

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



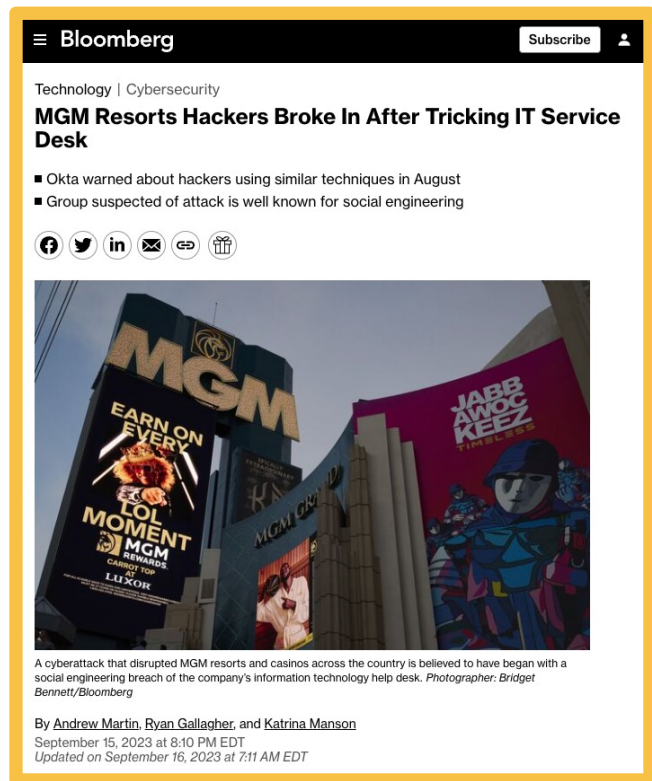
- ◆ **Used IT manager's account** to read documentation on two-factor authentication rollout
- ◆ Read IAM **system configuration articles** and **installation instructions** for remote tools and VPN
- ◆ Searched **internal code repository** for configuration files and credentials
- ◆ **Compromised IAM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



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





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**

