MGM Casino Attack

Calvin Ray Schmeichel
St. Cloud State University
Cybersecurity
Calvin.schmeichel@go.stcloudstate.edu

Will Novotny
St. Cloud State University
Cybersecurity
Will.Novotny@go.stcloudstate.edu

Griffin Davies
St. Cloud State University
Cybersecurity
griffin.davies@go.stcloudstate.edu

I. Introduction (Abstract)

In the ever-evolving landscape of cybersecurity, the MGM Ransomware breach of September 11, 2023, stands as a pivotal moment that strongly highlights the escalating challenges and complexities of digital security threats. This severe incident, which targeted MGM Resorts International, a titan in the hospitality and entertainment industry, resulted in staggering financial losses and operational disruptions, estimated at nearly $100 million. It marked not only a significant setback for MGM but also sent a ripple of concern across the global technology and cybersecurity communities.

This breach was orchestrated by the sophisticated coordination of two formidable cyber threat actors, Scattered Spider, and ALPHV. Their alliance and the methods employed in the attack underscore the need for a more robust and adaptive cybersecurity framework across various industries. The decision by MGM Resorts International to resist the demands of the ransomware, opting not to pay the ransom, added a profound ethical dimension to the incident. This stance highlighted the moral and financial dilemmas inherent in responding to ransomware attacks and opened up critical discourse on the strategies and implications involved in such situations.

The MGM breach, thus, serves not just as a case study in the impact of cyber threats but also as a catalyst for reexamining and reinforcing cybersecurity measures. It emphasizes the vulnerability of even the largest organizations to sophisticated cyber attacks and the need for constant vigilance and innovation in cyber defense strategies.

In this document, we delve into the intricacies of this high-profile cyberattack. We aim to dissect the techniques, tactics, and procedures employed by Scattered Spider and ALPHV, explore MGM's response, and propose effective countermeasures to enhance resilience against such formidable cyber adversaries. Our exploration will not only provide insights into this specific incident but also contribute to the broader understanding and preparation for future cyber threats in an increasingly interconnected world.

II. Problem Domain

The MGM Ransomware breach on September 11th, 2023, underscored the profound challenges presented by cyber threats in our digital age. The assault dealt a severe blow to MGM Casino, resulting in almost $100 million in cumulative damages. This incident not only rattled MGM but also sent shockwaves throughout the entire technology sector, laying bare the harsh reality that even sizable companies can fall prey to exploitation and remain susceptible to malicious attacks.

The threat actors Scattered Spider and ALPHV highlighted a new level of coordination and sophistication in cyber attacks, emphasizing the urgent need for enhanced cybersecurity

measures across industries. The principled decision by MGM Resorts not to pay the ransom added another layer to the narrative, bringing attention to the ethical and financial considerations surrounding ransomware incidents. The MGM breach serves as a critical case study, shaping future discussions on cybersecurity resilience and the evolving landscape of cyber threats.

III. Problem Statement

Address the Techniques, Tactics, and Procedures employed by Scattered Spider in conjunction with ALPHV during their offensive actions, to propose effective mitigations and countermeasures against these threat actors.

IV. Research Questions

A. What is MGM?

MGM refers to MGM Resorts International, a major hospitality and entertainment company that owns and operates hotels and casinos, including well-known properties on the Las Vegas Strip.

B. Who is Scattered Spider?

Scattered Spider is a versatile and prolific English-speaking hacking group known for its expertise in social engineering and SIM-swapping attacks. The group has been linked to various cyber-attacks, including the MGM hack.

From the article, “What Everyone Got Wrong About the MGM Hack”, “The threat actors known as “Scattered Spider” (also known by, or associated with: Scattered Swine, Oktapus, Octo Tempest, and a variety of other monikers) have been widely blamed for the MGM hack. They’re a versatile and prolific English-speaking group known for their skill in social engineering and SIM-swapping attacks.” [1] This gives us more insight into the hacker group Scattered Spider and what they are known for.

C. Who is ALPHV/Blackcat?

ALPHV, also known as BlackCat and Noberus, is a notorious Eastern European ransomware group. They are associated with extensive ransomware attacks globally and have targeted numerous organizations, including MGM Resorts International.

