MACRO PRAXIS | Research Institute

Turn Back Time (TBT) – Breach Analysis

MGM RESORTS BREACH

ANALYSIS AUTHOR: Bobby Boughton, MacroPraxis Research Institute Fellow

PUBLICATION DATE: April 10th 2024

BREACH: MGM RESORTS RANSOMWARE ATTACK – 2023

MITRE ATT&CK FRAMEWORK													
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
				Potential Deception Discovery				Actual Breach Discovery					

Breach Information:	
Breach Date:	**2023**
Breach Name:	**MGM ransomware attack**
Target Name:	MGM Resorts International
Attacker Name:	Scattered Spider and ALPHV (also known as BlackCat)
Type of Attack:	Social Engineering / Ransomware
Impact of Attack (1):	MGM did not pay the ransom. Chose prolonged outage and rebuild.
Impact of Attack (2):	The company reported that the attack resulted in approximately $100 million in lost revenue during the third quarter of 2023. Additionally, MGM incurred approximately $10 million in one-time expenses related to consulting services, legal fees, and other costs associated with the incident.
Impact of Attack (3):	In response to this incident, MGM Resorts agreed in January 2025 to a $45 million settlement to resolve multiple class-action lawsuits related to data breaches in 2019 and the 2023 ransomware attack.
Total Impact:	**$155M**

#	Tactics for MITRE ATT&CK:	Attack Tactics Description:	Security FAILURE:	Deception TECH:
1	Reconnaissance	The hacker group Scattered Spider utilized social engineering techniques to gather information about MGM employees. They specifically targeted individuals by collecting personal details from platforms like LinkedIn, which allowed them to	No direct failure	

		impersonate employees convincingly. This impersonation enabled the attackers to deceive MGM's IT help desk into resetting credentials, granting them unauthorized access to the company's internal systems.		
2	Resource Development	The attackers most likely: 1) Collected or purchased leaked credentials from previous breaches, 2) Used pre-existing infrastructure (such as cloud-based tools) to execute the attack, and 3) Acquired social engineering knowledge from past experience attacking other companies.	No direct failure	
3	Initial Access	The attackers employed social engineering techniques, specifically targeting MGM employees through phone-based phishing (vishing), to obtain valid user credentials.	MFA / Help Desk Training	
4	Execution	Utilizing the compromised credentials, the attackers executed malicious code within MGM's network to establish their presence.	EDR / PAM	
5	Persistence	They implemented mechanisms to maintain access, such as creating new user accounts or modifying existing ones.	IAM / PAM	Honey Tokens & Honey Token Accounts
6	Privilege Escalation	The attackers escalated their privileges to gain higher-level access, enabling broader control over the network.	IAM / PAM	Honey Tokens & Honey Token Accounts
7	Defense Evasion	Techniques were used to avoid detection, including disabling security tools and clearing logs.	EDR / SIEM	Decoy EDR & SIEM Services
8	Credential Access	They harvested additional credentials, possibly through methods like keylogging or credential dumping.	EDR / SIEM	Honey Tokens & Honey Token Accounts
9	Discovery	The attackers conducted internal reconnaissance to identify network structure, active hosts, and valuable assets. This is most likely when MGM started to notice unusual activity.	EDR / SIEM	Baits, Breadcrumbs & Decoys
10	Lateral Movement	Using the gathered information, they moved laterally across the network to access targeted systems (living off the land).	IDS / SIEM / Segments	Decoys & Fake RDP Sessions.
11	Collection	Data of interest, including sensitive customer information, was gathered from compromised systems. Reports indicate that they stole approximately 6 terabytes of data, including personal information such as names, contact details, dates of birth, driver's license numbers, passport numbers, and Social Security numbers.	IAM / MDR / SIEM	Baits, Breadcrumbs & Decoy Databases and Fake High Value Data
12	Command & Control	The attackers employed command and control (C2) software to maintain persistent access to MGM's systems. The attackers established a secondary	IAM / IR	Fake C2 Server Decoys & Deceptive

		Identity Provider (IdP) within MGM's Okta environment. This move allowed them to retain control over MGM's systems, even as the company's cybersecurity team attempted to remove their access. By setting up this secondary IdP, the attackers could issue authenticated requests, effectively maintaining their foothold within the network.		Authentication Responses
13	Exfiltration	The collected data was transferred out of MGM's network to external servers controlled by the attackers.	IDS / SIEM / IR	Fake High-Value Baits could have slowed down or stopped data theft.
14	Impact	The attackers deployed ransomware (BlackCat) to encrypt data and disrupt operations, leading to significant service outages.	EDR / SIEM	Ransomware Baits (fake encrypted files).

Key Takeaways:

1. **MGM likely detected the attack too late (during Stage 9 – Discovery), by which time attackers had already gained significant control over the network.**
2. **If deception technology had been deployed effectively, MGM could have detected the attack as early as Stage 5 – Persistence.** By planting honeytokens and fake admin accounts, MGM's security team could have received alerts about unauthorized access attempts long before the attackers moved to network reconnaissance and lateral movement.
3. **Earlier detection could have significantly reduced the financial impact** of the breach. With containment triggered at **Stage 5 instead of Stage 9**, the cost of the attack could have been **minimized or even reduced to zero**, avoiding the $155M in damages caused by downtime, legal settlements, and lost revenue.
4. **Deception technology should be integrated into a layered security approach** to act as an early-warning system, detecting and diverting attackers before they cause real damage.

Disclaimer:

The **Turn Back Time (TBT) Analysis** is a hypothetical evaluation based on publicly available breach information and industry best practices. It illustrates how deception technology could have **improved early detection and response capabilities**. However, **no cybersecurity solution can guarantee complete prevention of cyber threats**.

Deception technology is **one component of a multi-layered security strategy**, and its effectiveness depends on **deployment scope, integration with existing security tools, and evolving attack techniques**. This analysis is **for informational purposes only** and should not be interpreted as a **guarantee of breach prevention**.

The MACROPRAXIS Research Institute is **not liable for any cybersecurity incidents, financial losses, or damages** resulting from the use or implementation of deception technology. Customers are advised to conduct **independent security assessments** and integrate deception tools as part of a **comprehensive cybersecurity strategy**.