OmegaBlack

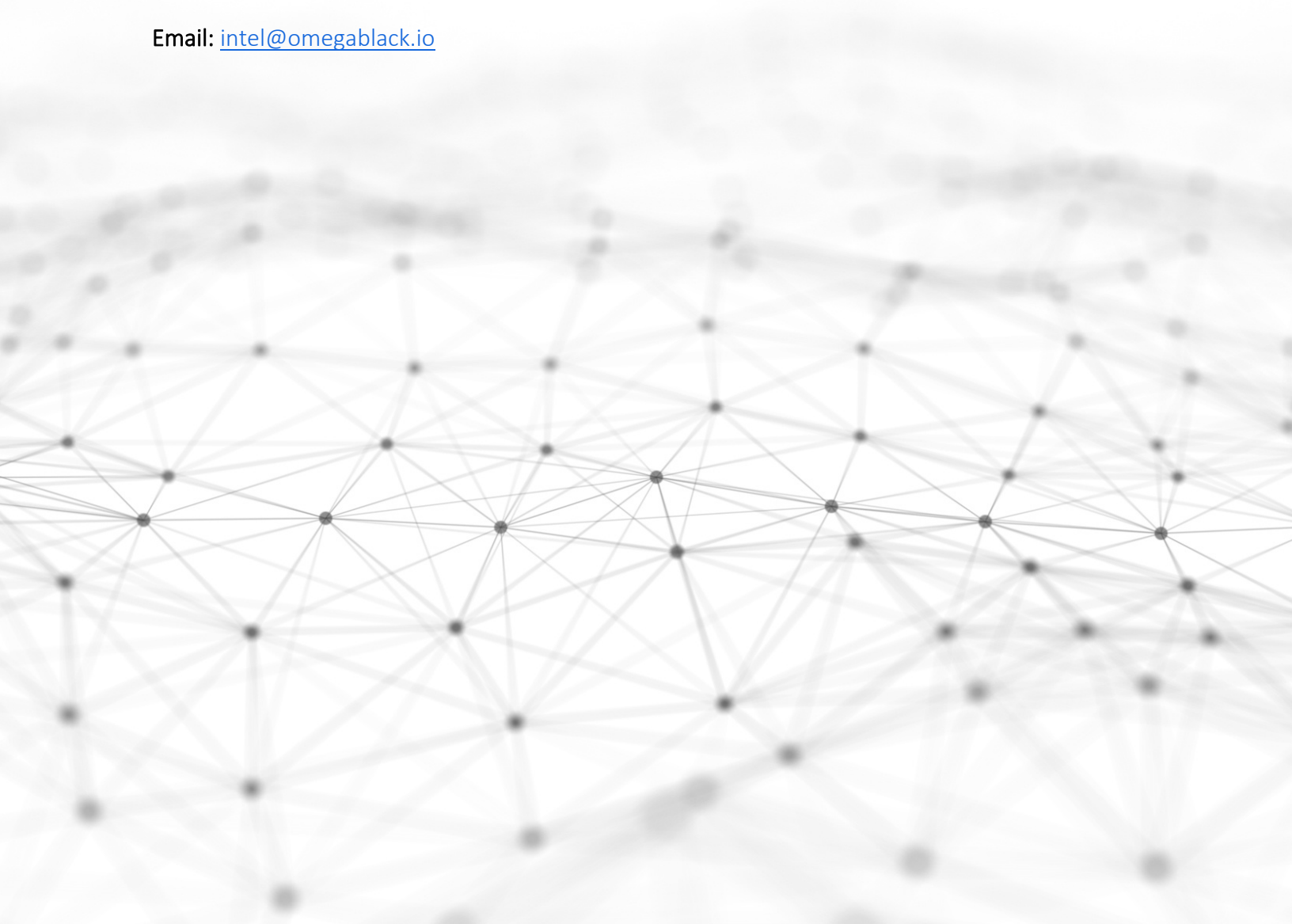
# Threat Actor Report – ScatteredSpider(UNC3944)

**Date:** 06/18/2025

**Prepared by:** Omega Threat Intelligence

**Prepared for:** Core Specialty

**Email:** intel@omegablack.io



**Original:** 06/18/2025

# TABLE OF CONTENTS

# THREAT ACTOR PROFILE – SCATTEREDSPIDER(UNC3944)

## 1 OVERVIEW

Scattered Spider is an English-Speaking cybercrimial group that has been active since at least 2022. known for its sophisticated social engineering tactics, the group primarily targets large enterprises across North America, especially within the telecommunications, technology, finance, and healthcare sectors. Scattered Spider is tracked under various identifiers including UNC3944, Muddled Libra, and Scatter Swine, and has been associated with the deployment of ransomware as part of affiliate operations with the ALPHV/BlackCat group.

