Scattered Spider: The Modus Operandi

Blogs

The latest cybersecurity trends, best practices, security vulnerabilities, and more

By Trellix · August 17, 2023
This story was also written by Phelix Oluoch

Executive Summary

Scattered Spider, also referred to as UNC3944, Scatter Swine, and Muddled Libra, is a financially motivated threat actor group that has been active since May 2022. Scattered Spider has largely been observed targeting telecommunications and Business Process Outsourcing (BPO) organizations. However, recent activity indicates that this group has started targeting other sectors, including critical infrastructure organizations.

Despite this change in targets, Scattered Spider continues to leverage a variety of social engineering tactics, including Telegram and SMS phishing, SIM swapping, MFA fatigue, and other tactics as part of their attacks. This group has often been observed impersonating IT personnel to convince individuals to share their credentials or grant remote access to their computers, has been linked to several past phishing campaigns and deployments of malicious kernel drivers – including the use of a signed but malicious version of the Windows Intel Ethernet diagnostics driver.

This blog takes a deep dive into the modus operandi of Scattered Spider; the recent events and tools leveraged by the threat actor, vulnerabilities exploited, and their impact. Additionally, the MITRE ATT&CK Techniques/Sub-Techniques and their mitigations. Finally, the known associated indicators of compromise that can be used to implement detection, prevention, and response strategies.

Recent Events

Scattered Spider typically exploits vulnerabilities such as CVE-2015-2291 and utilize tools like STONESTOP and POORTRY to terminate security software and evade detection.[1] The group demonstrates a deep understanding of the Azure environment and leverages built-in tools for their attacks.[2] Once initial access has been gained, Scattered Spider has been observed conducting reconnaissance of various environments, including Windows, Linux, Google Workspace, Azure Active Directory, Microsoft 365, and AWS, as well as conducting lateral movement and downloading additional tools to exfiltrate VPN and MFA enrollment data in select cases. The group has also been known to establish persistence through legitimate remote access tools such as AnyDesk, LogMeIn, and ConnectWise Control.[3]

By January 2023, Scattered Spider was involved in more than half a dozen incidents from mid-2022 where large outsourcing firms serving high-value cryptocurrency institutions and individuals were targeted.[4]

In December 2022, Scattered Spider conducted campaigns targeting telecom and BPO organizations.[5] The objective of the campaign appeared to be to gain access to mobile carrier networks and, as evidenced in two investigations, perform SIM swapping activity. Initial access was varied: Social engineering using phone calls and text messages to impersonate IT personnel, and either directing victims to a credential harvesting site or directing victims to run commercial Remote Monitoring and Management (RMM) tools. The campaigns were extremely persistent and brazen. Once the adversary was contained or operations are disrupted, they immediately moved to target other organizations within the telecom and BPO sectors.[6]

In the same month, their use of attestation signing to sign malware was discovered.[7] Microsoft disclosed the steps they took to implement blocking protections and suspend accounts that were used to publish malicious drivers that were certified by its Windows Hardware Developer Program. The problem was initiated after Microsoft was notified of rogue drivers being used in post-exploitation efforts, including deploying ransomware.[8]

In August 2022, Twilio identified unauthorized access to information related to 163 Twilio customers, including Okta. Mobile phone numbers and associated SMS messages containing one-time passwords were accessible to Scattered Spider via the Twilio console. The phishing kit used by the threat actor was designed to capture usernames, passwords, and OTP factors and targeted technology companies, telecommunications providers and organizations and individuals linked to cryptocurrency.[9]

Tools

Scattered Spider uses POORTRY and STONESTOP to terminate security software and evade detection.[10]

- POORTRY is a malicious driver used to terminate selected processes on Windows systems, e.g., Endpoint Detection and Response (EDR) agent on an endpoint.[11] To evade detection, attackers have signed POORTRY driver with a Microsoft Windows Hardware Compatibility Authenticode signature.[12]
- STONESTOP is a Windows userland utility that attempts to terminate processes by creating and loading a malicious driver.[13] It functions as both a loader/installer for POORTRY, as well as an orchestrator to instruct the driver with what actions to perform.[14]

