Analysis & Resilience Center
FOR SYSTEMIC RISK

FS-ISAC

Scattered Spider & BlackCat Ransomware: Mitigation Guidance

November 2023

Scattered Spider & BlackCat Ransomware: Mitigation Guidance

November 2023

Contents

Scattered Spider & BlackCat Ransomware: Mitigation Guidance

November 2023

Overview

Scattered Spider (aka UNC3944, Roasted 0ktapus, Scatter Swine) is a prolific financially-motivated cybercriminal group specializing in the use of social engineering tactics to obtain credentials to steal sensitive data for extortion. The threat actor initially gained notoriety by obtaining Okta identity credentials and multifactor authentication (MFA) codes to conduct supply chain attacks against Okta's clients. Scattered Spider's capabilities have increased over time to include bring-your-own-vulnerable-driver (BYOVD) attacks and to evade endpoint detection and response products. Scattered Spider recently conducted attacks against MGM Casino and Caesars Entertainment to drop ALPHV/BlackCat ransomware.

The group maintains a high-operational tempo and primarily attacks firms who specialize in customer relationship management, business process outsourcing, telecommunications, and technology sector entities but have been increasingly observed targeting global financial institutions. They frequently use SMS phishing campaigns and call help desks to obtain password resets and MFA bypass codes. Researchers note Scattered Spider has demonstrated a strong focus on stealing large amounts of sensitive data to extort their victims. For more on Scattered Spider tools, techniques, and procedures (TTPs) see the FBI and CISA's Joint Advisory on Scattered Spider.

Scattered Spider Social Engineering Techniques

Scattered Spider's methods used to obtain credentials include phishing, smishing, domain name look-alikes, push bombing, and subscriber identity module (SIM) swap attacks. Their goals are to obtain credentials, install remote access tools, and/or bypass multi-factor authentication (MFA).

The group is adaptive and will seek out any system or human vulnerability susceptible to their toolkit. In their social engineering campaigns, the group commonly poses as company IT/helpdesk staff to obtain employee credentials, deploy remote access tools, or obtain employee one-time passwords via multi-factor authentication.

See the Appendix for detailed descriptions of their techniques and mitigations using the MITRE ATT&CK framework.

Scattered Spider & BlackCat Ransomware: Mitigation Guidance

November 2023

Strategies to Deter Scattered Spider Exploits

Global financial institutions have implemented specific mitigation and control measures in response to Scattered Spider activities. This paper describes baseline detection, prevention, and cyber hygiene actions necessary to defend against this threat. Using these techniques will help prevent social engineering exploitation.

Detection and Suppression

- Establish detection for cloned login portals. Disable website login mechanism if adversary-in-the-middle conditions used by Phishing- as-a-Service are detected via client-side checks.
- Engage or build a "brand protection" service that monitors in real-time for domain registrations impersonating your brand. The service must detect and alert for domains that embed your or your partners' brand name and/or proprietary images or logos (or look-alikes) in a newly registered domain, and domains that match patterns used by known adversaries.
- Use threat intelligence to conduct passive DNS and public web certificate records for pivoting on known brand abuse domains and infrastructure. Threat actors may use a phishing kit to create several sites at a time all linked to the same IP, hosting provider, and certificate authority.
- Ensure detection is in place for large amounts of data or confidential/ proprietary data attempting to leave the environment through data-loss prevention tooling.
- Partner with mobile network operators (MNOs or telecom carriers) to detect when SMS messages are using your brand that do not come from your company's known messaging services. Some MNOs may also be able to provide brand abuse feeds.
- Work with technology companies to report malicious advertisements or SEO poisoning on search engines.
- Educate IT Help desk, Operations Help Desks, Customer Support staff (any function with the ability to initiate a password or credential change) about the social engineering and phishing schemes used by Scattered Spider and other threat actors. Education should include but not be limited to:

  - Frequent training that uses real phish examples from current high profile threat groups such as Scattered Spider
  - Immediate reporting protocols of suspicious messages and interactions to abuse teams
- **Actively monitor your service desk.** Add questions including the request of device serial numbers. Add layers of approvals with additional questions for admin users. Launch a zoom session for contractors to have manager verify the user on video.

