

# Fayow Threat Intelligence Report: Scattered Spider

*Josh Kelley* – May 5, 2024

## Executive Summary

SCATTERED SPIDER, a notorious cybercrime group, is distinguished by its sophisticated social engineering campaigns and diverse tactics targeting firms in customer relationship management, business process outsourcing, telecommunications, and technology sectors. Their hallmark is the use of a broad spectrum of Indicators of Compromise (IOCs) and techniques, including SMS phishing, voice phishing (vishing), and exploitation of multi-factor authentication through notification fatigue. Additionally, they have shown capabilities in SIM swapping and deploying ransomware, notably using ALPHV ransomware since April 2023. Their operations extend to harvesting user data for resale and engaging in extortion by threatening to release or sell stolen proprietary information, as evidenced in their January 2023 attack on a technology firm. Due to their novel approach to social engineering, and proven technical ability, Scattered Spider poses a distinct threat to Faywow.

## Assessment

Scattered Spider, also known as Roasted 0ktapus, Scatter Swine, UNC3944, Storm-0875, LUCR-3, Octo Tempest, is a financially motivated threat group active since at least May 2022, specializing in cybercrime targeting customer relationship management, business process outsourcing, telecommunications, and many other sectors. The group typically gains initial network access using credentials stolen via SMS phishing operations and advanced social engineering campaigns via voice phishing (Vishing). They often aim to access credentials or systems for SIM-swapping attacks, supporting secondary criminal activities outside the victim's environment.

This group is adept in deploying various tactics, techniques, and procedures (TTPs), utilizing built-in tools and commands (LOLBINs), legitimate remote access software, and different commonly available malware. Scattered Spider occasionally engages in more direct forms of social engineering, including interactive operations, making threats against individuals, and attempting to bribe individuals for system access.

Scattered Spider employs phishing to obtain login details for platforms such as Okta, Microsoft Office 365/Azure, VPNs, and edge devices. They also use voice phishing (vishing) to trick users into revealing one-time password (OTP) codes and exploit multi-factor authentication (MFA) through notification fatigue. The group is also suspected of using SIM swapping to circumvent MFA.

Scattered Spider's strategy involves breaching companies to subsequently attack their third-party clients, with a strong focus on the telecommunications and cryptocurrency sectors. They have also harvested user account data for resale. In a notable incident in January 2023, they allegedly stole proprietary source code from a technology firm and demanded a ransom to prevent its release or sale.

Furthermore, Scattered Spider engages in extortion, demanding payments from victims and deploying ransomware to monetize their access. Since April 2023, they have used Alpha Spider's BlackCat ransomware to encrypt data within compromised networks. Scattered Spider is identified as part of a larger, loosely affiliated group known publicly as "The Comm."