In April 2023, ALPHV (BlackCat) ransomware group used an updated version of POORTRY to compromise the US payments giant NCR, leading to an outage on its Aloha point of sale platform.[15, 16]

Vulnerability Exploits

Scattered Spider is known to exploit CVE-2015-2291 which is a vulnerability in the Intel Ethernet diagnostics driver for Windows (iqvw64.sys) that allows local users to cause a denial of service or possibly execute arbitrary code with kernel privileges via a crafted (a) 0x80862013, (b) 0x8086200B, (c) 0x8086200F, or (d) 0x80862007 IOCTL call.[17] Scattered Spider exploited CVE-2015-2291 to deploy a malicious kernel driver in the Intel Ethernet diagnostics driver for Windows (iqvw64.sys).[18]

Additionally, Scattered Spider has exploited CVE-2021-35464 which is a flaw in the ForgeRock AM server. ForgeRock AM server versions before 7.0 have a Java deserialization vulnerability in the `jato.pageSession` parameter on multiple pages. The exploitation does not require authentication, and remote code execution can be triggered by sending a single crafted `/ccversion/*` request to the server. The vulnerability exists due to the usage of Sun ONE Application Framework (JATO) found in versions of Java 8 or earlier.[19] Scattered Spider exploited CVE-2021-35464 to run code and elevate their privileges over the Apache Tomcat user on an AWS instance. This was achieved by requesting and assuming the permissions of an instance role using a compromised AWS token.[20]

Impact

Scattered Spider is known for theft of sensitive data and leveraging trusted organizational infrastructure for follow-on attacks on downstream customers.[21]

Trellix Product Coverage

Trellix Endpoint, Network, and Email Security offers a multi-layered detection strategy for Scattered Spider activities including checks on the IOCs and behavioral analysis to ensure that any potential threat is discovered and stopped from doing harm to our customers. To stay ahead of new and evolving threats, our products continuously monitor and update their threat intelligence databases. That includes the Trellix Multi-Vector Virtual Execution Engine, a new anti-malware core engine, machine-learning behavior classification and AI correlation engines, real-time threat intelligence from the Trellix Global Threat Intelligence (GTI) and Dynamic Threat Intelligence (DTI) Cloud, and defenses across the entire attack lifecycle to keep your organization safer and more resilient.

Trellix Protection

Product	**Signature**
Endpoint Security (ENS)	LINUX/Agent.bj
FireEye Scanner	Trojan.Linux.Generic.289912

MITRE ATT&CK Techniques/Sub Techniques

MITRE ATT&CK ENTERPRISE

INITIAL ACCESS	EXECUTION	PERSISTENSE	PRIVILEGE ESCALATION	DEFENCE EVASION	CREDENTIAL ACCESS	LATERAL MOVEMENT
T1566: Phishing	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1068: Exploitation for Privilege Escalation	T1036: Masquerading	T1056: Input Capture	T1021.001: Remote Services: Remote Desktop Protocol
T1133: External Remote Services	T1059: Command and Scripting Interpreter	T1133: External Remote Services	T1134.001: Access Token Manipulation: Token Impersonation/Theft	T1553.002: Subvert Trust Controls: Code Signing		T1210: Exploitation of Remote Services

T1190: Exploit Public-Facing Application	T1106: Native API	T1176: Browser Extensions	T1053: Scheduled Task/Job	T1134.001: Access Token Manipulation: Token Impersonation/Theft			
T1195.002: Compromise Software Supply Chain				T1140: Deobfuscate/Decode Files or Information			
				T1564: Hide Artifacts			

