Scattered Spider

Target Bio

Names/Alias: Scattered Spider, UNC3944, Storm-0875, Oktapus, Scatter Swine
Affiliations: Criminal group “The Com”
Motivation: Financial gain
First Activity: Mid-2022
Structure: Decentralized, age range 13-25 years old
Country of Basis: US, UK, and Canada
Targets: Large scale enterprise organizations
Methodology: Social Engineering, Spear Phishing, Help Desk attacks, Live-Off-The-Land
Most Recent Development: Working with “DragonForce” and collaborating with “ShinyHunters”

BLUF

Scattered Spider utilizes sophisticated social engineering techniques that target process vulnerabilities over technical ones. They utilize live off the land techniques and specialize in enterprise systems, making them extremely difficult to detect by traditional means. Defenses against such attacks must address process vulnerabilities by implementing phishing resistant MFA practices and application controls for software execution.

Background

Scattered Spider is an e-Crime threat actor that has gained notoriety in the last 4 years for highly technical attacks and data extortion [1]. The group uses complex social engineering tactics to target organization help desks with legitimate employee credentials to bypass MFA. Then they use live off the land techniques to avoid detection while extracting data and leveraging high levels of knowledge in Azure, AWS, and Google environments [2][3]. They have worked with ransomware groups since 2023, the most recent being DragonForce. They are described as “big game” hunters by the SANS institute and target large, enterprise organizations [4].

Summary (General Overview)

Scattered Spider is a mostly natively English-speaking, financially motivated threat group that falls under a larger network known as The Community (The Com) [4], a loosely organized criminal group composed of 13-25 year olds with other criminal groups such as 764, who are responsible for the exploitation of minors through extortion and distribution of CSAM [4][5]. Their main targets over the last three years have been higher valued targets opting to hunt for a specific victim, rather than accepting the opportunity to infiltrate a random business. Their main Multi-Factor Authentication (MFA) bypassing technique has been social engineering, where Scattered Spider attempts to spoof the identity of a real employee of a business by contacting the business’s IT Help Desk in order to attempt to have the MFA information altered on the real employee’s account so that the threat actor can infiltrate using the compromised account. Once they have infiltrated the account, the attackers will comb through shared files like SharePoint slides for network information, extracting any and all useful information for further exploitation [3].

Details & References

Analysis Summary

Scattered Spider relies on a combination of social engineering techniques combined with ransomware in recent years to exfiltrate large amounts of data from enterprise organizations [1][4]. They are unique in their tactics, as they do not predominantly rely on exploiting technical vulnerabilities, and instead target the processes and procedures of an organization by collecting intelligence on higher level IT employees and exploiting credentials [2][3][4]. Using open platforms like social media, the group could discern the answers to common security questions asked by the help desk, allowing them to bypass multi factor authentication [2]. The group has additionally engaged in double extortion techniques by both encrypting data on enterprise systems and exfiltrating the same data to use for extortion [2]. The group in recent months teamed with hacking groups Lapsus$ and Shiny Hunters to use combination of social engineering, ransomware, and data exfiltration on organizations. The most recent targets have been Red Hat, Salesforce, and Jaguar [6], the latter of which carrying an estimated loss of $2.5 million USD in damages to the UK economy [7]. The group has allegedly stated they are going underground, though this is highly unlikely to be the case as this is a common practice among hacking groups and fits their pattern of going underground for several months before reemerging later with a series of attacks [3][6][8]. Counter measures against these attacks are listed below and can be found in a document from CISA. These recommendations are:

1. Maintain offline backups of data that are stored separately from the source systems and tested regularly.
2. Enable and enforce phishing-resistant multifactor authentication (MFA).
3. Implementing application controls to manage and control software execution [1].

In addition to the measures from CISA, the Financial Services Information Sharing and Analysis Center (FS-ISAC) has released their own document with a list of strategies to deter Scattered Spider exploits. These strategy subjects range from Detection and Suppression, like training and further educating Help Desk employees, to Network Defenses, like implementing a web proxy and firewall that blocks any malicious infrastructure found [9].

Picture Credit: Palo Alto Networks

References

[1] *Scattered Spider* - CISA

[2] *M-Trends 2025 Report* - Google

[3] *2025 Threat Hunting Report* - CrowdStrike

[4] *Shaking up the Ransomware Game: Introducing Scattered Spider* - SANS

[5] FBI alerts tie together threats of cybercrime, physical violence from The Com

[6] Analyzing "Scattered Lapsus$ Hunters" breaches since 2021

[7] Jaguar Land Rover hack cost UK economy an estimated $2.5 billion, report says

[8] AI Ransomware, Hiring Fraud and the end of Scattered Lapsus$ Hunters - IBM

[9] *Scattered Spider & BlackCat Ransomware: Mitigation Guidance* - FS-ISAC