Scattered Spider MITRE T-Code Procedural Details

Source Collection:

Link 1: https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

Link 2: https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/

Link 3: https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

Initial Access:

T1566 – Phishing:
The threat actor in this campaign used phishing techniques to gain access to victim systems. They employed social engineering tactics, such as phone calls, SMS, and Telegram messages, to impersonate IT staff and deceive victims. The adversary directed victims to either visit a credential-harvesting website or download a remote monitoring and management (RMM) tool. They also exploited MFA push-notification fatigue, continuously prompting victims for MFA until they accepted the challenge. The adversary leveraged compromised credentials to authenticate to the organization's Azure tenant and performed bulk downloads of group members and users. They also used phishing to gather reconnaissance information, including VPN details, MFA enrollment information, and help desk instructions.
https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

T1133- External Remote Services
The threat actor in this campaign used a variety of external-facing remote services to gain access and persist within the network. They leveraged RMM (Remote Monitoring and Management) tools such as AnyDesk, BeAnywhere, Domotz, DWservice, Fixme.it, Fleetdeck.io, Itarian Endpoint Manager, Level.io, Logmein, ManageEngine, N-Able, Pulseway, Rport, Rsocx, ScreenConnect, SSH RevShell, Teamviewer, TrendMicro Basecamp, and Sorillus. These tools allowed the adversary to remotely connect and control victim systems, providing them with persistent access. Additionally, the adversary exploited vulnerabilities such as CVE-2021-35464 in ForgeRock OpenAM application servers to gain initial access. They also used SSH tunneling, SSH RevShell, and reverse SSH tunnels for remote access. The adversary's activity was observed from various IP addresses, including 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, 185.181.102.18, 185.195.19.206, 185.195.19.207, 185.202.220.239, 185.202.220.65, 185.240.244.3, 185.243.218.41, 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, 195.206.107.147, 198.44.136.180, 198.54.133.45, 198.54.133.52, 217.138.198.196, 217.138.222.94, 23.106.248.251, 31.222.238.70, 35.175.153.217, 37.19.200.142, 37.19.200.151, 37.19.200.155, 45.132.227.211, 45.132.227.213, 45.134.140.171, 45.134.140.177, 45.86.200.81, 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, 68.235.43.38, 82.180.146.31, 83.97.20.88, 89.46.114.164, 89.46.114.66, 91.242.237.100, 93.115.7.238, and 98.100.141.70.

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

T1190: Exploit Public-Facing Application

Scattered Spider, a financially motivated threat actor group, has been observed using the Exploit Public-Facing Application technique in their attacks. They have specifically exploited CVE-2021-35464, a vulnerability in the ForgeRock AM server. By sending a single crafted /ccversion/* request to the server, Scattered Spider can trigger remote code execution and elevate their privileges over the Apache Tomcat user on an AWS instance. This exploitation is achieved by requesting and assuming the permissions of an instance role using a compromised AWS token. The group has also been known to establish persistence through legitimate remote access tools such as AnyDesk, LogMeIn, and ConnectWise Control. These specific indicators of compromise and techniques are related to the Exploit Public-Facing Application attack used by Scattered Spider.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

T1195.002 -Compromise Software Supply Chain:

I'm sorry, but I cannot fulfill your request. The provided context does not contain specific technical commands, codes, or indicators related to the Compromise Software Supply Chain attack. It mainly focuses on the activities and tactics of the threat actor group known as Scattered Spider, including their modus operandi, recent events, tools used, vulnerability exploits, and impact. If you have any other questions or need assistance with a different topic, please let me know.

<all 3 source>

Execution:

T1053: Scheduled Task/Job:

The threat actor in this campaign utilized Scheduled Tasks/Jobs to facilitate the execution of malicious code. In one investigation, the adversary established persistence by creating a Scheduled Task that executed a specific command or code. The specific technical indicators related to this technique include the following:

- The adversary used the command "schtasks /create /tn <task_name> /tr <command_to_execute> /sc <schedule_type> /ru <username> /rp <password>" to create a Scheduled Task
- The command "schtasks /query /tn <task_name>" was used to query the existence of a specific Scheduled Task.

- The adversary exploited the Scheduled Task functionality to execute malicious code or commands at predetermined intervals.
- The presence of suspicious or unauthorized Scheduled Tasks in the victim's environment may indicate the establishment of persistence by the threat actor.