MITRE ATT&CK MOBILE

COLLECTION

NETWORK EFFECTS

T1616: Call Control

T1451: Sim Card Swap

Mitigations

1. M1051: Update software:
   Update software regularly by employing patch management for internal enterprise endpoints and servers to mitigate exploitation risk.[22]
2. M1017: User training.
   Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spear phishing, social engineering, and other techniques that involve user interaction.[23]
3. M1011: User Guidance:
   Users should be instructed to use forms of multifactor authentication not subject to being intercepted by a SIM card swap, where possible. More secure methods include application-based one-time passcodes (such as Google Authenticator), hardware tokens, and biometrics. Additionally, users should be encouraged to be very careful with what applications they grant phone call-based permissions to. Further, users should not change their default call handler to applications they do not recognize.[25]
4. M1049: Antivirus/Antimalware
   Anti-virus can be used to automatically quarantine suspicious files.[26]
5. M1040: Behavior Prevention on Endpoint
   Implement security controls on the endpoint, such as a Host Intrusion Prevention System (HIPS), to identify and prevent execution of potentially malicious files (such as those with mismatching file signatures).[27]
6. M1045: Code Signing
   Require signed binaries[28] and enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.[29]
7. M1038: Execution Prevention
8. Use tools that restrict program execution via application control by attributes other than file name for common operating system utilities that are needed.[30] Additionally, consider blocking the execution of known vulnerable drivers that adversaries may exploit to execute code in kernel mode. Validate driver block rules in audit mode to ensure stability prior to production deployment.[31]
9. M1021: Restrict Web-Based Content
   Restrict use of certain websites, block downloads/attachments, block JavaScript, restrict browser extensions, etc.[32]
10. M1022: Restrict File and Directory Permissions
    Use file system access controls to protect folders such as C:\Windows\System32.[33]

11. M1042: Disable or Remove Feature or Program
    Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.[34]
12. M1048: Application Isolation and Sandboxing
13. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualizations and application micro segmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist.[35]
14. M1031: Network Intrusion Prevention
    Use intrusion detection signatures to block traffic at network boundaries.[36]
15. M1032: Multi-factor Authentication
    Security applications that look for behavior used during exploitation can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.[37]
16. M1050: Exploit Protection
    Use intrusion detection signatures to block traffic at network boundaries.[38]
17. M1019: Threat Intelligence Program
    Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization.[39]
18. M1026: Privileged Account Management
    Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object.[40] Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command runas.[41]
19. M1018: User Account Management
    Restrict users and accounts to the least privileges they require. An adversary must already have administrator level access on the local system to make full use of this technique.[42]
20. 18. M1047: Audit
    Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. [43]
21. M1028: Operating System Configuration
    Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM . The associated Registry key is located at `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl`. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled.[44]
22. M1035: Limit Access to Resource Over Network
    Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.[45]
23. M1030: Network Segmentation
    Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.[46]
24. M1033: Limit Software Installation
    Block users or groups from installing unapproved software.[47]
25. M1016: Vulnerability Scanning
    Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.[48]
26. M0810: Out-of-Band Communications Channel
    Have alternative methods to support communication requirements during communication failures and data integrity attacks.[49]
27. M1057: Data Loss Prevention
    Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII), and restrict exfiltration of sensitive data.[50]

IOCs

IPV4

IPV4	Description
100.35.70.106	Adversary remote access
104.247.82.11	Adversary remote access
105.101.56.49	Adversary remote access
105.158.12.236	Adversary remote access
119.93.5.239	Adversary remote access
134.209.48.68	Adversary remote access
136.144.19.51	Adversary MFA registration
136.144.43.81	Adversary remote access
137.220.61.53	Adversary remote access
138.68.27.0	Adversary remote access
141.94.177.172	

Adversary remote access

142.93.229.86

Adversary remote access

143.244.214.243

Adversary remote access

144.76.136.153

IP associated with transfer.sh used for data exfil

146.190.44.66

Adversary remote access

146.70.103.228

Adversary MFA registration

146.70.107.71

Adversary remote access

146.70.112.126

Adversary remote access

146.70.127.42

Adversary MFA registration

146.70.45.166

Adversary remote access

146.70.45.182

Adversary remote access

149.28.125.96

Adversary remote access

152.89.196.111

Adversary remote access

157.245.4.113

Adversary remote access

159.223.208.47

Adversary remote access

159.223.213.174

Adversary remote access

159.223.238.0

Adversary remote access

162.118.200.173

Adversary remote access

162.19.135.215

Adversary remote access

164.92.234.104

Adversary remote access

165.22.201.77

Adversary remote access

165.22.201.77

Adversary remote access

165.22.201.77

Adversary remote access

167.99.221.10

	Adversary remote access
169.150.203.51	Adversary remote access
172.96.11.245	Adversary remote access
172.98.33.195	Adversary remote access
173.239.204.129	Adversary MFA registration
173.239.204.130	Adversary remote access
173.239.204.131	Adversary MFA registration
173.239.204.132	Adversary remote access
173.239.204.133	Adversary remote access
173.239.204.134	Adversary remote access
180.190.113.87	Failed adversary login
185.120.144.101	Adversary remote access