From the article, “What Everyone Got Wrong About the MGM Hack”, “ALPHV/BlackCat have also been linked to the attack. They’re a notorious Eastern European ransomware group that have targeted hundreds of organizations worldwide (including Reddit). Their RaaS (ransomware as a service) software is one of the most used ransomware families observed by IBM. Scattered Spider and ALPHV bring rather disparate skillsets to the table, so the idea that they might be collaborating is concerning to security experts.” [1] This quote gives us insight into who ALPHV is and their skills of expertise with hacking. Also, in this article

it suggests that ALPHV and Scatter Spider may have been working together on this MGM attack. However, there still is no concrete proof yet of this.

D. How was the attack conducted?

The attack on MGM Resorts International began with a vishing (phone-based phishing) call to the company's IT help desk. The attackers impersonated a privileged IT employee, likely using information obtained from social media and the company website, and gained access to a super administrator account with advanced privileges across MGM's systems. The attackers also utilized voice phishing attacks and deployed their own Identity Provider (IDP) to maintain continued access.

From the article, “What Everyone Got Wrong About the MGM Hack”, “It’s easy to hear these stories and ask why IT workers weren’t more suspicious. But vishing attackers can be extremely convincing (and they’re getting more convincing all the time), and in a massive company, it’s not as though the person on help desk duty knows everyone else on a first name basis. On top of that, IT desks are often under pressure to solve problems quickly, they aren’t always afforded the luxury of taking things slow when someone calls for help.” [1] This gives us an insight on what IT helpdesk deals with on a day-to-day basis and how it would be easy for a social engineering attack to occur.

E. What attack TTP were used (Techniques, Tactics, Procedures)?

The primary attack methods involved social engineering through a vishing call to the help desk, gaining access to a super administrator account. Subsequent actions included exploiting vulnerabilities in MGM's infrastructure, deploying ransomware, and encrypting essential systems. Scattered Spider demonstrated sophistication by establishing a secondary IDP to maintain control.

F. What is ransomware?

Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money, or ransom, is paid. In this context, the attackers used ransomware to encrypt MGM's systems and demanded payment for decryption.

G. How can organizations improve the security of their help desk systems to prevent social engineering attacks?

Organizations can enhance help desk security by implementing good user verification protocols, training employees to recognize social engineering tactics, and adopting social engineering-resistant multi-factor authentication (MFA). Regular security awareness programs and assessments can also strengthen defenses against social engineering attacks.

H. To what extent did social engineering play a role in the MGM hack, and how did the attackers gather information for impersonation?

Social engineering played a significant role in the MGM hack. The attackers used vishing calls to impersonate employees and gathered information from social media platforms like LinkedIn to convincingly impersonate legitimate users during the Helpdesk interaction.

I. Effects of not paying the ransomware vs. paying ransomware?

MGM chose not to pay the ransom, leading to significant disruptions and financial losses. However, paying the ransom can result in data recovery but may also encourage further attacks.

J. What was MGM's response to the attack/was it effective?

MGM responded to the attack by taking down its infrastructure to evict the hackers, causing disruptions to hotel and casino operations. The company refused to pay the ransom and experienced extended outages. MGM's response also included offering credit monitoring and identity protection to affected customers.

K. What are Scattered Spider's common attack techniques?

Scattered Spider's common attack techniques include voice phishing attacks, compromised credentials, and the establishment of a secondary Identity Provider (IDP) to maintain access.

V. Objectives

This project aims to gain an in-depth understanding of MGM's security and network infrastructure. This includes exploring the security measures implemented by MGM and analyzing how these controls were breached. Additionally, the project seeks to uncover detailed information about the entities responsible for these security breaches.

VI. Scope

The scope of this project was to learn more about the MGM security and network infrastructure. While also learning about how their security controls that were put in place were circumvented. And finding out more about the groups behind the attack. We then want to leverage this new discovered knowledge and apply possible solutions that MGM could have implemented.

VII. Research Contribution

Our research contribution to the field will be us gaining a better understanding of the attack. Since our wide and thorough research will provide so much information we will aggregate all of it into a concise research paper that anyone can read at a high level. We wanted to do this since we found there was a lack of in-depth analysis on the topic even months later

We would also like to provide a simple attack timeline with an outline of MGM's current security controls and open a dialogue on how these controls could have been better protected.

VIII. Hypothesis (Research Questions)

Research Question 1: “How effective was the attack?”.

