Scattered Spider Social Engineering Attack

Doc Ref No.: SQTK/ADV/2023/0062 - Scattered Spider - Social Engineering Attack – IoC

INDICATORS OF COMPROMISE

IoCs indicated here refer to Sequretek Advisory (SQTK/ADV/0062- Scattered Spider-Social Engineering Attack – 29 Nov 2023).

IPs

IPs
136[.]144[.]43[.]81
141[.]94[.]177[.]172
119[.]93[.]5[.]239
136[.]144[.]19[.]51
100[.]35[.]70[.]106

Domain

Domains
victimname-sso[.]com
victimname-servicedesk[.]com
victimname-okta[.]com

Scattered Spider Associated File Hashes (SHA-256):

Hash (SHA256)
0440ef40c46fdd2b5d86e7feef8577a8591de862cfd7928cdbcc8f47b8fa3ffc
9b1b15a3aacb0e786a608726c3abfc94968915cedcbd239ddf903c4a54bfcf0c
c8f9e1ad7b8cce62fba349a00bc168c849d42cfb2ca5b2c6cc4b51d054e0c497
5f6fec8f7890d032461b127332759c88a1b7360aa10c6bd38482572f59d2ba8b
6839fcae985774427c65fe38e773aa96ec451a412caa5354ad9e2b9b54ffe6c1
7f4555a940ce1156c9bcea9a2a0b801f9a5e44ec9400b61b14a7b1a6404ffdf6
d7c81b0f3c14844f6424e8bdd31a128e773cb96cccef6d05cbff473f0ccb9f9c
8e035beb02a411f8a9e92d4cf184ad34f52bbd0a81a50c222cdd4706e4e45104
648c2067ef3d59eb94b54c43e798707b030e0383b3651bcc6840dae41808d3a9
0d10c4b2f56364b475b60bd2933273c8b1ed2176353e59e65f968c61e93b7d99
274340f7185a0cc047d82ecfb2cce5bd18764ee558b5227894565c2f9fe9f6ab
42b22faa489b5de936db33f12184f6233198bdf851a18264d31210207827ba25
982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46dada624af0316044e
b6e82a4e6d8b715588bf4252f896e40b766ef981d941d0968f29a3a444f68fef
e23283e75ed2bdabf6c703236f5518b4ca37d32f78d3d65b073496c12c643cfe
acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918
3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08
4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93
443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58
4f94155e5a1a30f7b05280dd5d62c3410bcc52aea03271d086afa5dc5d97e585

Scattered Spider Associated File Hashes (SHA-1):

Hash (SHA1)
b2f955b3e6107f831ebe67997f8586d4fe9f3e98
91568d7a82cc7677f6b13f11bea5c40cf12d281b
994e3f5dd082f5d82f9cc84108a60d359910ba79
0bec69c1b22603e9a385495fbe94700ac36b28e5
17bd8fda268cbb009508c014b7c0ff9d8284f850
5ed22c0033aed380aa154e672e8db3a2d4c195c4
78cd4dfb251b21b53592322570cc32c6678aa468
c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91
cb25a5125fb353496b59b910263209f273f3552d

MITRE ATT&CK TACTICS AND TECHNIQUES

Technique Title	ID	Use
Initial Access		
Phishing	T1566	Scattered Spider threat actors use broad phishing attempts against a target to obtain information used to gain initial access.
		Scattered Spider threat actors have posed as helpdesk personnel to direct employees to install commercial remote access tools.
Phishing (Mobile)	T1660	Scattered Spider threat actors send SMS messages, known as smishing, when targeting a victim.
Phishing: Spear phishing Voice	T1566.004	Scattered Spider threat actors use voice communications to convince IT help desk personnel to reset passwords and/or MFA tokens.
Trusted Relationship	T1199	Scattered Spider threat actors abuse trusted relationships of contracted IT help desks to gain access to targeted organizations.
Valid Accounts: Domain Accounts	T1078.002	Scattered Spider threat actors obtain access to valid domain accounts to gain initial access to a targeted organization.
Execution		
Gather Victim Identity Information	T1589	Scattered Spider threat actors gather usernames, passwords, and PII for targeted organizations.
Phishing for Information	T1598	Scattered Spider threat actors use phishing to obtain login credentials, gaining access to a victim's network.
Persistence		
Persistence	TA0003	Scattered Spider threat actors seek to maintain persistence on a targeted organization's network.
Create Account	T1136	Scattered Spider threat actors create new user identities in the targeted organization.

