MGM Resorts Breach

C-Suite level threat review by applicable business area addressing active threats.

Phishing is a top initial attack avenue utilized by malicious actors. Phishing is when a threat actor attempts to gain access to an organization by masquerading as a trusted entity or identity. Given the centrality of identity to adversaries' attack repertoire, tools that manage identities are prime targets. It should come to no surprise then that there has been a rise in campaigns targeting Okta and its customers. The recent attacks on MGM resort and Caesars Entertainment, both Okta customers, are representative of this development. This report will delve into the MGM resort breach.

BlackCat and Scattered Spider:

BlackCat (also known as ALPHV) is a ransomware-as-a-service (RaaS) group, which means it sells predeveloped ransomware tools to affiliates. BlackCat confirmed that one of its affiliates is behind the MGM breach. That affiliate is thought to be Scattered Spider. Scattered Spider is a financially driven threat actor that has been active since at least May 2022 whose members are reportedly based in the United States and United Kingdom. The threat actor is known for its social engineering capabilities as well as its use of the Bring-Your-Own-Vulnerable-Driver (BYOVD) technique.

MGM Resorts Breach

Threat Level: High

Attack:

It is widely reported that the threat actors gained access to MGM's environment by using phishing techniques to convince service desk personnel to reset multi-factor authentication (MFA) for a highly privileged user. Once privileged access was obtained, the threat actors had many avenues of action. The actors could further escalate privileges, create accounts, and move laterally in the environment. It is being reported that the threat actors created a source identity provider which would have further expanded their ability to access applications in MGM's environment. The ability to create an identity provider is a legitimate Okta function that can only be utilized by highly privileged users. The attackers then disrupted operations by encrypting more than 100 ESXI hypervisors and exfiltrated data.

Remediation:

- Acquire just-in-time privilege capabilities. This enables an organization to temporarily grant privileged access on an as-needed basis, minimizing the likelihood that malicious actors will be able to utilize highly privileged access in attacks.
- Put in place phishing resistant authentication measures. You can find an overview of phishing resistant authentication measures here.
- Ensure your organization has response and recovery plans in place and is testing those plans annually. This will help support a swift response that minimizes the impacts of an attack.

MGM Breach Mapped to MITRE ATT&CK*

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Description
Reconnaissance	Gather Victim Org Information: Identify Roles (T1591.004)	Adversary gathered information about privileged user(s) to aid in phishing attempt.
Resource Development	Compromise Accounts (T1586) *Speculative*	It is possible the hackers had some level of compromise before calling the Help Desk, aiding in the phishing attempt for privileged access.
Initial Access	Phishing (T1566)	Convinced Service Desk personnel to re-set MFA for privileged user
Persistence	Create Account (T1136)	Created accounts to maintain access.
Persistence	Account Manipulation (T1098)	The attackers claimed to have gained global administrator privileges to MGM's Azure tenet.
Credential Access	Modify Authentication Process: MFA (T1556.006) *Speculative*	With highly privileged access, attackers could disable MFA defenses and add MFA devices.
Credential Access	Network Sniffing (T1040)	Sniffing passwords of Okta users.
Credential Access	OS Credential Dumping (T1003)	Attackers claimed to have dumped MGM's domain control hashes.
Impact	Data Encrypted for Impact (T1486)	Encrypted more than 100 ESXI hypervisors.
Exfiltration	Exfiltration (TA0010)	The threat actors claimed to have exfiltrated more than 6 TB of data.

**This is based on the best information available for use at the time (9/26/23) and is subject to change as facts come to light.*

MGM Resorts Breach:

- **Okta warns of social engineering attacks following a similar attack pattern to that of the MGM breach:** https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
- **Additional Analysis:** https://securityboulevard.com/2023/09/the-mgm-breach-and-the-role-of-idp-in-modern-cyber-attacks/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity
  - Develop playbooks of adversary TTPs

ABOUT K LOGIX
Cybersecurity Advisory and Consulting Services
Our white-glove approach empowers leaders to advance their security programs to strategically align with the business to reduce risk.