- Purpose: This question aims to assess the impact and severity of the cyberattack. Understanding the effectiveness of the attack helps in evaluating the scale of the breach and the magnitude of its consequences. This includes examining the extent of data compromise, the duration and scope of operational disruptions, and any long-term implications for MGM Resorts.
- Value: Assessing the effectiveness of the attack can provide insights into the capabilities of the attackers and the vulnerabilities in MGM Resorts' systems. This information is crucial for both the company and the wider cybersecurity community in understanding current threat landscapes and improving defense strategies.

Research Question 2: “How effective are these systems at detecting these attacks?”

- Purpose: This question focuses on the effectiveness of MGM Resorts' cybersecurity measures in detecting the attack. It involves evaluating the security infrastructure, the readiness of the systems to identify and flag malicious activities, and the speed of detection.
- Value: Investigating the detection capabilities sheds light on potential gaps in cybersecurity practices and highlights areas for improvement. Effective detection is a critical component of cybersecurity, as timely identification of threats can significantly mitigate damages.

Research Question 3: “What mitigations should have been in MGM’s response to these attacks?”

- Purpose: This question examines the adequacy and effectiveness of MGM Resorts' response to the cyberattack. It involves analyzing the immediate actions taken post-detection, the communication strategy with stakeholders, and the measures implemented to prevent future incidents.
- Value: Understanding the response to the attack is essential for developing robust incident response protocols. This includes lessons learned regarding crisis management, customer communication, and post-incident recovery. Effective mitigation strategies are key to minimizing the impact of cyberattacks and ensuring rapid recovery and resilience.

IX. Literature Review

a. CISA Report: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

i. **Structure and Style**: The document is structured in a formal, technical style, typical of government or agency reports. It's divided into sections like Summary, Technical Details, Mitigations, and Reporting. This structured approach aids in clearly presenting complex technical information.
ii. **Content and Themes**: The primary theme revolves around cybersecurity threats and mitigation strategies. It details the tactics, techniques, and procedures (TTPs) used by Scattered Spider, including social engineering, phishing, and SIM swap attacks. The advisory emphasizes the importance of awareness and preparedness against such cyber threats.
iii. **Purpose and Audience**: The document seems aimed at a professional audience involved in cybersecurity, IT management, and network defense. Its purpose is to inform and advise these professionals on current cyber threats and recommended countermeasures.
iv. **Language and Tone**: The language is technical, focusing on precision and clarity. It includes specific cybersecurity terminologies and references to the MITRE ATT&CK framework, indicating a high level of technical detail intended for a knowledgeable audience.
v. **Implications and Recommendations**: The advisory provides specific recommendations for mitigating cyber threats, such as implementing phishing-resistant multi-factor authentication, application controls, and maintaining offline backups. These recommendations reflect a proactive and defensive stance against cyber threats.

b. FBI IC3: https://www.ic3.gov/Media/News/2023/231116.pdf
i. **Structure and Style**: Like the first document, this one is formally and technically structured, indicating its intended use as a detailed advisory. It is divided into various sections, including a summary, technical details, and mitigations, which is characteristic of government or agency reports.
ii. **Content and Themes**: The document delves into the detailed operations of a cybercriminal group, covering their methods of attack and the types of threats they pose. It emphasizes on the importance of cybersecurity awareness and preparedness, a theme consistent with the first document.
iii. **Purpose and Audience**: Targeted at a professional audience in cybersecurity and IT management, this document serves as an informative piece on current cyber threats and strategies for counteraction. It is intended to advise and guide professionals in enhancing their defense mechanisms against such threats.
iv. **Language and Tone**: The document employs technical language, with specific terminologies and references that suggest a high level of detail aimed at an audience well-versed in cybersecurity.
v. **Implications and Recommendations**: It provides specific recommendations for mitigating cyber threats, similar to the "Scattered Spider" document. These

recommendations are intended to guide organizations in strengthening their defense against cybercriminal activities.

