Hands On Lab: Unit 8

MICS-252, Fall 2024

Threat Analysis

Prepared by: Karl-Johan Westhoff

email: kjwesthoff@berkeley.edu

UC Berkeley School of Information

MICS Course 252 Fall 2024 (Kristy Westphal)

1 Introduction

Threat intelligence is when an adversary is associated with the data. To better understand adversaries and how to account for them in threat modeling, it is useful to put adversaries into categories defined by what they want, what their capabilities are, and how they conduct their 'activities'[1] in this assignment I decided to look at threat actors who target cloud 'systems', many 'things' are moving/have moved to the cloud[2]. Cloud-ification offers security benefits:

- Someone else handles security often with synergies doing it for many customers
- Increased reliability, and availability etc.

But is also comes with a significant problem:

- Someone else is handling your security

With a 'someone else' is handling parts of your security as a part of their hosting service, there is a risk for responsibilities "falling between two stools", especially in complicated architectures with services from different cloud systems. This often makes enterprises terrible at security [2] defines a "toxic cloud triad" of highly privileged, publicly exposed workloads with weak configuration. The adversaries know this and targets default configuration and especially access control to breach and achieve persistence on cloud systems.

[1] Tactics Techniques and Procedures (TTP), "modus operandi" in classic spy terms
[2] A 'reaction' going in the opposite direction, in-sourcing and self-hosting is also occurring[1]

2 Scattered Spider

2.1 Description

According to MITRE[3] Scattered Spider has been active since 2022, and initially targeted customer relations systems and telecommunication companies. Apparently they figured out that they were good at obtaining credentials to systems using social engineering. They did this by portraying to be employees or internal IT often in longer duration social engineering acts, Hence MITRE concluded that they are native English speakers. Crowdstrike included a section on Scattered Spider in their 2024 Global Threat Report [4], shown in Appendix A and describes their modus of targeting IT services using elaborate social engineering.

2.2 Targets

CISA[5] has defined Scattered Spider as a cyber criminal group targeting information systems of large companies for extortion.
Most notably the group targeted the "MGM Grand" casino resort, the attack was carried out in 'joint venture'[3] with "ALPHV/BlackCat"[6][7], providing "Ransomware as a service"[4]. The attack disrupted operations for 10 days ,they had to shut down systems and operate 'manually', notify their customers and cost MGM $100M[6], but who knows - what happens in Vegas stays in Vegas.

Targets summary: Larger corporations for extortion

2.3 Modus Operandi

Scattered Spider are able to conduct elaborate social engineering campaigns, using open intelligence (LinkedIn etc.) to circumvent security measures (see quote in Appendix B). Furthermore they are able to leverage deep knowledge on various cloud systems (Azure Active Directory) and identity management (OKTA) get a foothold. From there various tools for monitoring and ex filtration (Fleetdeck etc.), credential extraction (e.g. Mimikatz) and malware (eg. ransomware) are deployed. CISA has compiled a list based on MITRE Att&ck in [5] and depicted in Appendix C.

The MGM attack [6] has a good write-up on how Scattered Spider gained initial foothold.

1. Use OSint (LinkedIn etc.) to identify a suitable employee and assume their identity

[3] This has neither been confirmed nor denied by either parties
[4] This whole hacker thing is increasingly becoming corporate

2. Call MGM IT requesting assistance to log in
3. A 10 minute phone call allegedly gave administrator privileges to MGM OKTA and Azure environments even with MFM in place (using phone sim hijacking)
4. Deploy reconnaissance and terminate security software (POORTRY/STONESTOP see Appendix D)[8]
5. Deploy command and control for persistence and ex-filtration

Modus Operandi Summary Use knowledge of systems and elaborate social engineering (voice phishing, "vishing") and advanced techniques (sim hijacking) to convince victim to provide credentials (even when these are multi factor (MFA))

2.4 TTP's

CISA article [5] Has a detailed set of tables with the MITRE att&ck Tactics and Techniques a condensed summary there of is :

- Reconnaissance/Resource Development:
  - Gather victim identities using SoMe profiles
  - Gather information in victim system/architecture
  - Fake SoMe accounts to back up phishing stories
  - Phone SIM hijacking, number stealing
- Initial Access, using 'Social Engineering'
  - Phishing targeted against IT access control, either posing as IT asking for credentials, or posing as employees requesting MFA reset etc.
  - Elaborate, convincing phone voice phishing 'acts' (Vishing), fluent in English
  - SMS phishing using hijacked numbers to convince credentials handover (smishing)
  - MFA fatigue (someone accepting after receiving many MFA approval notifications)
- Execution, Persistence, Privilege Escalation, Defense Evation
  - Collect data, credentials etc. using e.g Mimikatz see Appendix C
  - Impersonate IT gain remote desktop access (again requiring social skills to be convincing)
  - Create new users
- Extortion and data theft
  - Establish C2 infrastructure see Appendix C
  - Gather, compress and ex filtrate data
  - Extort Victim

2.5 Recommendations

3 Conclusion

I'm not so sure they can keep the vishing campaigns up, the use of their voice gives possibility for profiling and subsequent attribution

4 Notes

Include how the group typically targets, the methods that they use, and what their typical goal is.