## MITRE ATT&CK Table (based on v12)

|  |  |  |  |
| --- | --- | --- | --- |
| Tactics | Techniques | Sub Technique | D3FEND |
| TA0043 | T1589 |  | https://d3fend.mitre.org/offensive-technique/attack/T1589/ |
| TA0043 | T1598 |  | https://d3fend.mitre.org/offensive-technique/attack/T1598/ |
| TA0042 | T1583 | T1583.001 | https://d3fend.mitre.org/offensive-technique/attack/T1583.001/ |
| TA0042 | T1585 | T1585.001 | https://d3fend.mitre.org/offensive-technique/attack/T1585.001/ |
| TA0001 | T1566 |  | https://d3fend.mitre.org/offensive-technique/attack/T1566/ |
| TA0001 | T1660 |  | https://attack.mitre.org/versions/v14/techniques/T1660/ |
| TA0001 | T1566 | T1566.004 | https://d3fend.mitre.org/offensive-technique/attack/T1566/ |
| TA0001 | T1199 |  | https://d3fend.mitre.org/offensive-technique/attack/T1199/ |
| TA0001 | T1078 | T1078.002 | https://d3fend.mitre.org/offensive-technique/attack/T1078.002/ |
| TA0002 | T1648 |  | https://d3fend.mitre.org/offensive-technique/attack/T1648/ |
| TA0002 | T1204 |  | https://d3fend.mitre.org/offensive-technique/attack/T1204/ |
| TA0003 |  |  | https://attack.mitre.org/versions/v14/tactics/TA0003/ |
| TA0003 | T1136 |  | https://d3fend.mitre.org/offensive-technique/attack/T1136/ |
| TA0003 | T1556 | T1556.006 | https://d3fend.mitre.org/offensive-technique/attack/T1556.006/ |
| TA0003 | T1078 |  | https://d3fend.mitre.org/offensive-technique/attack/T1078/ |
| TA0004 |  |  | https://attack.mitre.org/versions/v14/tactics/TA0004/ |
| TA0004 | T1484 | T1484.002 | https://d3fend.mitre.org/offensive-technique/attack/T1484.002/ |
| TA0005 | T1578 | T1578.002 | https://d3fend.mitre.org/offensive-technique/attack/T1578.002/ |
| TA0005 | TA1656 |  | https://attack.mitre.org/versions/v14/techniques/T1656/ |
| TA0006 |  |  | https://attack.mitre.org/versions/v14/tactics/TA0006/ |
| TA0006 | T1606 |  | https://d3fend.mitre.org/offensive-technique/attack/T1606/ |
| TA0006 | T1621 |  | https://d3fend.mitre.org/offensive-technique/attack/T1621/ |
| TA0006 | T1552 | T1552.001 | https://d3fend.mitre.org/offensive-technique/attack/T1552.001/ |
| TA0006 | T1552 | T1552.004 | https://d3fend.mitre.org/offensive-technique/attack/T1552.004/ |
| TA0007 |  |  | https://attack.mitre.org/versions/v14/tactics/TA0007/ |
| TA0007 | T1217 |  | https://d3fend.mitre.org/offensive-technique/attack/T1217/ |
| TA0007 | T1538 |  | https://d3fend.mitre.org/offensive-technique/attack/T1538/ |
| TA0007 | T1083 |  | https://d3fend.mitre.org/offensive-technique/attack/T1083/ |
| TA0007 | T1018 |  | https://d3fend.mitre.org/offensive-technique/attack/T1018/ |
| TA0007 | T1539 |  | https://attack.mitre.org/versions/v14/techniques/T1539/ |
| TA0008 |  |  | https://attack.mitre.org/versions/v14/tactics/TA0008/ |
| TA0008 | T1021 | T1021.007 | https://d3fend.mitre.org/offensive-technique/attack/T1021/ |
| TA0009 | T1213 | T1213.003 | https://d3fend.mitre.org/offensive-technique/attack/T1213.003/ |
| TA0009 | T1213 | T1213.002 | https://d3fend.mitre.org/offensive-technique/attack/T1213.002/ |
| TA0009 | T1074 |  | https://d3fend.mitre.org/offensive-technique/attack/T1074/ |
| TA0009 | T1114 |  | https://d3fend.mitre.org/offensive-technique/attack/T1114/ |
| TA0009 | T1530 |  | https://d3fend.mitre.org/offensive-technique/attack/T1530/ |
| TA0011 | T1219 |  | https://d3fend.mitre.org/offensive-technique/attack/T1219/ |
| TA0010 |  |  | https://attack.mitre.org/versions/v14/tactics/TA0010/ |
| TA0040 | T1486 |  | https://d3fend.mitre.org/offensive-technique/attack/T1486/ |
| TA0040 | T1567 | T1567.002 | https://attack.mitre.org/versions/v14/techniques/T1567/002/ |
| TA0040 | T1657 |  | https://attack.mitre.org/versions/v14/techniques/T1657/ |

## Victims

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Date Reported | Sector | City/State/Province/etc. | Country/Region | |
| Twilio | 2022-08-10 | NAICS 517 | San Francisco, CA | | USA |
| MGM Resorts International | 2023-09-10 | NAICS 71 | Las Vegas, NV | | USA |
| Caesars Entertainment | 2023-09-14 | NAICS 71 | Las Vegas, NV | | USA |