Network Defenses

Internet-facing/External

- **Monitor for compromised credentials and suspicious login attempts of bank employees**, including monitoring for unauthorized corporate mobile phone use.
- **Use email security platform** for detection and prevention of phishing emails and automated quarantine of suspected and confirmed phishing emails detected before delivery to the recipient.
- **Implement internet-facing vulnerability detection and alerting** program for vulnerabilities used by Scattered Spider
- **Implement web proxy and firewall blocks for any malicious infrastructure found.**

Internal

- **Implement firewall rules to prevent malware from communicating with sites** categorized as Remote Access, Uncategorized, Suspicious, Malicious & File Storage/Sharing.
- **Implement robust endpoint detection and response (EDR) tools** on all computers (including cloud) to detect privileged escalation attempts as well as lateral movements of malware.
- **Implement security hardening techniques to virtual infrastructure controls**:
  - Lockdown ESXi into lockdown/protective mode.
  - Disable secure shell to ESXi

- Limit Active Directory access to ESXi

Login Security

- Tune multi-factor authentication (MFA):
  - Do not use email-based MFA
  - Require MFA for all interactions with the help desk voice channel
  - Require and confirm MFA enrollment for BYOD equipment
  - Monitor privileged logins for unusual activity
  - Require enterprise to use FIDO/passkey MFA for external access
  - Establish email alerts users on all new registered devices for MFA as well as require manager approval through the formal access provisioning process
  - Establish MFA throttling limits
- Monitor for login anomalies including geographic and IP diversity and frequency.
- Have rules to detect and prevent users from logging in using anonymous VPN services. Leverage known anonymous VPN IP Address categorization lists or feeds

Critical Baseline Cyber Hygiene Practices to Defend Against Ransomware

Account Management

- Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with National Institute for Standards and Technology (NIST) standards for developing and managing password policies.
- Require phishing-resistant multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems such as SaaS. Monitor logins for unusual activity and consider throttling limits. Review existing accounts to ensure MFA is properly configured i.e., no email allowed. Ensure inactive accounts are deleted.
- Audit user accounts with administrative privileges and configure

access controls according to the principle of least privilege. Clean up test accounts.

- Implement time-based access for accounts set at the admin level and higher. This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- Disable any password reset utility service that is internet-facing.

Email

- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Vulnerability Management

- Keep all operating systems, software, and firmware up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.
- Block installation of non-approved software, including remote monitoring and management (RMM) software.
- Disable or restrict internet access to management interfaces such as firewalls, VPNs, virtual infrastructure, etc.

Network Access

- Segment networks to help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- Limit the execution of applications and scripts to only approved software. If threat actors are not able to run unapproved software,

they will have difficulty escalating privileges and/or moving laterally.

- Block unused network ports.
- Install asset management software on all endpoints to detect for unwanted systems software such as Remote Monitoring and Management (RMM) that may be infected. Analyze the traffic and establish a baseline of in/out and set up alerts.

Detection and Monitoring

- Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host. Use robust EDR for all environments, including cloud-based ones.
- Install, regularly update, and enable real time detection for antivirus software on all hosts.
- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts. Monitor for unusual activity on non-production servers, especially file transfer servers.

Data Protection

- Maintain offline backups of data, and regularly maintain backup and restoration. By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.
- Utilize Data Loss Prevention (DLP) tools and consider limits on the size of data files being sent externally.

Recovery

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, the cloud).

Awareness and Training

- Create policies to include cybersecurity awareness training, organizational users learn and perform more secure behaviors.

Appendix: Scattered Spider: Known Tactics, Techniques & Procedures (TTPs)

Mitre ATT&CK Techniques	Mitre ATT&CK Mitigations
Phishing for Information [T1598]	M1054 Software Configuration M1017 User Training
Impersonation [T1656]	M1019 Threat Intelligence Program M1017 User Training
User Execution [T1204]	M1040 Behavior Prevention on Endpoint M1038 Execution Prevention M1031 Network Intrusion Prevention M1021 Restrict Web-Based Content M1017 User Training
Remote Access Software [T1219]	M1038 Execution Prevention M1037 Filter Network Traffic M1031 Network Intrusion Prevention
Phishing [T1566]	M1049 Antivirus/Antimalware M1031 Network Intrusion Prevention M1021 Restrict Web-Based Content M1054 Software Configuration M1017 User Training
MFA Request Generation [T1621]	M1036 Account Use Policies M1032 Multi-factor Authentication M1017 User Training
Financial Theft [T1657]	M1018 User Account Management M1017 User Training