1. Begin by choosing a threat actor group from the MITRE page.

2. Utilizing open source intelligence, research who the group typically targets, what methods they use to attack their targets and what they are generally after.

3.Identify any known tactics, techniques and procedures.

4. Make recommendations on actions that a SOC can take with the data that you have found on your chosen threat group.

5. Be sure to document all of the sources that you utilize in your research.

5 Notes

The one size fits all for cloud security means that the same holes are found in many walls. This can be utilized to get a foothold in many locations using the same methodology.

References

[1] *We have left the cloud*. `https://world.hey.com/dhh/we-have-left-the-cloud-251760fb`. Accessed: 2024-10-17.

[2] *Cloud Security Epic Fails*. `https://youtu.be/3zsArvBRumY?feature=shared`. Accessed: 2024-10-17.

[3] *MITRE Scattered Spider*. `https://attack.mitre.org/groups/G1015/`. Accessed: 2024-10-17.

[4] *CROWDSTRIKE 2024 GLOBAL THREAT REPORT*. `https://www.crowdstrike.com/global-threat-report/`. Accessed: 2024-10-17.

[5] *CISA Scattered Spider*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a. Accessed: 2024-10-17.

[6] *ALPHV: Hackers Reveal Details of MGM Cyber Attack*. https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/. Accessed: 2024-10-18.

[7] *The chaotic and cinematic MGM casino hack, explained*. https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware. Accessed: 2024-10-18.

[8] *TrellixScattered Spider The Modus Operandi*. https://www.trellix.com/blogs/research/scattered-spider-the-modus-operandi/. Accessed: 2024-10-17.

Appendices

A Scattered Spider Section from Crowdstrike's 2024 Report

SCATTERED SPIDER Conducts Sophisticated Social Engineering Campaigns

Identity-based techniques are also central to SCATTERED SPIDER tradecraft. Throughout 2023, this adversary conducted sophisticated social engineering campaigns to access victim accounts. SCATTERED SPIDER's tactics included SMS phishing (smishing) and voice phishing (vishing) to harvest credentials and phone calls made to victim organization help desks to persuade support personnel to provide password and/or MFA resets for targeted accounts. In many cases, SCATTERED SPIDER also leveraged earlier intrusions at telecom organizations to SIM swap targeted employee phone numbers, enabling the adversary to then receive SMS messages containing OTP codes.

SCATTERED SPIDER deliberately selects social engineering campaign targets from employees in information security and other IT-related teams. This is likely due to direct employee access to security tools as well as applications and documentation that may support lateral movement and further account compromise. In a minority of incidents, SCATTERED SPIDER targeted accounts belonging to employees who had direct access to company financial resources.

Additionally, SCATTERED SPIDER often configured residential proxies to appear as though they were logging in to victim accounts from the same geographical area as the legitimate account owner. In doing so, the adversary further exhibited its understanding of identity-related security policies in enterprise organizations.

Figure 1: *Crowdstrike, Global Threat Report 2024, Scattered spider section from [4]*

B Comment on the MGM attacks and 'vishing' modus

CISO's comment on the use of social engineering in the MGM attack, from VOX[7]:
"There's always a little back door, and all the best defenses and all the expensive tools can be fooled by one good social engineering attack," Peter Nicoletti, global chief information security officer at cybersecurity company Check Point Software, told Vox.

C CISA compiled list of soft/malware tools

Table 1: Legitimate Tools Used by Scattered Spider

Tool	Intended Use
Fleetdeck.io	Enables remote monitoring and management of systems.
Level.io	Enables remote monitoring and management of systems.
Mimikatz [S0002]	Extracts credentials from a system.
Ngrok [S0508]	Enables remote access to a local web server by tunneling over the internet.
Pulseway	Enables remote monitoring and management of systems.
Screenconnect	Enables remote connections to network devices for management.
Splashtop	Enables remote connections to network devices for management.
Tactical.RMM	Enables remote monitoring and management of systems.
Tailscale	Provides virtual private networks (VPNs) to secure network communications.
Teamviewer	Enables remote connections to network devices for management.

In addition to using legitimate tools, Scattered Spider also uses malware as part of its TTPs. See Table 2 for some of the malware used by Scattered Spider.

Figure 2: *'Legitimate' software tools used by Scattered Spider[5]*

Malware	Use
AveMaria (also known as WarZone [S0670])	Enables remote access to a victim's systems.
Raccoon Stealer	Steals information including login credentials [TA0006], browser history [T1217], cookies [T1539], and other data.
VIDAR Stealer	Steals information including login credentials, browser history, cookies, and other data.

Figure 3: *'Malware' tools used by Scattered Spider[5]*

D Tools used to evade detection

Scattered Spider typically exploits vulnerabilities such as CVE-2015-2291 [8]

- POORTRY is a malicious driver used to terminate selected processes on Windows systems, e.g., Endpoint Detection and Response (EDR) agent on an endpoint.11 To evade detection, attackers have signed POORTRY driver with a Microsoft Windows Hardware Compatibility Authenticode signature.

- STONESTOP is a Windows userland utility that attempts to terminate processes by creating and loading a malicious driver.13 It functions as both a loader/installer for POORTRY, as well as an orchestrator to instruct the driver with what actions to perform