## 2 CRITICAL FINDINGS

- **Smishing and Social Engineering Entry Point**: Scattered Spider frequently initiates attacks through SMS-based phishing (smishing), often impersonating internal IT personnel or identity management services. Messages trick victims into visiting credential-harvesting portals or calling fraudulent helpdesks. This human-centric vector bypasses traditional email security solutions and relies heavily on exploiting trust and urgency.
- **Helpdesk Impersonation and MFA Fatigue**: The group impersonates legitimate helpdesk or IT support staff to convince users to approve MFA push notifications. In some cases, they directly call targets or use pretexting to reset credentials via internal support. This “push fatigue” technique exploits user behavior and support workflows rather than technical vulnerabilities.
- **SIM Swapping and Phone Number Hijacking**: Scattered Spider has successfully executed SIM swap attacks to take control of victims’ phone numbers. This enables them to intercept MFA codes or password reset messages, gaining access to sensitive enterprise accounts even when MFA is enabled.
- **Abuse of Identity Platforms**: Once initial access is obtained, attackers exploit identity platforms such as Okta, Microsoft Entra ID (formerly Azure AD), and VPN services to escalate privileges and maintain access. They have been observed generating session tokens and impersonating users by hijacking legitimate sessions through stolen cookies or SSO bypass techniques.
- **Use of Legitimate Remote Access Tools**: Scattered Spider leverages trusted remote management and remote desktop tools, such as AnyDesk, TeamViewer, and ScreenConnect, to establish persistent, hands-on-keyboard access. These tools are often whitelisted in enterprise environments and allow attackers to blend into normal IT activity.
- **Cloud and SaaS Exploitation**: The group actively targets cloud-based admin portals and SaaS environments. They use legitimate admin functionality within these platforms (e.g., user provisioning, access role changes) to deepen control over the environment, often going undetected by standard endpoint monitoring.
- **Multi-Stage Reconnaissance and Exfiltration**: Post-compromise activity includes lateral movement, enumeration of cloud assets, and exfiltration of sensitive data. File transfer utilities such as Rclone and WinSCP are used to move large volumes of data to attacker-controlled

infrastructure. These tools are typically benign and evade common DLP and malware detection mechanisms.

- **Coordination with Ransomware Operators**: Scattered Spider has been linked to data extortion campaigns in coordination with ALPHV/BlackCat ransomware. In some incidents, they gain access and exfiltrate data, while BlackCat handles encryption and ransom negotiations. This division of labor suggests affiliate-based cooperation within a broader cybercrime ecosystem.
- **Frequent Infrastructure Rotation and OPSEC**: The threat actor demonstrates strong operational security. Domains used in smishing and phishing campaigns are often short-lived and registered with privacy protection. VPNs, residential proxy services, and encrypted communication channels obscure the source of attacks, making attribution and tracking more difficult.
- **Persistent Threat to High-Value Sectors**: Scattered Spider prioritizes industries with access to valuable personal or financial data. Their targets often include telecommunications firms, managed service providers (MSPs), and cloud-first enterprises, especially those with decentralized IT helpdesk procedures and high employee counts. CISA and partner agencies have warned that the group's continued targeting of these sectors represents an elevated and persistent threat.

# 3 OMEGA ASSESSMENT

## 3.1 INFRASTRUCTURE TRADECRAFT

Scattered Spider (UNC3944) demonstrates an exceptionally agile and deceptive infrastructure strategy that supports its broader social engineering operations. Unlike malware-centric threat actors, this group prioritizes infrastructure that facilitates identity deception, MFA manipulation, and short-lived credential phishing. Their domain choices and hosting behaviors reveal a highly tailored, iterative approach to targeting and evasion.

**Keyword Analysis of Domain Infrastructure**

Analysis of confirmed Scattered Spider campaigns reveals consistent use of key terms within attacker-registered domains. These terms are chosen to simulate internal IT resources and trusted access platforms. High-frequency keywords include:

> "internal," "connect," "duo," "vpn," "helpdesk," "servicenow," "corp," "schedule," "okta," "servicedesk," "rsa," "info," "support," "mfa," "sso," "help," and "service."

These keywords are typically embedded into attacker-controlled infrastructure via:

- Hyphenated impersonation domains, e.g. sso-company[.]com
- Subdomain lookalikes, e.g. sso.c0mpany[.]com
- Typo squatted combinations, e.g. c0mpanysso[.]com

These domains are leveraged in smishing and vishing campaigns where victims are socially engineered into interacting with credential harvesting portals. The infrastructure closely mimics enterprise SSO or helpdesk services, facilitating high-success phishing operations that bypass email-based filtering controls.