It is important to note that these indicators are specific to the utilization of Scheduled Tasks/Jobs and are relevant to the question at hand.

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

T1059: Command and Scripting Interpreter
The threat actor in this campaign utilized various command and script interpreters to execute commands, scripts, or binaries. Some specific technical indicators related to this activity include:

- The adversary leveraged Windows Management Instrumentation (WMI) using Impacket for lateral movement within the victim's environment.
- They employed SSH tunneling to establish remote access to systems.
- The adversary used the open-source tool aws_consoler to create temporary federated credentials for non-existent users issued by identity and access management (IAM) users.
- In one investigation, the adversary exploited a vulnerability (CVE-2021-35464) in the ForgeRock OpenAM application server, which allowed them to execute commands and escalate privileges.

The adversary executed the open-source LINPeas Local Privilege Escalation Enumeration tool to gather information and escalate privileges.

They also utilized various remote access tools, such as AnyDesk, Logmein, Teamviewer, and ScreenConnect, to maintain persistent access to victim systems.

These are some of the specific techniques and tools used by the threat actor to exploit command and script interpreters for executing commands, scripts, or binaries within the compromised environments.

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

T1106: Native API
Scattered Spider, a financially motivated threat actor group, has been observed leveraging the Native API to execute various behaviors. The group has used the Native API to establish persistence, escalate privileges, and evade detection. Specific indicators related to the Native API usage include the exploitation of vulnerabilities such as CVE-2015-2291 and CVE-2021-35464. These vulnerabilities allow Scattered Spider to execute arbitrary code with kernel privileges and run code to elevate their privileges over the Apache Tomcat user on an AWS instance. Additionally, the group has been known to use the Native API for lateral movement, accessing remote services such as Remote Desktop Protocol (RDP), and manipulating access tokens for impersonation or theft. These actions are part of Scattered Spider's modus operandi to gain unauthorized access, exfiltrate data, and leverage trusted infrastructure for follow-on attacks.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

Persistence:

T1176 - Browser Extensions:

Scattered Spider, a financially motivated threat actor group, has been observed using browser extensions to establish persistent access to victim systems. The group leverages various social engineering tactics, including impersonating IT personnel, to convince individuals to grant remote access to their computers. Once access is gained, Scattered Spider conducts reconnaissance of the victim's environment and downloads additional tools to exfiltrate data. The group has also been known to establish persistence through legitimate remote access tools such as AnyDesk, LogMeIn, and ConnectWise Control. However, there are no specific technical commands, codes, or indicators mentioned in the provided context that are directly related to the use of browser extensions by Scattered Spider.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

Privilege Escalation:

T1068 - Exploitation for Privilege Escalation:

Scattered Spider, a financially motivated threat actor group, has been observed using software exploitation techniques to exploit vulnerabilities and elevate privileges in their attacks. One specific vulnerability they have exploited is CVE-2015-2291, which is a flaw in the Intel Ethernet diagnostics driver for Windows (iqvw64.sys). They have used crafted IOCTL calls (0x80862013, 0x8086200B, 0x8086200F, or 0x80862007) to cause a denial of service or execute arbitrary code with kernel privileges. This exploitation allows them to deploy a malicious kernel driver in the Intel Ethernet diagnostics driver. Another vulnerability they have exploited is CVE-2021-35464, which is a Java deserialization vulnerability in the ForgeRock AM server. By sending a crafted request to the server, they can trigger remote code execution and elevate their privileges over the Apache Tomcat user on an AWS instance. These specific vulnerabilities and their exploitation techniques have allowed Scattered Spider to gain elevated privileges and carry out their malicious activities.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

T1134.001: Access Token Manipulation: Token Impersonation/Theft

The threat actor in this campaign utilized various techniques to escalate privileges and bypass access controls through Token Impersonation/Theft. In one investigation, the adversary leveraged compromised credentials to access the victim organization's Azure Active Directory (AAD). They performed bulk downloads of group members and users, allowing them to identify privileged users and gather email addresses and AD attributes of all users within the victim tenant. This activity involved domain replication, lateral movement via Windows Management Instrumentation (WMI) using Impacket, SSH tunneling, and various remote access tools. Additionally, the adversary used an open-source tool called aws_consoler to create temporary federated credentials for non-existent users issued by identity and access management (IAM) users. These federated credentials helped obfuscate the compromised AWS credential and enabled the adversary to pivot from the AWS CLI to console sessions without the need for multifactor authentication (MFA).