Modify Authentication Process: Multi-Factor Authentication	T1556.006	Scattered Spider threat actors may modify MFA tokens to gain access to a victim's network.
Valid Accounts	T1078	Scattered Spider threat actors abuse and control valid accounts to maintain network access even when passwords are changed.
Persistence	TA0003	Scattered Spider threat actors seek to maintain persistence on a targeted organization's network.
Privilege Escalation		
Privilege Escalation	TA0004	Scattered Spider threat actors escalate account privileges when on a targeted organization's network.
Domain Policy Modification: Domain Trust Modification	T1484.002	Scattered Spider threat actors add a federated identify provider to the victim's SSO tenant and activate automatic account linking.
Defense Evasion		
Modify Cloud Compute Infrastructure: Create Cloud Instance	T1578.002	Scattered Spider threat actors will create cloud instances for use during lateral movement and data collection.
Impersonation	TA1656	Scattered Spider threat actors pose as company IT and/or helpdesk staff to gain access to victim's networks.
Credential Access		
Credential Access	TA0006	Scattered Spider threat actors use tools, such as Raccoon Stealer, to obtain login credentials.
Forge Web Credentials	T1606	Scattered Spider threat actors may forge MFA tokens to gain access to a victim's network.

Multi-Factor Authentication Request Generation	T1621	Scattered Spider sends repeated MFA notification prompts to lead employees to accept the prompt and gain access to the target network.
Unsecured Credentials: Credentials in Files	T1552.001	Scattered Spider threat actors search for insecurely stored credentials on victim's systems.
Unsecured Credentials: Private Keys	T1552.004	Scattered Spider threat actors search for insecurely stored private keys on victim's systems.
Discovery		
Discovery	TA0007	Upon gaining access to a targeted network, Scattered Spider threat actors seek out SharePoint sites, credential storage documentation, VMware vCenter, infrastructure backups and enumerate AD to identify useful information to support further operations.
Browser Information Discovery	T1217	Scattered Spider threat actors use tools (e.g., Raccoon Stealer) to obtain browser histories.
Cloud Service Dashboard	T1538	Scattered Spider threat actors leverage AWS Systems Manager Inventory to discover targets for lateral movement.
File and Directory Discovery	T1083	Scattered Spider threat actors search a compromised network to discover files and directories for further information or exploitation.
Remote System Discovery	T1018	Scattered Spider threat actors search for infrastructure, such as remote systems, to exploit.
Steal Web Session Cookie	T1539	Scattered Spider threat actors use tools, such as Raccoon Stealer, to obtain browser cookies.
Lateral Movement		
Lateral Movement	TA0008	Scattered Spider threat actors laterally move across a target network upon gaining access and establishing persistence.

Remote Services: Cloud Services	T1021.007	Scattered Spider threat actors use pre-existing cloud instances for lateral movement and data collection.
Collection		
Data from Information Repositories: Code Repositories	T1213.003	Scattered Spider threat actors search code repositories for data collection and exfiltration.
Data from Information Repositories: Sharepoint	T1213.002	Scattered Spider threat actors search SharePoint repositories for information.
Data Staged	T1074	Scattered Spider threat actors stage data from multiple data sources into a centralized database before exfiltration.
Email Collection	T1114	Scattered Spider threat actors search victim's emails to determine if the victim has detected the intrusion and initiated any security response.
Command and Control		
Remote Access Software	T1219	Impersonating helpdesk personnel, Scattered Spider threat actors direct employees to run commercial remote access tools thereby enabling access to and command and control of the victim's network. Scattered Spider threat actors leverage third-party software to facilitate lateral movement and maintain persistence on a target organization's network.
Exfiltration		
Exfiltration	TA0010	Scattered Spider threat actors exfiltrate data from a target network to for data extortion.

Impact		
Data Encrypted for Impact	T1486	Scattered Spider threat actors recently began encrypting data on a target network and demanding a ransom for decryption. Scattered Spider threat actors has been observed encrypting VMware ESXi servers.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Scattered Spider threat actors exfiltrate data to multiple sites including U.S.-based data centers and MEGA[.]NZ.
Financial Theft	T1657	Scattered Spider threat actors monetized access to victim networks in numerous ways including extortion-enabled ransomware and data theft.

Table 4: MITRE ATT&CK Techniques/Sub Techniques