185.123.143.197

Adversary remote access

185.123.143.201

Adversary remote access

185.123.143.205

Adversary remote access

185.123.143.217

Adversary remote access

185.156.46.141

Adversary remote access

185.181.102.18

Adversary remote access

185.195.19.206

Adversary remote access

185.195.19.207

Adversary remote access

185.202.220.239

Adversary remote access

185.202.220.65

Adversary remote access

185.240.244.3

Registered authenticator app and adversary VPN logins

185.243.218.41

Adversary remote access

185.247.70.229

Adversary remote access

185.45.15.217

Adversary remote access

185.56.80.28

Adversary remote access

185.56.80.28

Adversary remote access

188.166.101.65

Reverse SSH tunnel

188.166.117.31

Adversary remote access

188.166.92.55

Adversary remote access

188.214.129.7

Adversary remote access

192.166.244.248

Adversary remote access

193.149.129.177

Adversary remote access

193.27.13.184

Adversary remote access

193.37.255.114	Adversary remote access
194.37.96.188	Adversary remote access
195.206.105.118	Adversary remote access
195.206.107.147	Adversary remote access
198.44.136.180	Azure MFA registration
198.54.133.45	Adversary remote access
198.54.133.52	Adversary remote access
207.148.0.54	Adversary remote access
213.226.123.104	Adversary remote access
217.138.198.196	Adversary remote access
217.138.222.94	Adversary remote access
23.106.248.251	

	Adversary remote access
31.222.238.70	Adversary remote access
35.175.153.217	Adversary remote access
35.175.153.217	Adversary remote access
37.19.200.142	Adversary remote access
37.19.200.151	Adversary remote access
37.19.200.155	Adversary remote access
45.132.227.211	Adversary remote access
45.132.227.213	Adversary remote access
45.134.140.171	Adversary IP used to download documents from victim SharePoint
45.134.140.177	Adversary remote access
45.156.85.140	Adversary remote access

45.156.85.140
Adversary remote access
45.32.221.250
Adversary remote access
45.86.200.81
Adversary remote access
45.91.21.61
Adversary remote access
5.182.37.59
Adversary remote access
51.210.161.12
Adversary remote access
51.89.138.221
Adversary MFA registration
62.182.98.170
Adversary remote access
64.190.113.28
Adversary remote access
64.227.30.114
Adversary remote access
67.43.235.122
Adversary remote access
68.235.43.20

Adversary remote access

68.235.43.21

Adversary remote access

68.235.43.38

Failed adversary login activity

79.137.196.160

Adversary remote access

82.180.146.31

Failed adversary login activity

83.97.20.88

Adversary remote access

89.46.114.164

Failed adversary login activity

89.46.114.66

Adversary remote access

91.242.237.100

Adversary remote access

92.99.114.231

Adversary remote access

93.115.7.238

Adversary remote access

98.100.141.70

Adversary remote access

IPV6

IPV6	Description
2a01:4f8:200:1097::2	IPv6 associated with transfer.sh used for data exfiltration

CIDR

CIDR	Description
2a01:4f8:200:1097::2	IPv6 associated with transfer.sh used for data exfiltration

SHA256

SHA256	File Name	Description
N/A	change.m31!!!	Password used by adversary extensively
3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08	<redacted>.exe	Packed Fleet Deck binary
cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005	IlatZ	Backconnect TCP malware used to read and execute shellcode from C2, executed via OpenAM exploit

acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918

insomnia.exe

API debugging utility

N/A

linpeas.log

LINPeas Local Privilege Escalation Enumeration tool output log

N/A

linpeas.sh

LINPeas Local Privilege Escalation Enumeration tool

982dda5eec52dd54ff6b0b04fd9ba8f4c566534b78f6a46dada624af0316044e

lockhuntersetup_3-4-3.exe

File unlocking tool (for deletion of locked files)

