Threat Intelligence Report: Scattered Spider Analysis

Table of Contents

Project Overview

Project: Advanced Threat Actor Profiling
Analyst: Nyerovwo Obarueroro
Date: November 18, 2025
Threat Level: High

Executive Summary

Scattered Spider represents one of the most sophisticated cybercriminal threats targeting enterprises today. This English-speaking group, composed mainly of individuals aged 16-25, has evolved from basic credential theft to executing high-impact ransomware attacks across multiple sectors including hospitality, retail, telecommunications, and critical infrastructure.

Their unique ability to bypass multi-factor authentication through advanced social engineering makes them a "post-MFA" threat actor that requires immediate defensive attention.

Threat Actor Profile

Attribute	Details
Primary Aliases	UNC3944, Muddled Libra, Octo Tempest, StarFraud, Scatter Swin
Type	Financially motivated cybercriminal group / Ransomware affiliate
Motivation	Financial gain through ransomware operations and data extortion
Target Sectors	Hospitality, Entertainment, Retail, Telecommunications, Technology, Financial Services, MSPs
Operational Focus	Social engineering, identity system compromise, initial access brokerage

Attribute	Details
Associated Groups	ALPHV/BlackCat, Qilin, DragonForce

Indicators of Compromise

IP Addresses

```
185.208.156.251
84.200.205.9
137.220.43.146
149.248.8.85
149.28.41.193
146.45.77.214
143.198.116.59
2a01:4f8:200:1097::2
```

Malicious Domains

Phishing/Impersonation Domains:

```
complete-sendgrid[.]com
aws-us3-manageprod[.]com
internal-ssologin[.]com
targetsname-sso[.]com
oktalogin-targetcompany[.]com
grid-sso[.]com
login-enterprisesso[.]com
```

File Hashes

MD5:

```
1155560e1e4ea8fcce047514a52950859
192644d5f4fc2313bca0224210c0b6c7
52746d457f8ec149fd13dea85b654b19
```

SHA1:

```
0272b018518fef86767b01a73213716708acbb80
10b9da621a7f38a02fea2625660364d600df85
```

SHA256:

```
3ea2d190879c8933363b222c686009b81ba8af9eb6ae3696d2f420e187467f08
4188736108d2b73b57f63c0b327fb5119f82e94ff2d6cd51e9ad92093023ec93
443dc750c35afc136bfea6db9b5ccbdb6adb63d3585533c0cf55271eddf29f58
```

Exploited Vulnerabilities

- CVE-2021-35464
- CVE-2023-35199
- CVE-2024-3400
- CVE-2021-21551
- CVE-2022-38028

MITRE ATT&CK Mapping

Tactic	Technique ID	Description
Reconnaissance	T1589.001	Gather Victim Identity Information
Initial Access	T1660	Social Engineering via SMS phishing
Credential Access	T1621	Multi-Factor Authentication Request Generation
Credential Access	T1555.005	Credentials from Password Stores
Lateral Movement	T1021.001	Remote Desktop Protocol
Persistence	T1087	Cloud Accounts
Impact	T1486	Data Encrypted for Impact

MISP Implementation

Steps Performed:

- ☑ Created dedicated Scattered Spider event in MISP
- ☑ Imported IOCs via Freetext Import (IPs, domains, hashes, CVEs)
- ☑ Applied taxonomy tags: `OSINT:Scattered-Spider`
- ☑ Mapped TTPs to MITRE ATT&CK framework
- ☑ Published event for correlation and analysis
- ☑ Verified all attributes using OSINT and Malware Patrol reports

Detection Recommendations

1. Identity & Access Controls

- Enforce phishing-resistant MFA across all accounts
- Monitor for suspicious authentication patterns
- Alert on MFA reset/enrollment modifications
- Implement strict verification for helpdesk password resets

2. Endpoint Security

- Restrict RMM tools (AnyDesk, TeamViewer, Splashtop, RDP)
- Monitor for unusual remote management tool usage
- Implement application allowlisting and least privilege

3. Network Monitoring

- Block known malicious IPs and domains at firewall/DNS level
- Monitor for data exfiltration patterns
- Implement SSL inspection for threat detection

4. Cloud Security

- Monitor SaaS configuration changes and suspicious API calls
- Alert on privilege escalations in cloud environments
- Restrict legacy authentication protocols
- Enforce conditional access policies

5. User Awareness

- Train staff to recognize MFA fatigue attacks
- Conduct social engineering simulations
- Reinforce verification procedures for identity validation

SOC Alerting Strategy

```
High Priority Alerts:
  - Multiple MFA push notifications in short timeframe
  - RDP connections from unknown IP ranges
  - Suspicious cloud tenant configuration changes
  - Data transfers to known malicious IPs
  - Helpdesk password reset requests without proper verification

Medium Priority Alerts:
  - New device registrations in identity providers
  - Unusual remote management tool usage
  - Access to sensitive data stores from new locations
  - Failed MFA attempts followed by successful authentication

Low Priority Alerts:
  - Geographic impossible travel scenarios
  - After-hours access from unusual locations
  - Multiple account lockouts in short period
```

Incident Response Playbooks

- Identity Compromise Response
- Ransomware Containment Procedures

- Data Exfiltration Response
- Cloud Account Takeover Recovery

Conclusion

Scattered Spider represents a persistent and adaptive threat in the cybersecurity landscape. Their demonstrated ability to consistently bypass multi-factor authentication and execute sophisticated social engineering attacks positions them as a highly dangerous, "post-MFA" adversary.

The group's evolution from credential theft to high-impact ransomware operations against critical sectors underscores their increasing operational maturity and financial motivation. Defending against this advanced threat requires a proactive and layered security approach that assumes determined adversaries will breach standard controls.

The recommendations outlined in this report—focusing on hardened identity systems, comprehensive monitoring, and robust incident response—provide a critical framework for mitigation. Ultimately, maintaining resilience against Scattered Spider demands continuous vigilance, regular updates to defensive measures, and an intelligence-driven security posture that evolves as rapidly as the threat itself.

References

- MITRE ATT&CK Framework
- MISP Threat Intelligence Platform
- OSINT Security Feeds
- Malware Patrol Reporting
- Trustwave SpiderLabs Analysis
- CISA Known Exploited Vulnerabilities Catalog