Scattered Spider Threat Actor Profile

Contact Us

Home / Threat Actors / Scattered Spider Threat Actor Profile

Scattered Spider Overview

Scattered Spider (also known as UNC3944 and Roasted 0ktapus) is a relatively new, financially motivated threat group that has been active since at least May 2022. The group is yet to receive a Microsoft designation but will fall into the Tempest (financially motivated) category once registered. The group commonly gains initial network access via stolen credentials obtained from SMS phishing operations and have been detected utilising Azure Serial Console to attain administrative console access to virtual machines (VMs) whilst executing a command prompt over the serial port.

Scattered Spider are reported to use a loader named ‘STONESTOP’ to install a malicious signed driver dubbed ‘POORTRY’, which is designed to terminate processes associated with security software and to delete files as part of a Bring Your Own Vulnerable Driver (BYOVD) attack. The group has been attributed to creating the STONESTOP and POORTRY toolkit to terminate security software.

Historically, Scattered Spider has mainly gained initial access to the victim environment via theft of administrative credentials by email and SMS phishing attacks or the use of stealware. Once credentials have been obtained, Scattered Spider use these to impersonate the admin and use sensitive data to gain access to the environment. Furthermore, they have also been observed continuing phishing attacks against other users, by leveraging the employee database. This is likely to maintain persistence and provides them with lateral movement within the network.

Targeted Sectors

Scattered Spider have targeted many sectors during their time in operation, including telecommunication, Business Process Outsourcing (BPO), Managed Security Service Provider (MSSP), financial services, cryptocurrency, entertainment, and transportation sectors.

Threat Actor Motivations

The motives of Scattered Spider can be evaluated by observing the strategies they apply within the context of their campaigns. Due to their target set, as well as the list of intrusion methods attributed to the group, it is highly likely Scattered Spider operations are motivated on the basis of financial gain.

Activity Timeline

June – December 2022: Scattered Spider targeted telecommunications and BPO companies to gain access to mobile carrier networks and perform SIM swapping.

January 2023: Scattered Spider initiated a BYOVD attack campaign against various targets to exploit a high-severity vulnerability (CVE-2015-2291) in the Intel Ethernet diagnostics driver.

January 2023: Scattered Spider deploys phishing web pages to expand their target scope to include technology sector organisations .

May 2023: Scattered Spider expand their attack vector arsenal by abusing the Microsoft Azure Serial Console on virtual machines (VMs) to install third-party remote management tools within target environments .

Associated Malware

BURNTCIGAR: Scattered Spider utilise this malware loader to disable endpoint detection tools and to exploit vulnerabilities in security systems to terminate defence services.

Cuba Ransomware (COLDDRAW): A ransomware variant that is delivered via malspam campaigns or the Hancitor loader.

POORTRY: A Windows kernel driver that terminates security software and deletes files as a component of BYOVD attacks. It is often used in conjunction with a userland component called STONESTOP, which installs the POORTRY driver and instructs it on what actions to perform. The first signed POORTRY drivers were observed in June 2022, whereby Scattered Spider were attributed to the creation of the respective toolkits.

STONESTOP: Scattered Spider utilise this tool to install and command operations of the POORTRY Windows kernel driver.

Indicators of Compromise

Scattered Spider Associated File Hashes (SHA-256):

- 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):

- b2f955b3e6107f831ebe67997f8586d4fe9f3e98
- 91568d7a82cc7677f6b13f11bea5c40cf12d281b
- 994e3f5dd082f5d82f9cc84108a60d359910ba79
- 0bec69c1b22603e9a385495fbe94700ac36b28e5
- 17bd8fda268cbb009508c014b7c0ff9d8284f850
- 5ed22c0033aed380aa154e672e8db3a2d4c195c4

- 78cd4dfb251b21b53592322570cc32c6678aa468
- c2387833f4d2fbb1b54c8f8ec8b5b34f1e8e2d91
- cb25a5125fb353496b59b910263209f273f3552d

Scattered Spider Associated IP Addresses:

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

Mitre Methodologies

Reconnaissance
T1589.001 – Gather Victim Identity Information: Credentials

Resource Development
T1584.001 – Compromise Infrastructure: Domains
T1586 – Compromise Accounts
T1587.002 – Develop Capabilities: Code Signing Certificates

Initial Access
T1566 – Phishing
T1078.003 – Valid Accounts: Local Accounts
T1078.004 – Valid Accounts: Cloud Accounts
T1189 – Drive-by Compromise
T1190 – Exploit Public-Facing Application

Execution
T1047 – Windows Management Instrumentation
T1059.001 – Command and Scripting Interpreter: PowerShell

Persistence
T1078 – Valid Accounts
T1547.006 – Boot or Logon Autostart Execution: Kernel Modules and Extensions
T1078.003 – Valid Accounts: Local Accounts
T1078.004 – Valid Accounts: Cloud Accounts

Privilege Escalation
T1068 – Exploitation for Privilege Escalation
T1078 – Valid Accounts

T1547.006 – Boot or Logon Autostart Execution: Kernel Modules and Extensions
T1078.003 – Valid Accounts: Local Accounts
T1078.004 – Valid Accounts: Cloud Accounts

Defense Evasion
T1078 – Valid Accounts
T1562.001 – Impair Defenses: Disable or Modify Tools
T1078.003 – Valid Accounts: Local Accounts
T1078.004 – Valid Accounts: Cloud Accounts
T1553.002 – Subvert Trust Controls: Code Signing
T1578 – Modify Cloud Compute Infrastructure

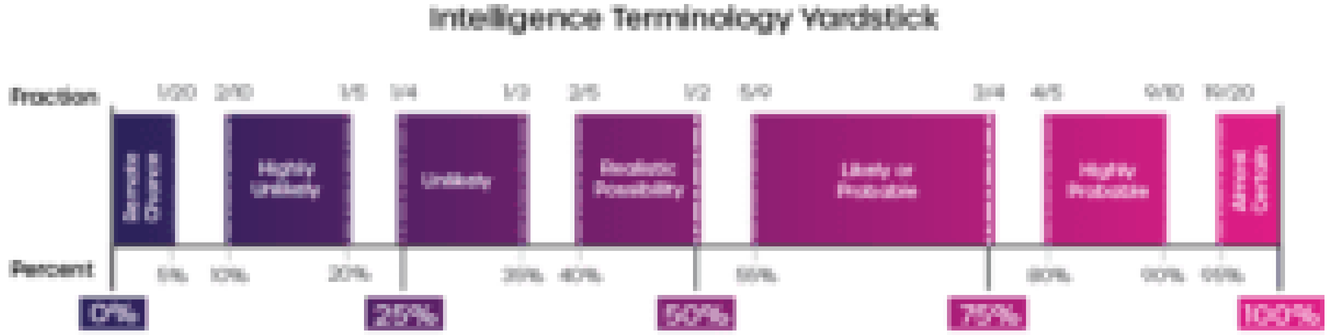
Credential Access
T1111 – Multi-Factor Authentication Interception
T1621 – Multi-Factor Authentication Request Generation

Lateral Movement
T1021 – Remote Services

Command and Control
T1219 – Remote Access Software
T1572 – Protocol Tunneling

Impact
T1486 – Data Encrypted for Impact
T1499 – Endpoint Denial of Service

Additional information


Intelligence Terminology Yardstick

This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events

-
-
-

Powered by GDPR Cookie Compliance

Privacy Overview

This website uses cookies so that we can provide you with the best user experience possible. Cookie information is stored in your browser and performs functions such as recognising you when you return to our website and helping our team to understand which sections of the website you find most interesting and useful.