X. Methodology

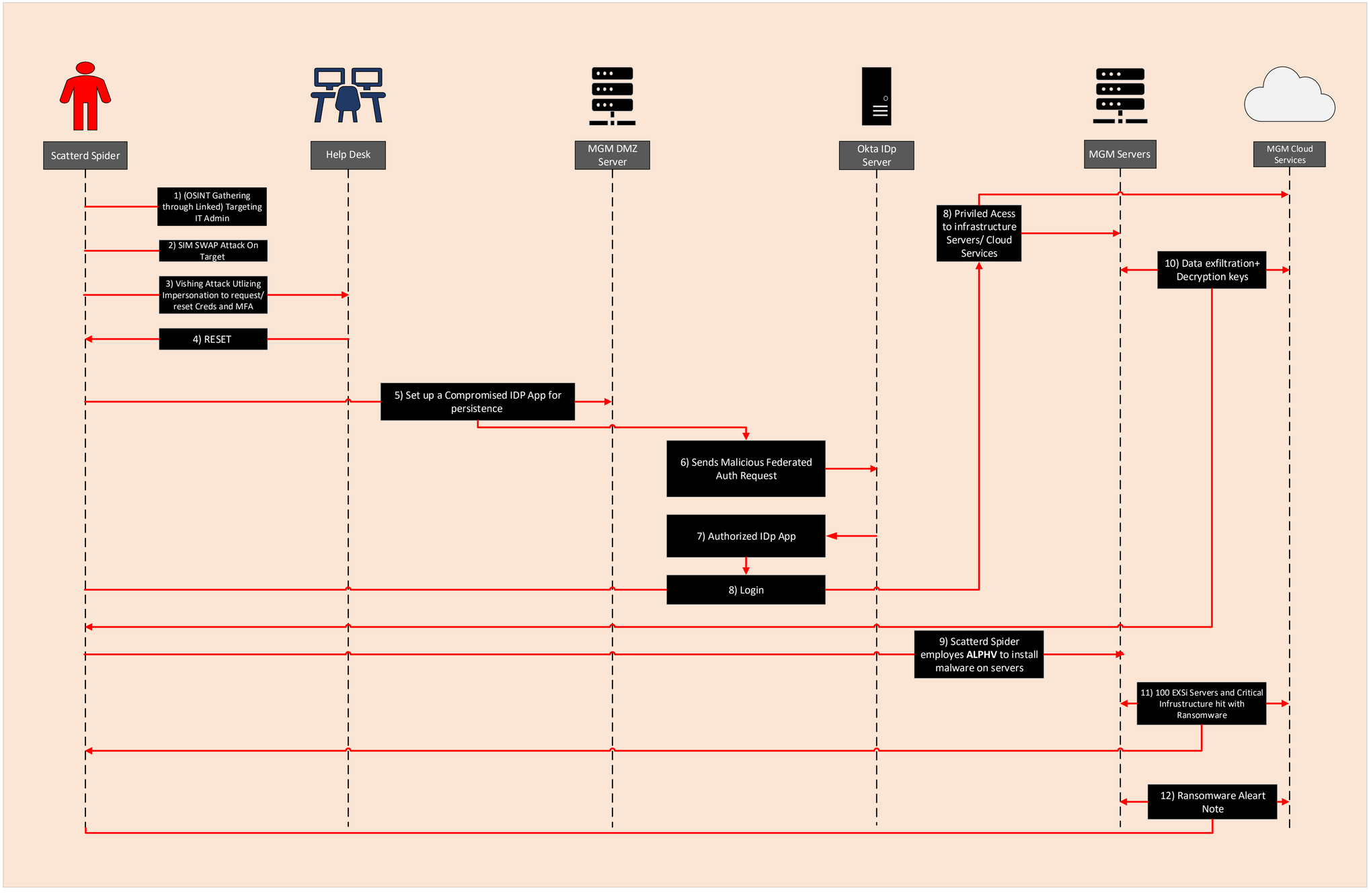
Our main research design for this project was to have a mixed method of quantitative, and qualitative approaches through occurring broad information on the topic. We then wanted to apply these findings to our results and have an equal quantitative and qualitative look at those.

The sampling we used for this study was referencing mainly research documents on the subject of what was written from September 2023 or newer.

XI. Results (Chart)

This attack timeline matrix maps the flow of the attack in an easily understandable format, Associated below the figure is a list of events and MITRE ATT&CK TTPs associated with the corresponding events, as well as proposed mitigations and countermeasures that could have been incorporated to prevent the attack.