443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58

mpbec

“Midgetpack” packed binary used to establish connections to 67.43.235.122 on ports 4444 and 8888

References

[1]https://www.bleepingcomputer.com/news/security/malicious-windows-kernel-drivers-used-in-blackcat-ransomware-attacks/
[2]https://www.bleepingcomputer.com/news/security/hackers-use-azure-serial-console-for-stealthy-access-to-vms/
[3]https://occamsec.com/scattered-spider-iocs/
[4]https://unit42.paloaltonetworks.com/muddled-libra/
[5]https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/
[5]https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/
[7]https://thehackernews.com/2022/12/ransomware-attackers-use-microsoft.html
[8]https://msrc.microsoft.com/update-guide/vulnerability/ADV220005
[9]https://sec.okta.com/scatterswine
https://www.bleepingcomputer.com/news/security/malicious-windows-kernel-drivers-used-in-blackcat-ransomware-attacks/
[10]https://www.mandiant.com/resources/blog/hunting-attestation-signed-malware
[11]https://www.bleepingcomputer.com/news/microsoft/microsoft-signed-malicious-windows-drivers-used-in-ransomware-attacks/
[12]https://www.mandiant.com/resources/blog/hunting-attestation-signed-malware
[13]https://www.sentinelone.com/labs/driving-through-defenses-targeted-attacks-leverage-signed-malicious-microsoft-drivers/
[14]https://securityaffairs.com/146536/malware/blackcat-ransomware-uses-kernel-driver.html
[15]https://status.aloha.ncr.com/incidents/cnl38krr6n6b

[16] https://nvd.nist.gov/vuln/detail/CVE-2015-2291

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

[18] https://nvd.nist.gov/vuln/detail/CVE-2021-35464

[19] https://www.sisainfosec.com/threat-a-licious/scattered-spider-a-sophisticated-threat-actor-that-can-reverse-defense-mitigation/#:~:text=Scattered%20Spider%2C%20a%20financially%20motivated,sites%2C%20and%20employing%20MFA%20fatigue.

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

[21] https://attack.mitre.org/mitigations/M1051/

[22] https://attack.mitre.org/mitigations/M1017/

[23] https://cyber-kill-chain.ch/mitigations/M1011/

[24] https://attack.mitre.org/mitigations/M1011/

[25] https://attack.mitre.org/mitigations/M1049/

[26] https://attack.mitre.org/mitigations/M1040/

[27] https://attack.mitre.org/mitigations/M1045/

[28] https://attack.mitre.org/mitigations/M0945/

[29] https://attack.mitre.org/mitigations/M1038/

[31] https://attack.mitre.org/mitigations/M1038/

[32] https://attack.mitre.org/mitigations/M1021/

[33] https://attack.mitre.org/mitigations/M1022/

[34] https://attack.mitre.org/mitigations/M1042/

[35] https://attack.mitre.org/mitigations/M1048/

[36] https://attack.mitre.org/mitigations/M1031/

[37] https://attack.mitre.org/mitigations/M1032/

[38] https://attack.mitre.org/mitigations/M1050/

[39] https://attack.mitre.org/mitigations/M1019/

[40] https://attack.mitre.org/techniques/T1134/

[41] https://attack.mitre.org/mitigations/M1026/

[42] https://attack.mitre.org/mitigations/M1018/

[43] https://attack.mitre.org/mitigations/M1047/

[44] https://attack.mitre.org/mitigations/M1028/

[45] https://attack.mitre.org/mitigations/M1035/

[46] https://attack.mitre.org/mitigations/M1030/

[47] https://attack.mitre.org/mitigations/M1033/

[48] https://attack.mitre.org/mitigations/M1016/

[49] https://attack.mitre.org/mitigations/M0810/

[50] https://attack.mitre.org/mitigations/M1057/

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers.