Threat Intelligence Report

Devan Rajendran drajendr@andrew.cmu.edu

On September 11, 2023, MGM Resorts International was the victim for a significant cyberattack orchestrated by the threat actor group Scattered Spider, known to be affiliated with the ALPHV or BlackCat ransomware group. This attack was a combination of ransomware and data exfiltration and had wide-reaching impacts on MGM's financial stability, operations, and reputation. The incident reportedly caused an $8.4 million loss in daily revenue and was expected to result in a $100 million impact in the company's 3rd quarter. Beyond the financial costs, the attack disrupted essential operations at MGM properties, including online reservations, digital room key systems, and casino functionality, which led to long lines and considerable inconvenience for guests and staff. Additionally, the attackers reportedly stole personal identifiable information (PII) such as names, contact information, gender, date of birth, and driver's license numbers, compromising customer confidentiality and potentially damaging trust in MGM Resorts.

The attack was enabled through tactics involving social engineering, specifically vishing, to impersonate MGM employees and obtain critical access credentials. The attackers exploited the opportunity of gaining information from publicly available sources, mainly LinkedIn profiles, to effectively impersonate an employee, allowing them to bypass weak identity and access management (IAM) controls within MGM's systems. Once inside, the attackers utilized privilege escalation tactics to gain additional access to sensitive systems and deploy ransomware. The reason for the attack can be classified as an attempt for financial gain. By encrypting data and exfiltrating sensitive information, they compromised the confidentiality and availability of MGM's systems, aiming for financial gains through the ransom demand.

Risk analysis of this incident, and a similar attack on Caesar's Entertainment, suggests a high probability of similar exploitation attempts in the future, especially given Scattered Spider's effective use of social engineering and MGM's apparent IAM weaknesses. The attack showed the weaknesses in the system such as untrained professionals and a lack of multi-faceted defense strategy, and the effect that such a hack can have on the loss of customer trust and the brand reputation. The attackers' sophisticated methods underscore the need for stronger security measures to protect sensitive information and critical systems from similar vulnerabilities.

In response, MGM Resorts could benefit from several preventive strategies. Implementing robust security awareness training for all employees would improve resilience against social engineering attacks, such as phishing and vishing. Enhancing IAM protocols, including multi-factor authentication (MFA) configurations and periodic audits, would add further protection against unauthorized access. Regular vulnerability assessments and penetration testing are also crucial to identify and address weaknesses within the network. Additionally, real-time monitoring and a clearly defined incident response plan would help detect and mitigate threats early, potentially preventing similar incidents from escalating to the level of impact experienced in this case.

In summary, this cyberattack highlights the need for organizations to adopt a multifaceted security approach that addresses both technical vulnerabilities and human factors. Through more comprehensive defense strategies and employee training, MGM and similar organizations can work toward preventing similar attacks in the future.

References

Sarah Braithwaite, “ALPHV: Hackers Reveal Details of MGM Cyber Attack”, 24 Oct 2023, https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/

Eddy Berry, “Lessons Learned from the MGM Cyberattack”, 02 May 2024, https://www.tracesecurity.com/blog/articles/lessons-learned-mgm-cyberattack

Brian Ahern , Executive Director, Communications, “MGM Resorts Update On Recent Cybersecurity Issue”, 5 Oct 2023, https://investors.mgmresorts.com/investors/news-releases/press-release-details/2023/MGM-RESORTS-UPDATE-ON-RECENT-CYBERSECURITY-ISSUE/default.aspx

Team ZCySec, “MGM Resorts Data Breach FAQ: What happened, Who was affected, What was the impact?”, https://zcybersecurity.com/mgm-resorts-data-breach-faq-what-happened-who-was-affected-what-was-the-impact