remote monitoring and management (RMM) tools during their intrusions, such as AnyDesk, Splashtop, FleetDeck, RustDesk, and Tactical RMM, to ensure they maintained backdoor access even if one of their methods were discovered.[61] Also, lateral movement within the target environment was often facilitated through remote desktop protocol (RDP) connections from compromised computers to minimize external network artifacts in logs, which avoids alerting the defenders.[62] Additionally, Scattered Spider leverages POORTRY and STONESTOP, two malwares, to terminate a security software on Windows and avoid being detected by defenders. [63] To monitor if their activities have been detected, Scattered Spider is also known to search the victim's collaboration tools, such as Slack, Microsoft Teams, and Microsoft Exchange, for emails or conversations about the intrusion and any security response. They also join incident remediation and response calls, likely to understand how the security teams are hunting for them and develop new ways to maintain access in response to the victim's defenses. To support this, the threat actor sometimes create new identities within the environment and backstop them with fake social media profiles. [64]
Compromise	Scattered Spider most often created unmanaged virtual machines within the victims' own environments, from which they launched their attacks. In some cases, they even created internet-accessible virtual machines in the victim's cloud environment. When deploying ransomware, the threat actors is known to specifically target business-critical virtual machines and other systems, likely in an attempt to maximize the impact on the victim.[65]
Exploitation	The threat actor will encrypt data for impact and inhibit system recovery, blocking user access to the network, until ransom requests are met.
MITRE ATT&CK Techniques deployed	• Phishing: Spearphishing Link – T1566.002 • Phishing: Spearphishing Voice – T1566.004 • External Remote Services – T1133 • Exploit Public-Facing Application – T1190 • Command and Scripting Interpreter – T1059 • Exploitation for Privilege Escalation – T1068 • Access Token Manipulation: Token Impersonation/Theft – T1134.001 • Masquerading: Match Legitimate Name or Location – T1036.005 • Subvert Trust Controls: Code Signing – T1553.002 • Input Capture: GUI Input Capture – T1056.002

[59] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35464

[60] https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware/

[61] https://unit42.paloaltonetworks.com/muddled-libra/

[62] https://unit42.paloaltonetworks.com/muddled-libra/

[63] https://www.sentinelone.com/labs/driving-through-defenses-targeted-attacks-leverage-signed-malicious-microsoft-drivers/

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

[65] https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware/

	• Remote Services: Remote Desktop Protocol – T1021.001 • Remote Services: Cloud Services – T1021.007 • Exploitation of Remote Services – T1210 • Resource Hijacking – T1496 • Gather Victim Identity Information: Credentials – T1589.001 • Gather Victim Identity Information: Email Addresses – T1589.002 • Gather Victim Identity Information: Employee Names – T1589.003 • Phishing for Information: Spearphishing Service – T1598.001 • Phishing for Information: Spearphishing Voice – T1598.004 • Acquire Infrastructure: Domains – T1583.001 • Establish Accounts: Social Media Accounts – T1585.001 • Establish Accounts: Email Accounts – T1585.002 • Phishing (Mobile) – T1660 • Trusted Relationship – T1199 • Serverless Execution –T1648 • User Execution: Malicious Link – T1204.001 • Modify Authentication Process: Multi-Factor Authentication – T1556.006 • Valid Accounts: Default Accounts – T1078.001 • Valid Accounts: Domain Accounts – T1078.002 • Valid Accounts: Cloud Accounts – T1078.004 • Domain Policy Modification: Domain Trust Modification – T1484.002 • Modify Cloud Compute Infrastructure: Create Cloud Instance – T1578.002 • Forge Web Credentials – T1606 • Multi-Factor Authentication Request Generation – T1621 • Unsecured Credentials: Credentials in Files – T1552.001 • Unsecured Credentials: Private Keys – T1552.004 • Browser Information Discovery – T1217 • Cloud Service Dashboard – T1538 • File and Directory Discovery – T1083 • Remote System Discovery – T1018 • Steal Web Session Cookie – T1539 • Data from Information Repositories: Sharepoint – T1213.002 • Data from Information Repositories: Code Repositories – T1213.003 • Email Collection: Local Email Collection – T1114.001 • Email Collection: Remote Email Collection – T1114.002 • Data from Cloud Storage – T1530 • Remote Access Software – T1219 • Data Encrypted for Impact – T1486 • Exfiltration Over Web Service: Exfiltration to Cloud Storage – T1567.002 • Financial Theft – T1657 • Account Discovery: Email Account – T1087.003 • Account Discovery: Cloud Account – T1087.004 • Account Manipulation: Additional Cloud Credentials – T1098.001 • Account Manipulation: Additional Cloud Roles – T1098.003 • Account Manipulation: Device Registration – T1098.005 • Acquire Access – T1650 • Compromise Accounts: Cloud Accounts – T1586.003 • Impersonation – T1656 • Ingress Tool Transfer – T1105

	• Network Service Discovery – T1046 • OS Credential Dumping: DCSync – T1003.006 • Permission Groups Discovery: Cloud Groups – T1069.003 • Web Service – T1102 • Windows Management Instrumentation – T1047 • Gather Victim Network Information: Domain Properties – T1590.001 • Gather Victim Org Information: Identify Roles – T1591.004 • Obtain Capabilities: Malware – T1588.001 • Obtain Capabilities: Tool – T1588.002 • Obtain Capabilities: Vulnerabilities – T1588.006 • Protocol Tunneling – T1572 • Proxy – T1090 • Search Open Websites/Domains – T1593 • Search Victim-Owned Websites – T1594

Activity	
Activity score	This threat actor is **VERY ACTIVE**.