MGM Attack Timeline Matrix



Event 1) Scattered Spider utilizes Open Source Intelligence to find IT Admin on Linkedin.

MITRE ATT&CK | Gathering Victim Identity Information, Tatic: Reconnaissance, ID T1589.
Mitigation: Private social accounts, only accept requests from known individuals.

Event 2) Utilizing found intelligence, Scattered Spider Social engineers IT Admin's SIM provider.

MITRE ATT&CK | Impersonation, Tatic: Defense Evasion, ID DS0015.
Mitigation: Try to use non-SMS multifactor authentication, if the attacker successfully performs a SIM swap attack, utilizing a different form of multifactor authentication will prevent this attack.

Event 3, 4) Utilizing SIM swapped phone line, Scattered Spider utilizes social engineering via spearvishing to the company help desk to reset MFA/login credentials gaining initial access.

MITRE ATT&CK | Impersonation, Tatic: Defense Evasion, ID DS0015
MITRE ATT&CK | Spearphishing Voice, Tatic: Initial Access, ID T1566.004
MITRE ATT&CK | Trusted Relationship, Tatic: Initial Access, ID T1199
Mitigation: Set up voice authentication procedures within the help desk to properly authenticate the caller.

Event 5, 6, 7, 8) Scattered Spider utilizes an elevated user account to set up an additional IDp application as a back door for persistence, and privilege escalation that gets authorized by OKTA IDp.

MITRE ATT&CK | Domain Policy Modification: Domain Trust Modification. Tatic: Defense Evasion, Privilege Escalation, Permissions: Administrator ID T1484.
MITRE ATT&CK | Privilege Escalation, ID TA0004
MITRE ATT&CK | Persistence, ID TA0003
Mitigation: Apply Least Privilege Principle, Regular Audits, and Monitoring.

Event 9, 10) Scattered Spider, now has access to critical servers and cloud services, utilizing the help of ALPHV and their ransomware as a service, Scattered Spider loads malware onto 100 EXSi instances and other critical infrastructure. After the significant data is exfiltrated along with the decryption keys to the ALPHV ransomware.

MITRE ATT&CK | Exfiltration Over Web Service: Exfiltration to Cloud Storage, Tatic: Exfiltration, ID T1567.002
MITRE ATT&CK | Lateral Movement, ID TA0008

Mitigation: Data Loss Prevention, Network Monitoring, Proxy and Firewall Rules, Secure CASB Rules, Data Encryption.

Event 11, 12) Scattered Spider, now has initialized ALPHV's ransomware over EXSi instances and critical infrastructure servers, leaving alerts and notices to MGM.

MITRE ATT&CK | Data Encrypted for Impact, Tatic: Impact, ID T1486
MITRE ATT&CK | Financial Theft, Tatic: Impact, ID T1657
Mitigation: Regular Backups, Network Security, IDPS, Endpoint Protection, Incident Response Plan.

XII. Insights

Research Question 1 Answered: "How effective was the attack?".

The effectiveness of the cyberattack on MGM Resorts on September 11, 2023, can be assessed in terms of the extent of disruption caused and the amount of sensitive data compromised. Based on the available information:

1. **System Disruptions**: The attack led to significant system outages at MGM Resorts Las Vegas properties, indicating a substantial impact on their operational capabilities. The shutdown of computer systems, including those at prominent locations like the MGM Grand Hotel and casino, suggests that the attack effectively disrupted the company's routine operations. This is further confirmed by confirming it lost around $100 million.

2. **Data Breach**: The attack was particularly effective in terms of the data breach. An unauthorized third party obtained personal information of MGM Resorts customers, including names, contact information, gender, dates of birth, and driver's license numbers [**MGM Press Release:**]. The range of this data theft indicates a high level of effectiveness in penetrating MGM Resort's data security measures.

3. **Duration of Impact**: The ongoing nature of the system outages, as reported, also points to the attack's effectiveness. The ability of the attackers to maintain a persistent impact on MGM Resorts' systems suggests that the cyberattack was not only initially effective but also had a lasting effect.

4. **Response Time**: The time taken by MGM Resorts to detect, respond to, and recover from the attack also contributes to the assessment of the attack's effectiveness. This and the fact that MGM responded with a 10-day system shutdown to attempt to shield themselves from the attack obfuscates their response time.