## Indicators of Compromise (IOC)

## Malware

|  |  |
| --- | --- |
| Malicious Tool Name | Brief Description |
| AveMaria (also known as WarZone [S0670]) | Enables remote access to a victim’s systems. Offline information stealer and remote access trojan (RAT). dd-mm-yy\_hh.mm.ss |
| Raccoon Stealer | Steals information including login credentials [TA0006], browser history [T1217], cookies [T1539], and other data. |
| VIDAR Stealer | Steals information including login credentials, browser history, cookies, and other data. |
| BlackCat | Rust based ransomware capable of encrypting Windows, Linux, ESXi, and more. |

## Legitimate Tools

|  |  |  |
| --- | --- | --- |
| Name | Intended Use | Tactic |
| Fleetdeck.io | **Remote Management and Monitoring** | **T1219** |
| Level.io | **Remote Management and Monitoring** | **T1219** |
| Pulseway | **Remote Management and Monitoring** | **T1219** |
| Screenconnect | **Remote Management and Monitoring** | **T1219** |
| Splashtop | **Remote Management and Monitoring** | **T1219** |
| Tactical.RMM | **Remote Management and Monitoring** | **T1219** |
| Tailscale | **VPN** |  |
| AnyDesk | **Remote Management and Monitoring** | **T1219** |
| TeamViewer | **Remote Management and Monitoring** | **T1219** |
| RustDesk | **Remote Management and Monitoring** | **T1219** |

## Hacking Tools

|  |  |  |
| --- | --- | --- |
| Name | Intended Use | Tactic |
| Impacket | **Python tool collection** | **S0357** |
| Mimikatz | **Credential dumping** | **S0002** |
| LaZagne | **Post-exploitation toolset** | **S0349** |
| Ngrok | **Reverse proxy tool** | **S0580** |

## Network

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Network Artifact | Details | Intrusion Phase |
| Domain | {}-sso.[com|net] | Lookalike domain schema | TA0001 |
| Domain | sso-{}.[com|net] | Lookalike domain schema | TA0001 |
| Domain | {}sso.com.[com|net] | Lookalike domain schema | TA0001 |
| Domain | {}-help.com | Lookalike domain schema | TA0001 |
| Domain | {}-helpdesk.com | Lookalike domain schema | TA0001 |
| Domain | {}-servicedesk.com | Lookalike domain schema | TA0001 |
| Domain | {}-servicenow.[com|net] | Lookalike domain schema | TA0001 |
| Domain | servicenow-{}.com | Lookalike domain schema | TA0001 |
| Domain | {}-internal.com | Lookalike domain schema | TA0001 |
| Domain | {}-schedule.[ca|com] | Lookalike domain schema | TA0001 |
| Domain | {}-okta.[com|net] | Lookalike domain schema | TA0001 |

## Common Vulnerabilities and Exposures (CVEs)

|  |  |  |  |
| --- | --- | --- | --- |
| CVE # | CVSS | Patch Available | NVD Publish Date |
| CVE-2015-2291 | 7.8 | Yes | 2017-08-09 |
| CVE-2021-3156 | 7.8 | Yes | 2021-01-26 |
| CVE-2022-21894 | 4.4 | Yes | 2022-01-11 |

### Data Sources:

* CISA Cybersecurity Advisory: Scattered Spider https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
* Mandiant Threat Intelligence: Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety https://cloud.google.com/blog/topics/threat-intelligence/unc3944-sms-phishing-sim-swapping-ransomware
* CISA Cybersecurity Advisory: #StopRansomware: ALPHV Blackcat https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
* MITRE [G1015]: https://attack.mitre.org/groups/G1015/
* Scattered Spider: The Modus Operandi https://www.trellix.com/blogs/research/scattered-spider-the-modus-operandi/

### Reporting Tool:

* CTI-Blueprints https://github.com/center-for-threat-informed-defense/cti-blueprints/releases