How a Simple LinkedIn Search Took Down a Multi-Billion-Dollar Casino Enterprise

Aidan Sharpe

December 18, 2023

2023-12-18

How a Simple LinkedIn Search Took Down a Multi-Billion-Dollar Casino Enterprise

Aidan Sharpe

December 18, 2023

Slides with a gray background, appearing in this right-hand column are speaker notes slides. The audience would ever only see the slides in the other column with a white background. This gives the speaker access to additional information, key points, and sources for those points. The speaker notes and the presentation content should be taken into account.

The Victims


MGM RESORTS INTERNATIONAL®

The MGM Resorts website is currently unavailable.

We apologize for the inconvenience.

To make a hotel reservation at any of our destinations, please call 855-788-4775.

MGM Rewards members may call Member Services from 6 AM to 11 PM Pacific time at 866.761.7111.

To contact a concierge, please call:

Aria	702.590.9520
Beau Rivage	228.386.7111
Bellagio	702.693.7075
Borgata	609.317.1000
The Cosmopolitan of Las Vegas	877.893.2003
Delano Las Vegas	702.632.4760
Empire City Casino	866.745.7111
Excalibur	877.660.0660
Luxor	702.632.4760
Mandalay Bay	702.632.4760
MGM Grand Detroit	877.888.2121
MGM Grand Las Vegas	877.660.0660
MGM National Harbor	844-646-6847
MGM Northfield Park	330.908.7625
MGM Springfield	413.273.5000
New York-New York	702.740.3311
NoMad Las Vegas	702.730.7010
Park MGM	702.730.7010
Vdara	702.590.9520

Thank you for your patience.

Figure: A screenshot of the MGM Resorts website following the attacks

The Victims

Figure: A screenshot of the MGM Resorts website following the attacks

- Hackers took MGM Resorts offline in mid-September of this year
- According to Forbes - *Inside The Ransomware Attack That Shut Down MGM Resorts*, the attack "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 with LinkedIn

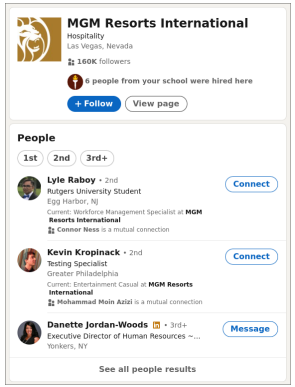

Figure: LinkedIn gives everyone easy access to employee information

Social Engineering with LinkedIn

Figure: LinkedIn gives everyone easy access to employee information

- LinkedIn allows anyone to see employees and their positions
- Hackers contacted a help desk to obtain login credentials or one-time codes using an employee identity, according to Reuters - *MGM Resorts breached by 'Scattered Spider' hackers: sources*.
- Once hackers obtained IT credentials, they had access to anything that IT personnel had access to. Usually, IT have fairly extensive privileges.
- Such high privileges caused tremendous damages

The Damages

- Likely ransomware attack
- Widespread network outages
- Digital payment systems and slot machines down
- Rough figures put damages over $40 Million

└The Damages

The Damages

- Likely ransomware attack
- Widespread network outages
- Digital payment systems and slot machines down
- Rough figures put damages over $40 Million

- Due to the "high visibility of the disruption", the attack was likely ransomware. This leads to system outages, data loss, and ultimately revenue loss
- According to Forbes - *2 Casino Ransomware Attacks: Caesars Paid, MGM Did Not*, at the time of writing, the MGM website had been down for about 85 hours.
- According to Forbes - *Inside The Ransomware Attack That Shut Down MGM Resorts*, the affected properties had revenues of about $13 Million per day.

Hackers

- Group was unclear at first
- Scattered Spider initially given credit
- ALPHV / Black Cat claimed responsibility

Hackers
- Group was unclear at first
- Scattered Spider initially given credit
- ALPHV / Black Cat claimed responsibility

- Initially it seemed like sources disagreed on the group behind the attack, but it was the complexity of the hacking world that led to the confusion.
- Prior to the MGM attack, the another casino enterprise, Caesar's, was hit with ransomware and paid the ramsom. The group behind this attack was Scattered Spider (UNC3944), according to Reuters.
- When MGM was attacked Scattered Spider was a top suspect, but the affiliated group, ALPHV / Black Cat claimed responsibility, according to Forbes.

Lessons Learned

- Employee identity verification
- Effective attacks can be simple
- Backup everything!

Lessons Learned
- Employee identity verification
- Effective attacks can be simple
- Backup everything!

- Taking privileges away from IT makes the job of IT unreasonably difficult. Implementing an employee identification system would ensure that credentials and one-time codes are only given to authorized people.
- Another important takeaway is that social engineering attacks do not have to be complex to be effective. Allocating resources to prevent social engineering attacks with proper protocols makes simple attacks a lot more difficult.
- Ransomware attacks usually result in tremendous data loss. If proper isolated backup systems are put into place, the amount of data loss can be minimized drastically.

References

- Forbes - Inside The Ransomware Attack That Shut Down MGM Resorts
- Forbes - 2 Casino Ransomware Attacks: Caesars Paid, MGM Did Not
- Reuters - MGM Resorts breached by 'Scattered Spider' hackers: sources

References

- Forbes - Inside The Ransomware Attack That Shut Down MGM Resorts
- Forbes - 2 Casino Ransomware Attacks: Caesars Paid, MGM Did Not
- Reuters - MGM Resorts breached by 'Scattered Spider' hackers: sources