

# Scattered Spider Case Study

## Scattered Spider Case Study

- ◆ SOC responded to report of **new two-factor device**
- ◆ **Weeks later**, restored IT systems and infrastructure
- ◆ Lapsus\$ and Scattered Spider use **social engineering and reconnaissance**
- ◆ They **demand ransom** through ransomware or data exfiltration



# Infrastructure Breach



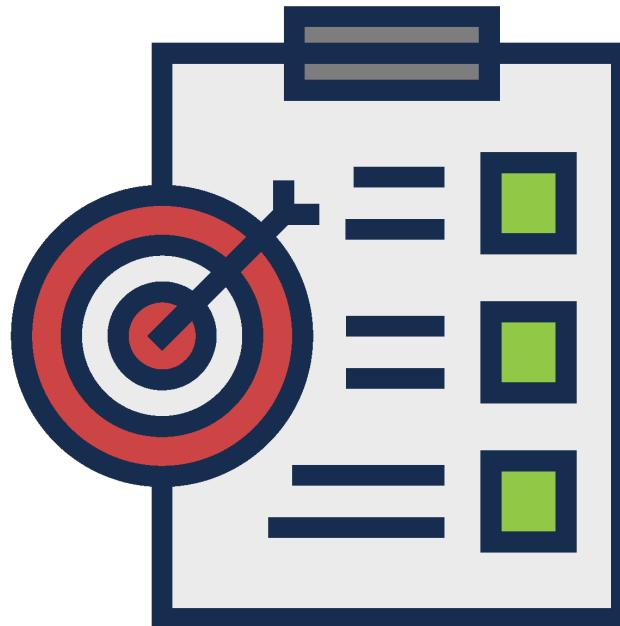


- ◆ Initial target was an **IT admin**, likely intentional
- ◆ Group used LinkedIn or **public info** to **find a target** with IT system access
- ◆ **Harvested credentials** to add a two-factor authentication token via a support method weakness
- ◆ **Accessed user's email** through a legacy one-factor protocol to verify the new token



- Used IT manager's account to read documentation on two-factor authentication rollout
- Read IAM system configuration articles and installation instructions for remote tools and VPN
- Searched internal code repository for configuration files and credentials
- Compromised IAM infrastructure to gain access to any account

# Objectives



- ◆ Groups are interested in **fame and notoriety**, not just money
- ◆ Hospitality company **repeatedly thwarted** ransomware attempts
- ◆ In **retaliation**, threat group **caused damage** using stolen cloud infrastructure credentials
- ◆ This resulted in **several weeks of recovery efforts**

# Similar Incidents

≡ Bloomberg Subscribe ...

Technology | Cybersecurity

## MGM Resorts Hackers Broke In After Tricking IT Service Desk

- Okta warned about hackers using similar techniques in August
- Group suspected of attack is well known for social engineering





A cyberattack that disrupted MGM resorts and casinos across the country is believed to have begun with a social engineering breach of the company's information technology help desk. Photographer: Bridget Bennett/Bloomberg

By Andrew Martin, Ryan Gallagher, and Katrina Manson  
September 15, 2023 at 8:10 PM EDT  
Updated on September 16, 2023 at 7:11 AM EDT

[www.bloomberg.com](http://www.bloomberg.com)

# 2023 MGM Attack:

- ◆ Used **social engineering** to access employee account
- ◆ Obtained **password reset** with basic information
- ◆ Targeted **IAM infrastructure** and deployed ransomware
- ◆ MGM **refused ransom**, spent weeks restoring systems

Similar Incidents



Technology | Cybersecurity

## Caesars Entertainment Paid Millions to Hackers in Attack

- Hackers stole data, extorted company, people familiar said
- Caesars breach came in weeks before MGM announced cyberattack



Caesars Palace in Las Vegas, Nevada. Photographer: Bridget Bennett/Bloomberg

By William Turton

September 13, 2023 at 2:52 PM EDT

Updated on September 14, 2023 at 9:55 AM EDT

[www.bloomberg.com](http://www.bloomberg.com)

# 2023 Caesar Attack:

- ◆ Caesar's paid a **\$15m ransom** to restore systems and prevent data release
- ◆ SEC 8-K filing stated **no material effect** on financial condition
- ◆ Initial attack vector was **social engineering by phone**

Similar Incidents



# Lessons Learned



## Lessons Learned

- ◆ Social engineering remains a **successful breach vector**
- ◆ Threat groups use **advanced** tactics
- ◆ Two-factor authentication is **not foolproof** due to bypass methods
- ◆ Attacks exploit **weak help desk** processes and MFA fatigue
- ◆ Organizations must implement **defense in depth**