In summary, the cyberattack on MGM Resorts was effective in causing operational disruptions and in breaching sensitive customer data, reflecting a significant impact on both the company's operational integrity and customer data security.

Research Question 2 Answered: "How effective are these systems at detecting these attacks?"

The MGM systems seemed to lack in effectiveness. Since scattered spiders used "perform discovery, specifically searching for SharePoint sites, credential storage documentation, VMware vCenter infrastructure, backups, and instructions for setting up/logging into Virtual Private Networks (VPN). The threat actors enumerate the victim's Active Directory (AD), perform discovery and exfiltration of victim's code repositories, code-signing certificates, and source code." [3]. It was later proved that the threat actors even got into internal Slack and Microsoft Teams calls to lessen in on conversations regarding the threat actor's intrusion and any security response.

Research Question 3 Answered: "What mitigations should have been in MGM's response to these attacks?"

The CISA and FBI had many mitigation recommendations for MGM. This included:

- Implement application controls: MGM should implement stricter control on employees' ability to install software. They recommend the concept of "allowlisting" certain applications their employees can use.
- They could also reduce the threat of malicious actors by:
    - Auditing remote access tools
    - Reviewing logs for execution of remote access software
    - Using security software
    - Requiring authorized remote access solutions
    - Blocking both inbound and outbound connections on common remote access software ports and protocols at the network perimeter.
    - Applying recommendations
    - [3]

XIII. Conclusions

The MGM Ransomware breach on September 11, 2023, highlighted the escalating threats faced by organizations in the digital age. MGM Resorts International suffered significant financial losses, nearly $100 million, exposing vulnerabilities to sophisticated cyber actors like Scattered Spider and ALPHV.

The attack, employing advanced social engineering tactics and a secondary Identity Provider, showcased the need for a more complex cybersecurity framework.

MGM's decision not to pay the ransom added an ethical aspect to the incident, sparking discussions on response strategies.

Our research delved into the attack's complexity, emphasizing the importance of user verification, training, and multi-factor authentication. Insights into the attack's impact and the effectiveness of cybersecurity measures contribute to a better understanding of evolving threats.

Mitigation recommendations from CISA and FBI offer actionable steps for organizations like MGM to enhance their defenses. The MGM breach serves as a crucial case study, providing valuable lessons for securing cybersecurity in the face of evolving threats.

Overall, this attack was a very severe cybersecurity attack that took advantage of many vulnerabilities and a lack of user training. This attack on MGM will be an example for companies to stay up-to-date on their cybersecurity training and mitigation techniques. It is important for companies to stay secure when dealing with customers and how a cyber attack can ruin a company's reputation.

XIV. Future Works

A. Interviews from people from MGM would be a great way to learn about the MGM attacks. This would allow us to have a better understanding of the techniques and methods used to help mitigate the attack. They could also provide us with more research methods. They can give us details about how to safely prevent such an attack. Another, good part of interviewing people is it would allow us to know what type of common attacks do they see the most in the industry. Overall interviewing someone who works at MGM would give us a lot of insight into the MGM attacks.

B. Advanced user verification protocols, would include exploring and implementing advanced user verification protocols that go beyond basic information such as name, employee identification number, and date of birth. Investigate the integration of biometric authentication or behavioral analytics to strengthen identity verification processes.

C. Develop targeted training programs to enhance employees' awareness of voice phishing (vishing) attacks. Conduct simulated vishing exercises to educate staff on recognizing and responding to social engineering tactics employed by threat actors.

D. Implement real-time monitoring and anomaly detection systems to identify unusual patterns of behavior, especially within help desk interactions. Leverage artificial intelligence and machine learning algorithms to detect and respond to potential security threats promptly.

E. Conduct regular incident response tabletop exercises to test and refine the organization's response to cyber incidents. Simulate various scenarios, including

social engineering attacks, to ensure that the incident response team is well-prepared to mitigate and recover from potential breaches.

F. Conduct regular security assessments, including penetration testing and vulnerability assessments, to identify and address potential weaknesses in the organization's cybersecurity infrastructure. Use the findings to proactively enhance security measures and stay ahead of evolving cyber threats.
G. Investigate the legal and ethical considerations surrounding ransom payments in cybersecurity incidents. Work with legal and compliance teams to develop clear guidelines and policies on whether to pay or not pay a ransom, considering the potential consequences and ethical implications.

