

## **Forbes - Inside The Ransomware Attack That Shut Down MGM Resorts**

Article Link

- ALPHV/BlackCat claims responsibility
- Damages included most electronic systems
  - “wreaked havoc on MGM’s operations, forcing guests to wait hours to check in and crippling electronic payments, digital key cards, slot machines, ATMs and paid parking systems.”
- Social engineering attack using an MGM IT personnel identity found on LinkedIn
  - The attack took about 10 minutes to execute
- Likely a ransomware attack due to “the high visibility of the disruption.”
- Estimated that the properties effected bring in \$13 million daily
  - The article was written more than 60 hours after the attack, with systems still down at the time of publishing.

## **Reuters - MGM Resorts breached by ‘Scattered Spider’ hackers: sources**

Article Link

- The group, Scattered Spider (UNC3944), is given credit for the attack
- Caesars Entertainment had been attacked with ransomware recently
  - They paid the ransom
- Shares of Caesars Entertainment and MGM both fell as a result of the attack on MGM
- Used social engineering to obtain login credentials or one-time-password codes
- Likely a ransomware attack
- Recommends that other casinos should be on high alert watching for hackers trying to cash in on the hype while the attack is in recent memory

## **Forbes - 2 Casino Ransomware Attacks: Caesars Paid, MGM Did Not**

Article Link

- Caesars was attacked only weeks before MGM
- MGM’s website and mobile app offline for nearly four days
- Cyberattacks up over 150% globally in the second quarter of 2023 compared to the first
- The group ALPHV/Black Cat claimed responsibility for MGM attack
  - The group Scattered Spider is affiliated and hit Caesar’s
- The social engineering attack took 10 minutes to execute
  - The MGM company support desk was called after an MGM tech employee was identified on LinkedIn.
  - Caesar’s attack was also social engineering

- “Threat actors often determine a ransom sum after researching a company’s financial documents, going so far as to determine its insurance coverage limit beforehand.”
- Reputation is important to these types of groups, so if ransom is paid, the attackers typically live up to their promises.
  - Conversely, giving them the money encourages more attacks
- As of the time of writing (September 14th) the MGM Resorts website had been down for about 85 hours.