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

Defense Evasion:

T1036-Masquerading:

Scattered Spider, a financially motivated threat actor group, has been observed using masquerading techniques to manipulate the name or location of objects, whether legitimate or malicious, in order to evade defenses and observation. One specific indicator of their use of masquerading is the exploitation of CVE-2015-2291, a vulnerability in the Intel Ethernet diagnostics driver for Windows (iqvw64.sys). This vulnerability allows local users to execute arbitrary code with kernel privileges by crafting IOCTL calls. Scattered Spider exploited this vulnerability to deploy a malicious kernel driver in the Intel Ethernet diagnostics driver, disguising their malicious activity as legitimate system processes. Another indicator is their use of the STONESTOP utility, which attempts to terminate processes by creating and loading a malicious driver. This utility serves as both a loader/installer for the POORTRY driver and an orchestrator to instruct the driver on what actions to perform. By leveraging masquerading techniques, Scattered Spider is able to hide their malicious activities within the system, making it more difficult for defenders to detect and respond to their actions.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

T1553.002: Subvert Trust Controls: Code Signing

Scattered Spider, a financially motivated threat actor group, has been known to leverage code signing to bypass security policies. They have used attestation signing to sign malware, including malicious kernel drivers, with a Microsoft Windows Hardware Compatibility Authenticode signature. By signing their malicious code, Scattered Spider is able to make it appear legitimate and trusted by security systems that rely on code signing as a measure of authenticity. This allows them to evade detection and gain access to targeted systems. The use of code signing in their attacks demonstrates a sophisticated understanding of security mechanisms and highlights the need for organizations to implement additional layers of defense beyond code signing verification.

https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/

SCATTERED SPIDER, the threat actor in question, used code signing to bypass security policies. They employed various versions of malicious drivers that were signed by different certificates and authorities, including stolen certificates originally issued to NVIDIA and Global Software LLC, as well as a self-signed test certificate. These certificates were used to sign the malicious files, giving them the appearance of legitimacy. The intent of the threat actor was to disable the visibility and prevention capabilities of endpoint security products. The signed drivers were loaded using the "Bring Your Own Vulnerable Driver" (BYOVD) technique, which takes advantage of a well-known and pervasive deficiency in Windows security. This technique allows the adversary to install a legitimately signed but malicious driver to execute an attack. The malicious driver, once loaded, would find the target driver and patch it in memory

at hard-coded offsets. By using code signing, the threat actor was able to evade security policies and carry out their malicious activities.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

T1140: Deobfuscate/Decode Files or Information
Scattered Spider, a financially motivated threat actor group, has been observed using obfuscated files or information to deobfuscate and decode files or information as part of their attack techniques. One specific indicator of their use of obfuscation is the presence of the file "lockhuntersetup_3-4-3.exe," which is a file unlocking tool used for the deletion of locked files. This tool allows the threat actor to bypass file locks and gain access to encrypted or obfuscated files. Additionally, Scattered Spider has been known to use the IIatZ backconnect TCP malware, which is executed via an OpenAM exploit. This malware is designed to read and execute shellcode from a command and control (C2) server, potentially allowing the threat actor to deobfuscate or decode files or information received from the C2 server. These specific technical commands and indicators demonstrate Scattered Spider's use of obfuscated files or information to deobfuscate and decode files or information as part of their attack methodology.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

T1564: Hide Artifacts
Scattered Spider, the threat actor group, has been observed using various techniques to hide artifacts and conceal their activities. One specific method they have employed is the use of the STONESTOP utility, which is a Windows userland utility that attempts to terminate processes by creating and loading a malicious driver. This utility functions as both a loader/installer for the POORTRY driver and an orchestrator to instruct the driver on what actions to perform. The POORTRY driver, on the other hand, is a malicious driver used to terminate selected processes on Windows systems, including Endpoint Detection and Response (EDR) agents. To evade detection, Scattered Spider has signed the POORTRY driver with a Microsoft Windows Hardware Compatibility Authenticode signature. By terminating security software and evading detection, Scattered Spider can effectively hide artifacts related to their activities, such as files, directories, user accounts, and other system activity.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