XV. REFERENCES

1. Sudbeck, R. (n.d.). What everyone got wrong about the MGM hack. Kolide. https://www.kolide.com/blog/what-everyone-got-wrong-about-the-mgm-hack
2. Gupta, S. (n.d.). In-depth analysis of the 2023 MGM Resorts Cyberattack (VIRSEC systems blog). https://industrial-software.com/community/news/in-depth-analysis-of-the-2023-mgm-resorts-cyberattack-virsec-systems-blog/
3. Scattered spider: Cisa. Cybersecurity and Infrastructure Security Agency CISA. (2023, December 1). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
4. Scattered spider. Scattered Spider, Roasted 0ktapus, Group G1015 | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/versions/v14/groups/G1015/
5. CrowdStrike 2023 global threat report: Executive summary. crowdstrike.com. (2023, March 27). https://www.crowdstrike.com/resources/reports/global-threat-report-executive-summary-2023/
6. MGM Resorts Update on recent cybersecurity issue. (n.d.). https://investors.mgmresorts.com/investors/news-releases/press-release-details/2023/MGM-RESORTS-UPDATE-ON-RECENT-CYBERSECURITY-ISSUE/default.aspx
7. Thompson, A. (2023, November 16). The MGM resorts attack: Initial analysis. Identity Security and Access Management Leader. https://www.cyberark.com/resources/blog/the-mgm-resorts-attack-initial-analysis
8. NBCUniversal News Group. (2023, September 15). Who are the hackers that breached MGM's Las Vegas operations? NBCNews.com. https://www.nbcnews.com/tech/security/mgm-las-vegas-hackers-scattered-spider-rcna105238
9. ABC News Network. (n.d.). ABC News. https://abcnews.go.com/Business/mgm-reeling-cyber-chaos-5-days-after-attack/story?id=103148809
10. MGM Resorts says cyberattack cost $100 million, resulted in theft of customer info. The Record from Recorded Future News. (2023, October 6). https://therecord.media/mgm-resorts-cyberattack-cost-millions
11. Arntz, P. (2023, November 20). Scattered spider ransomware gang falls under government agency scrutiny. Malwarebytes. https://www.malwarebytes.com/blog/news/2023/11/scattered-spider-ransomware-gang-falls-under-government-agency-scrutiny
12. U.S. cybersecurity agencies warn of scattered spider's Gen Z Cybercrime Ecosystem. The Hacker News. (2023, November 20). https://thehackernews.com/2023/11/us-cybersecurity-agencies-warn-of.html

13. MGM and Caesars Hackers: Who are they? | Cybernews. (n.d.). https://cybernews.com/editorial/mgm-caesars-explained-scattered-spider/
14. Zurier, S. (2023, November 14). FBI takes heat from industry for not making arrests in MGM-Caesars cases. SC Media. https://www.scmagazine.com/news/fbi-takes-heat-from-industry-for-not-making-arrests-in-mgm-caesars-cases
15. Red Canary | Your managed detection and response ally. (n.d.-b). https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
16. Ahl, I. (2023, November 9). LUCR-3: Scattered spider getting SAAS-y in the cloud. LUCR-3: Scattered Spider Getting SaaS-y in the Cloud. https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud
17. Manson, K., & Tarabay, J. (2023, September 11). MGM resorts says it shut down some systems after cyberattack. Bloomberg.com. https://www.bloomberg.com/news/articles/2023-09-11/mgm-resorts-says-it-shut-down-some-systems-following-cyberattack
18. Morrison, S. (2023, September 15). The chaotic and cinematic MGM Casino Hack, explained. Vox. https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware
19. Coleman, J. (2023, September 15). Okta CEO on MGM Breach: Companies are under “Massive attack from Cybercriminals.” CNBC. https://www.cnbc.com/2023/09/15/okta-ceo-on-mgm-breach-companies-under-attack-from-cybercriminals.html
20. Dow Jones & Company. (2023, October 6). WSJ News Exclusive | MGM Resorts refused to pay ransom in cyberattack on casinos. The Wall Street Journal. https://www.wsj.com/tech/cybersecurity/mgm-resorts-refused-to-pay-ransom-in-cyberattack-on-casinos-3a53fa6d