Peter MacMillan

CS 462-14779

December 3, 2023

Data Breach and Cyber Attacks on Las Vegas' Biggest Casinos

Earlier this fall, both MGM Grand and Caesar's Palace experienced similar data breaches and had a lot of data leaked. Most of this information was loyalty member's account information and several pieces of PII. This has shown that even places that we think have top-notch security systems in place, they are vulnerable to attacks just like the rest of us.

Ransomware and Social Engineering

In order to know what happened during this event, we must know what a ransomware attack is and how it works. This type of attack is applied when a type of malware infects a computer or network system. This malware steals and locks access to important information from all users who are part of the system. Only the person who can get past the encryption created by the malware is the same one that unleashed the malware itself. The idea around the ransomware attack is that the hacker or perpetrator demands some sum of money to then give back the information and access back to the users. This type of attack has become increasingly popular in recent years and has cost several companies billions of dollars in damages.

Another thing to be wary of is social engineering, a known technique used by people and hackers alike. The premise of social engineering is obtaining information from an individual and using that information to gain access to a system illegitimately. This technique solely relies on and exploits human error by manipulating or goading the target into revealing private

information, access, or valuables. (What is social engineering?) There are several ways to induce social engineering, including posing as a government agency or authority figure, even posing as a trusted brand. This can be used further, and perpetrators can pose as employees or people businesses have contracts with and can be exposed to these attacks if they are not careful.

Who was behind the Attack?

Moving on, we will now take a look at the group that was allegedly behind both attacks on the casino giants. A group called Scattered Spider, an affiliate of ALPHV/BlackCat, are the ones responsible for the attacks. According to the FBI and CISA, this group is comprised of threat actors that are considered experts in social engineering and use several techniques to gain access (Scattered Spider, CISA). This group is known to target larger companies and their contracted information technology help desks. Members of this group are known to use several social engineering techniques in order to gain access to systems. These are but a few of them; phishing, push bombing, and SIM swap attacks. We all know that phishing is posing as a trusted entity and gaining access to systems through bogus emails or web pages. Once they have gained access to a system it can be rather difficult to flush them out completely. Push bombing is comparable to an overflow in a few aspects. This type of attack repeatedly sends and triggers login attempts versus a single-sign-on portal or public apps or services. The objective of this is to have the target become tired of the notifications or make a mistake and allow access. SIM swapping, or SIM jacking, is defined as illegally taking over a user's cell phone number. Common methods of this include tricking the phone carrier to port the number to a new SIM that is under the control of the adversary. This can allow an attacker to gain access through an internet connected phone and allow themselves to breach a network if they know how to do so.

Groups like these are well equipped with knowledge and tools to enact attacks and breaches such as these.

What happened in the MGM Grand Casino Attack?

This attack, to me, is a marvel and begs the question, "how secure are our systems really?" During this attack, Shattered Spider implemented a ransomware attack after gaining access to the systems in the casino. This is just a standard attack vector, and it proved costly as about $100 million worth of damages was caused. The kicker was the fact that it only took a 10-minute phone call for this group to gain access to the records of tenants and residents staying at the resort. This group is also especially good at a technique dubbed "vishing" which is gaining access to a system through a convincing phone call rather than having to rely on emails to gain access (Morrison, the chaotic and cinematic MGM Casino Hack, explained). What happened goes as follows: the hackers picked an employee and then found their information on LinkedIn. The hackers then impersonated them to call MGM's IT help desk to obtain credentials to access and infect the systems. This may have been the fastest way to breach a system in quite a while.

What happened in the Caesar's Palace Casino Attack?

While I cannot say the same thing happened during this attack, a more well-known method occurred and was the cause of the breach in question. This was the work of a social engineering attack. According to a report, an outsourced IT vendor was caught in a social engineering scheme, and it resulted in unauthorized access to Caesar's network and the exfiltration of data, which included personal information of state residents (Velotta, Caesars releases new details on Cyberattack). This indeed was a ransomware attack as well and it was reported that Caesar's did end up paying about $15 million to the hackers to have the situation

under control. The exact range of what data was stolen is still up in the air, however, we do know that the loyalty program database was leaked, but no payment information was accessed (Ikeda).

What was the Root Cause for the Attack?

People may be asking; how did this happen or why did this happen? These questions are not easily answerable, but it proves that companies and other entities are still vulnerable to cyberattacks of any variety. There doesn't appear to be any sort of motivation as to why this attack occurred. This type of attack shows us that social engineering continues to be a prevalent method of gaining access to computer and network systems. As far as ransomware attacks go, they have been becoming more and more frequent as of late. Several companies this year have fallen victim to them, having to shell out large sums in order to get that information back.

How was the public affected by the Attack?

The general public was horrified to know that some of their information was being held hostage or even leaked out onto the dark web. It may not have had the societal backlash as some of the more important and devastating cyber-attacks that have occurred this year, but it still stands to be one of the more impressive feats of hacking this year. This attack puts into perspective how vulnerable we really are and how small things such as phone calls and subtle conversations can turn the tide and allow someone to gain access illegitimately.

What was the Timeline of both Attacks?

The overall timeline for these attacks took place from September 7 to September 18 of 2023. The social engineering attack was launched against the vendor employed by Caesar's Entertainment on September 7th. Four days later, on the 11th, MGM resort releases a statement saying, "a cyber security incident" has affected company systems. On September 12th, another

statement is released by MGM that reports that all “resorts including dining, entertainment, and gaming are still operational” and that they are able to access their hotel rooms. They made a mention that all front desk staff was ready to assist if needed (Powell). On the same day, guests report a number of issues with the online booking system. It was reported that their website was down. September 13th was the day where VX Underground, through a post on X, saying that the MGM attack was the result of vishing and that ALPHV was responsible for the attack. The same day, sources close to the attack said that Scattered Spider was responsible for the hack. A report from Moody’s, a financial services company, said that the attack may negatively impact the credit of MGM and highlighted key risks on MGM’s heavy reliance on technology (Powell). September 18th, a few reports came out saying that both hacker groups were working together in order to launch the attack against the casino titans. Okta, an IT service management company, reported that five of its clients, most notably MGM and Caesar’s, were victims of the hacking groups since August 2023 (Powell).

How is this Attack still Relevant Today?

As mentioned above, this attack shows how human error and social engineering techniques can unhinge an entire corporation or entity in no time flat. With society’s ever-increasing reliance or dependency on technology, these attacks may become more and more frequent. This goes to show no matter how secure you think your systems are, there will always be a flaw in that security. It just takes one person to isolate that flaw and expose it. There is no real way to keep anything 100% secure but there are practices that can make it easier. Some that are being implemented are proper training against phishing and vishing emails and calls. Proper knowledge of both can assist in the mitigation of cyberattacks in the future. Another possible defense is to maintain dual or multi-factor authentication. This would ensure that there are

several layers someone would have to go through in order to access something vs having a one-way road right to it. MFA still has not been perfected but strides are being made to shore up and improve it.

Conclusion

The two cyberattacks on the world's largest casinos spurred a little fear in the eyes of the public. While their systems would not be considered critical infrastructure, you could look at it in that way. Imagine if hackers were to turn to our state or even national frameworks. Both of these attacks outline the importance of understanding what social engineering is and how to recognize it. Ransomware attacks are some of the most volatile attacks that can be administered towards computer and network systems. They are becoming more and more prevalent in today's world. The use of IDS, intrusion detection systems, and IPS, intrusion prevention systems, could pave the way towards eliminating and mitigating this type of attack. This threat to the internal frameworks of corporations and threat to leaked PII happened over a span of 11 days: September 7th to September 18th. This attack showed us that we as a society can be too dependent on technology and not pay attention to what is around us. Another thing that these attacks has taught us is that human error is as important as ever and continues to be an issue for society to control.

Ikeda, Scott. “Caesars Entertainment Discloses Cyber Attack, Ransom Payment Made Weeks before MGM Heist.” *CPO Magazine*, 18 Sept. 2023, www.cpomagazine.com/cyber-security/caesars-entertainment-discloses-cyber-attack-ransom-payment-made-weeks-before-mgm-heist/.

Morrison, Sara. “The Chaotic and Cinematic MGM Casino Hack, Explained.” *Vox*, 15 Sept. 2023, www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware.

Powell, Olivia. “A Full Timeline of the MGM Resorts Cyber Attack.” *Cyber Security Hub*, 27 Sept. 2023, www.cshub.com/attacks/news/a-full-timeline-of-the-mgm-resorts-cyber-attack.

“Scattered Spider: Cisa.” *Cybersecurity and Infrastructure Security Agency CISA*, 1 Dec. 2023, www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a.

Velotta, Richard N. “Caesars Releases New Details on Cyberattack.” *Journal*, Las Vegas Review-Journal, 10 Oct. 2023, www.reviewjournal.com/business/casinos-gaming/caesars-releases-new-details-on-cyberattack-2918145/.

“What Is Social Engineering?” *IBM*, 2022, www.ibm.com/topics/social-engineering.