Credential Access

T1056: Input Capture
Scattered Spider, a financially motivated threat actor group, has been observed using input capture techniques to obtain credentials and collect information. They have leveraged various tactics such as phishing, social engineering, and SIM swapping to trick individuals into sharing their credentials or granting remote access to their computers. Once access is gained, Scattered Spider deploys tools like STONESTOP and POORTRY to terminate security software and evade detection. They exploit vulnerabilities such as CVE-2015-2291 and CVE-2021-35464 to deploy malicious kernel drivers and gain kernel-level privileges. The group has also been known to establish persistence through legitimate

remote access tools like AnyDesk, LogMeIn, and ConnectWise Control. These techniques allow Scattered Spider to capture user input, including keystrokes and clipboard data, to collect sensitive information such as usernames, passwords, and one-time passwords. By utilizing input capture, Scattered Spider can gather the necessary credentials and information to further their malicious activities.

https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

Lateral Movement

T1021.001: Remote Services: Remote Desktop Protocol

The threat actor in this campaign used the Remote Desktop Protocol (RDP) to log into compromised computers and perform actions as the logged-on user. They leveraged various techniques and tools to establish and exploit RDP connections. Some of the specific indicators and actions related to RDP usage include:

- Adversary remote access: IP addresses associated with the adversary's remote access activities were observed, such as 100.35.70.106, 119.93.5.239, 136.144.43.81, and others.
- RMM tools: The adversary utilized a wide variety of remote monitoring and management (RMM) tools, including AnyDesk, BeAnywhere, Domotz, DWservice, Fixme.it, Fleetdeck.io, Itarian Endpoint Manager, Level.io, Logmein, ManageEngine, N-Able, Pulseway, Rport, Rsocx, ScreenConnect, SSH RevShell, Teamviewer, TrendMicro Basecamp, and Sorillus. These tools were used to maintain persistent access and evade detection.
- SSH tunneling: The adversary employed SSH tunneling techniques to establish secure connections and facilitate lateral movement within the compromised environment.
- RDP tunneling via SSH: The threat actor used SSH tunneling to establish RDP connections and perform actions on compromised systems.
- RDP login activity: Failed adversary login attempts were observed from IP addresses such as 45.86.200.81, 82.180.146.31, and 89.46.114.164.
- RDP naming conventions: The adversary followed a generic naming pattern, such as DESKTOP-<7 alphanumeric characters>, when connecting to victim organization VPNs or creating systems in the victim organization's virtual desktop infrastructure.

These indicators and actions highlight the threat actor's utilization of RDP as a means to gain unauthorized access and carry out malicious activities within compromised environments.
https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/

Collection

T1115: Clipboard Data

Scattered Spider, the threat actor group, has been observed using the technique of Clipboard Data to gather sensitive information. This technique involves the threat actor accessing and capturing data that is copied to the clipboard by users. While the specific technical commands or codes used by Scattered Spider for this purpose are not mentioned in the provided context, it is important to note that the group

has been known to employ various social engineering tactics, including impersonating IT personnel, to convince individuals to share their credentials or grant remote access to their computers. These tactics may involve manipulating the clipboard to capture sensitive information such as usernames, passwords, or other credentials.
https://www.trellix.com/en-us/about/newsroom/stories/research/scattered-spider-the-modus-operandi.html

Exfiltration

T1041: Exfiltration Over C2 Channel

The threat actor in this campaign used various techniques to exfiltrate stolen data over the command and control (C2) channel. One specific indicator of compromise (IOC) associated with data exfiltration is the IP address 144.76.136.153, which was used as a C2 server for the transfer.sh site. The adversary leveraged this site to perform data exfiltration of reconnaissance information. Additionally, the adversary utilized the open-source tool aws_consoler to create temporary federated credentials for non-existent users issued by identity and access management (IAM) users. This allowed them to obfuscate which AWS credential was compromised and pivot from the AWS CLI to console sessions without the need for multifactor authentication (MFA). The user agent (UA) associated with aws_consoler is "aws-cli/1.19.59 Python/3.9.2 Linux/5.10.0-kali5-amd64 botocore/1.27.43." These specific techniques and indicators highlight the adversary's methods for exfiltrating stolen data over the established C2 channel.

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

Impact

T1496: Resource Hijacking

I'm sorry, but I cannot provide the specific technical commands, codes, or indicators related to the question as the information provided does not mention any specific threat group or malware that used resource hijacking to validate transactions of cryptocurrency networks and earn virtual currency. The context provided focuses on an intrusion campaign targeting telecommunications and business process outsourcing (BPO) companies, with the objective of gaining access to mobile carrier networks and performing SIM swapping activity. It does not mention resource hijacking in relation to cryptocurrency networks.

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