Scattered Spider

C-Suite level threat review by applicable business area addressing active threats.

Since our latest coverage of Scattered Spider in February of 2023, the adversarial group has been busy spinning new webs. Scattered Spider, also known as Star Fraud, UNC3944, Octo Tempest, Scattered Swine, and Muddled Libra, is an expert group of social engineers comprised of malicious actors from across the globe. Engaging in various methods of data exfiltration, Scattered Spider is part of an interconnected labyrinth of cyber criminals who have dubbed themselves "the Community" or "the Com." This medley of threat actors leverages each other's strength and intelligence, sharing services like "the latest malware and experience negotiating ransoms and laundering money" (CBS News). Such nefarious partners include infamous Russian gangs such as BlackCat who, in conjunction with Scattered Spider, claimed involvement with the September 2023 MGM Resorts International ("MGM") cyber-attack. As this group continues to act and expand, we anticipate more sophisticated attacks that are enabled by fluent western actors using foreign nation state software.

Scattered Spider

Threat Level: High

Attack:

Scattered Spider has employed a variety of attack methods throughout its existence, leveraging malware such as AveMaria, Raccoon Stealer, and VIDAR Stealer. Through means of phishing, impersonation, and inciting MFA fatigue, Scattered Spider has become a known enemy of substantial organizations and their third-party help desks. The Cybersecurity and Infrastructure Security Agency (CISA) has identified various techniques that have been employed by Scattered Spider, including but not limited to:

- MITRE T1598 and MITRE T1566 – these techniques utilize phishing methods to gain access to sensitive information. These methods include phishing, smishing, vishing, and whaling, among others.
- MITRE T1656 – adversaries leverage this technique by means of impersonation, feigning relationships with targets such as colleague, former acquaintance, or Help Desk personnel.
- MITRE T1204 – this technique, "User Execution," relies on action on the part of the user to help threat actors with such nefarious activity as the execution of malicious code.
- MITRE T1219 – threat actors use legitimate desktop support tools, such as ScreenConnect or AnyDesk, to connect and control in-network systems remotely.
- MITRE T1621 – relying on user action, adversaries may generate MFA requests in the hopes of inciting MFA fatigue, thus bypassing MFA mechanisms.

Remediation:

- Ensure all users, including contractors, are trained at a defined cadence to recognize and report suspicious behaviors.
    - Awareness activities should incorporate potential phishing techniques and other entry attempts, such as continuous and unusual MFA prompts or impersonation tactics.
- Log all remote maintenance sessions and ensure they are conducted securely to mitigate the risk of misuse.
- Safeguard MFA methods and abide by industry best practice, mitigating the chance of exploitation.

Scattered Spider

Recent Attacks

MGM Resorts International

As one of the world's largest entertainment operators, the attack on MGM proved catastrophic, with operations disrupted for nearly 10 days according to Vox. While the effects of the attack are still unfolding, MGM can expect revenue losses, customer mistrust, and other reputational hazards. Utilizing history of past Scattered Spider attacks, security research suggests the adversaries used "fraudulent phone calls to employees and help desks to "phish" for login credentials. The hackers then use these credentials to access the network or deploy their ransomware" (Inszone). Reminiscent of MITRE ATT&CK tactics T1598, T1566, and T1656, Scattered Spider has proven a pattern in their operations that organizations can leverage to help secure their environment against similar attacks.

Caesars Entertainment

Taking another swipe at a foundational Las Vegas hot spot, Scattered Spider is believed to be behind the September 2023 Caesars Entertainment group hack. The company noted, "hackers stole a huge trove of customer data" (TechCrunch). Unlike MGM who was able to skirt the need to pay ransom, Caesars relented nearly $15 million toward preventing the release of the thieved data. TechCrunch similarly noted that "Caesars confirmed the cyberattack was caused by social engineering on an outside IT vendor." Sound familiar?

Malware and Tools Used by Scattered Spider

Tactics	Malware, tools, services
Reconnaissance	Linkedin
Initial Access	EIGHTBAIT (0ktapus phishing kit)
Persistence	RattyRat, bedevil, AADInternals
Privilege Escalation	LINpeas, aws_consoler, STONESTOP, POORTRY, KDMapper, HashiCorp Vault, Trufflehog, GitGuardian, Jecretz, pacu
Defense Evasion	privacy.sexy
Credential Access	Mimikatz, ProcDump, DCSync, LAPSToolkit, LaZagne, gosecretsdump
Discovery	RustScan, ADRecon, ADExplorer, PingCastle, MicroBurst, Advanced Port Scanner, Angry IP Scanner, Angry Port Scanner, SharpHound, CIMplant, ManageEngine, LANDESK, PDQ Inventor, Govnomi, PureStorage FlashArray
Lateral Movement	Impacket, CitrixReceiver, CitrixWorkspaceApp, mobaxterm, ngrok, OpenSSH, proxifier, PuTTY, socat, Wstunnel, RDP, Cloudflare Tunnel client, Chrome Remote Desktop, PsExec, Sshimpanzee
Collection	Atomic, Vidar, Meduza, Raccoon, Snaffler, Hekatomb, Lumma, DBeaver, MongoDB Compass, Azure SQL Query Editor, Cerebrata, FiveTran, AveMaria
Command and Control	RMM tools (listed below), rsocx, NSOCKS, TrueSocks, Twingate
Exfiltration	Telegram, Rclone, MEGAsync, Storage Explorer
Impact	BlackCat ransomware

Source: https://blog.sekoia.io/scattered-spider-laying-new-eggs/#h-iocs-amp-technical-details

Scattered Spider:

- **Technical analysis of Scattered Spider's capabilities:**https://socradar.io/dark-web-profile-scattered-spider/
- **News report on Scattered Spider activity:** https://www.cbsnews.com/news/scattered-spider-blackcat-hackers-ransomware-team-up-60-minutes/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports