MGM Ransomware Attack

Posted by Mike Heumann, September 19, 2023

The MGM Casino was hacked into on 9/11-9/12 2023 by a group known as Scattered Spider using ALPHV. ALPHV is a Ransomware as a Service (RaaS) threat actor that emerged onto the hacking scene in 2021. The attack was a social engineering 'vishing' attack, a type of phishing that relies on calling victims to access computer systems. The Scattered Spider group contacted MGM IT employees to get them to provide them with system access, using an MGM employee's personal information (taken off of LinkedIn) to impersonate them. From there, the group stole and encrypted MGM's data, demanding crypto payments in return for releasing the data.

"There's always a little back door, and all the best defenses and all the expensive tools can be fooled by one good social engineering attack," - Peter Nicoletti

The attack has paralyzed the MGM for the past week. The MGM slot machines have been taken offline, hotel staff have been forced to check in guests manually leading to long lines, guests were locked out of their rooms as their room card keys no longer worked (forcing hotel staff to hand out physical room keys), and staff have been hand writing casino winnings receipts for customers. Additionally, MGM employee paychecks are late due to the digital shutdown.

Wendi Whitmore, senior vice president at Palo Alto Networks, is currently investigating multiple breaches connected to the hacking group. She explained that hackers will "...typically try to get a password reset by calling the help desk: 'I've been traveling, I've just come back from vacation' — some sort of a ruse that's plausible enough," she said. "A lot of help desks have metrics on being able to resolve an incident quickly." Such metrics, while good at ensuring that IT teams are responsive, are incentives that encourage IT teams to hurry and give people credentials instead of properly

investigating the caller. Another wrinkle in the operation is that Scattered Spider is made up of native English speakers, making the attacks more believable, in this instance, than if they had a non-native English accent.