## 3.2 INFRASTRUCTURE HOSTING TRENDS

**Preferred Autonomous System Numbers (ASNs)**

Hosting for malicious infrastructure has been observed across the following ASNs, which appear repeatedly across different campaigns:

- AS39287 (ABSTRACT, FI)
- AS13335 (Cloudflare, Inc)
- AS399486 (VIRTUO, CA)
- AS14061 (DIGITALOCEAN-ASN, US)
- AS20473 (AS-CHOOPA, US)

**Registrar Preferences**

Domain registrations are frequently traced to a handful of recurring registrars, indicating either convenience or specific features leveraged by the threat actor:

- NiceNIC
- Hosting Concepts B.V.
- NameSilo, LLC
- GoDaddy

These platforms offer easy onboarding, privacy protection, and (in some cases) fast provisioning of new domains, which aligns with the group's use of short-lived infrastructure.

## 3.3 OPERATIONAL TEMPO AND DETECTION CHALLENGES

Scattered Spider frequently rotates infrastructure, with domains often active for less than seven days. This operational tempo underscores the group's use of agile campaigns and disposable infrastructure to avoid blacklisting and detection.

To maintain visibility into these campaigns, defenders should implement structured and automated hunting methodologies. While traditional IOCs such as IPs and hashes remain relevant, Scattered Spider's heavy reliance on rapid domain generation and impersonation tactics requires defenders to pivot toward behavioral patterns, keyword matching, and short-window detection logic. Defenders who rely solely on passive detection or threat feeds may miss the infrastructure before it disappears.

# 4 RECOMMENDATIONS

This section outlines specific mitigation strategies for defending against Scattered Spider (UNC3944) campaigns, with a focus on social engineering entry points, identity platform abuse, remote access software exploitation, and cloud-based persistence and exfiltration.

1. **Restrict Use of Remote Access and RMM Tools**
   - Audit all systems for unauthorized installations of AnyDesk, TeamViewer, ScreenConnect, and other RMM software.
   - Remove unused or unapproved remote access tools from all endpoints.
   - Enforce application allowlisting to prevent execution of unauthorized RMM binaries.
   - Monitor EDR and SIEM logs for unexpected launches of remote access applications and lateral movement behavior.
2. **Enhance MFA Protections and Identity Security**
   - Transition from push-based MFA to phishing-resistant methods such as FIDO2 security keys or hardware tokens.
   - Detect and alert on MFA fatigue scenarios, including multiple push requests in a short time.
   - Monitor for suspicious session persistence, such as unusual refresh token behavior or unexpected Okta/Microsoft Entra ID session creations.
   - Regularly audit administrative accounts and limit persistent elevated privileges.
3. **Harden Helpdesk and User Verification Workflows**
   - Implement out-of-band verification procedures for all password resets and MFA changes initiated through helpdesk channels.
   - Train helpdesk staff to recognize social engineering tactics, including impersonation of employees and executives.
   - Require positive user verification through pre-established internal channels for sensitive account actions.
4. **Prevent Data Exfiltration Through Known Tactics**
   - Block outbound SFTP traffic (TCP port 22) except where explicitly required and approved.
   - Monitor for the use of data transfer tools such as Rclone, WinSCP, and transfer.sh across endpoints.
   - Inspect DNS and firewall logs for communication with known exfiltration domains and infrastructure (e.g., 144.76.136.153, 2a01:4f8:200:1097::2).
   - Implement Data Loss Prevention (DLP) controls on critical servers and cloud storage services.
5. **Monitor for Known Adversary Infrastructure and Artifacts**
   - Block or alert on communications to known Scattered Spider IP addresses listed in Appendix I.
   - Use IOC feeds to detect and alert on SHA256 hashes such as acadf15ec363fe3cc373091cbe879e64f935139363a8e8df18fd9e59317cc918 (insomnia.exe) and cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005 (IIatZ malware).

- Inspect logs for use of the password string change.m31!!! as an indicator of compromise.

6. **Secure Cloud and SaaS Administrative Interfaces**
   - Enable logging and alerting on anomalous behavior within identity providers (e.g., unexpected user creation, MFA method changes, login anomalies).
   - Apply least privilege principles to cloud admin roles and require just-in-time elevation for high-risk operations.
   - Monitor access to sensitive SaaS portals, especially from untrusted IP ranges or unexpected geographies.

# APPENDICES

## APPENDIX I – INDICATORS OF COMPROMISE

### 4.1 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 |

| IPV4 | Description |
|---|---|
| 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 |
| 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 |

| IPV4 | Description |
|---|---|
| 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 |
| 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 |
| 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 |

| IPV4 | Description |
|---|---|
| 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 |
| 45.32.221.250 | 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 |

## 4.2 IPV6

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

## 4.3 CIDR

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

## 4.4 SHA256

| SHA256 | File Name | Description |
|---|---|---|
| N/A | change.m31!!! | Password used by adversary extensively |
| 3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08 | <redacted>.exe | Packed Fleet Deck binary |
| cce5e2ccb9836e780c6aa075ef8c0aeb8fec61f21bbef9e01bdee025d2892005 | IIatZ | 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 |

| SHA256 | File Name | Description |
| --- | --- | --- |
| | | 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 |