MGM Gambles and Loses to a Cyberattack

MGM Resorts had repeated cyber attacks, but has not learned from past mistakes, it is now an example of the rise in vishing, says Heather Stratford, Drip7 CEO.

MGM

SPOKANE, WASHINGTON, UNITED STATES, September 21, 2023 /EINPresswire.com/ -- On Sept 11th, 2023, MGM Resorts International, a renowned hospitality and entertainment company with a prominent presence in Las Vegas, fell victim to a devastating ransomware attack. They initially reported that a “cybersecurity issue” was affecting some of its systems.

The attackers' successful infiltration is still in progress and currently has cost MGM a reported $52 million financial loss as well as disrupted their day-to-day operations. Hotel bookings, reservations, and guest information were compromised, leading to significant reputational damage for the company. The fallout from this attack has been staggering with crippling losses to revenue and no end in sight.

> “The training of all people with access to digital systems is essential and why Drip7 was founded. Regular cyber training can build a culture shift, with people as the first line of cyber defense.”
>
> *Heather Stratford, Drip7 Founder and CEO*

MGM had previous cyber attacks and the third-party cybersecurity firm Boston-based Bitsight had given them an “F” grade for their patching cadence.[1] MGM had a 2019 breach that was disclosed in 2020 where hackers stole sensitive data from about 10.5 million MGM customers. The data from that breach was marketed and sold on the dark web. BetMGM, owned 50 percent by MGM, had a disclosed breach in May of 2022.[2]

Could the recent attack have been prevented? Both internal and external people will be debating that question for the next several years. But what we do know is that MGM’s cyber posture was not adequate. They had repeated breaches and failing to adequately train their employees, they suffered the largest attack vector for any organization.

MGM continued to have cyber issues because they didn't significantly address cyber weaknesses and learn from their mistakes. “This is why the training of all people with access to the digital systems is essential and why Drip7 was founded,” states Heather Stratford, CEO/Founder of Drip7. “Regular cyber training and reinforcement in a gamified environment can build a culture shift, deploying people as the first line of cyber defense.”

The Rise of Vishing

The current MGM cyber attack has been reported to be from Scattered Spider that used a Ransomware-as-a-service (RaaS Model) known as ALPHV or BlackCat. The attack was a combination of ransomware and vishing. Vishing is a form of social engineering that involves manipulating individuals into revealing confidential information over the phone. In the case of MGM, it's believed that attackers used vishing techniques to gain access to the company's internal systems.

Specifically, “the hackers found an employee’s information on LinkedIn and impersonated them in a call to MGMs help desk to obtain credentials.”[3] It all comes down to passwords and access. It took 10 minutes to successfully make the attack. This highlights the growing trend of cybercriminals using various methods beyond traditional phishing emails to breach organization defenses. As technology evolves, so do the tactics employed by malicious actors.

The impact of the breach will have ripple effects. First, impact on daily revenue. “Cybersecurity issues” have silenced slot machines and shut down internal computer systems, costing the hotel and casino chain as much as $8.4 million per day in daily revenue, reports The New York Post.[4] Moody’s Corporation has stated that due to MGM’s heavy reliance on computers for much of its operations, its credit rating could go down as a result of the cyberattack.[5]

Caesars Entertainment, also in Las Vegas, had a breach and reportedly paid millions in ransom. “Caesars admitted to the breach in a filing with the Securities and Exchange Commission on September 14, 2023, where it says an ‘outsourced IT support vendor’ was the victim of a ‘social engineering attack’ that resulted in sensitive data about members of its customer loyalty program being stolen.”[6]

According to Forbes, both companies are now statistics in a worldwide trend. Cyberattacks were up globally 156 percent in the second quarter of 2023 compared to the first three months of the year, according to a report from the World Economic Forum.[7]

Phishing is still the start of more than 90 percent of cyber attacks. But according to the IBM report X-Force Threat Intelligence Index 2022 when phone calls or vishing is laid over traditional phishing the attack is three times more likely to succeed. When we talk to people, we build trust with them. And that is what Scattered Spider or any other criminal cyber group is hoping for.

FBI Director Christopher Wray in his September 18, 2023 address at the Mandiant/mWISE 2023

Cybersecurity Conference, invited the private sector to work collectively with the government to stay ahead of the threat of cyber attacks.[8]

The introduction of artificial Intelligence in attacks is helping criminals leverage more social media data faster and help develop a more complete picture of their targets. The key to making an attack successful is often knowing more about a company, what systems they use and the culture they have in place. It's a straight play from the old movie by Robert Redford and Paul Newman, "The Sting." Clever impersonation to gain access to what you want using any means necessary to complete the deception.

The MGM Resorts International Las Vegas ransomware attack is a cautionary tale for organizations worldwide. It underscores the evolving tactics of cybercriminals, the dangers of vishing, and the audacity of ransomware groups like Scattered Spider. As the world becomes increasingly interconnected, it is imperative that organizations prioritize robust cybersecurity measures and incident response plans to defend against and mitigate the impact of such devastating attacks. It is critical to determine the lessons we learn from all the breaches in 2023. The attacks are shifting, and both the big and small targets are falling.

Heather Stratford is a national thought-leader in the Training and Cybersecurity fields. She is the founder and CEO of Drip7, a gamified microlearning platform for cybersecurity, compliance education and onboarding. She has started and exited several technology companies. Heather has written and been quoted in many media outlets, spoken at conferences, and been a trainer at events. She has consulted and spoken for multiple U.S. government agencies, State and Local governments, higher education, enterprise level businesses including fin/tech. Heather is a an Adjunct Professor at Whitworth University.

1. https://www.casino.org/news/mgm-had-f-cybersecurity-grade-prior-to-ransomware-attack/
2. https://www.securityweek.com/betmgm-confirms-breach-hackers-offer-sell-data-15-million-customers/
3. https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware
4. https://nypost.com/2023/09/18/mgm-losing-up-to-8-4m-per-day-over-cybersecurity-issue/
5. https://www.businessinsurance.com/article/20230914/NEWS06/912359825/MGM-Resorts-breached-by-%E2%80%98Scattered-Spider%E2%80%99-hackers-Sources
6. https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware
7. https://www.forbes.com/sites/suzannerowankelleher/2023/09/14/2-casino-ransomware-attacks-caesars-mgm/?sh=2035c857402d
8. https://www.fbi.gov/news/speeches/director-wrays-remarks-at-the-mandiantmwise-2023-cybersecurity-conference

Deb McFadden
Drip7

+1 509-703-5400
PR@drip7.com
