MGM Resorts International September 2023 Ransomware Attack

Incident Name	MGM Resorts International September 2023 Ransomware Attack
Date of Incident	10th September 2023
Summary	On September 11th, 2023, MGM Resorts International announced that they are currently dealing with a cyber attack that is impacting their company's systems and all 31 of their resorts, many of which are located in Las Vegas. Numerous systems are currently offline, including the main website, casino floor machines and services, reservations, and the MGM Rewards app. Customers have been instructed to contact each hotel directly using their phone numbers to address MGM rewards-related issues. As a result of this attack, customers are experiencing long queues, difficulties accessing hotel rooms, and disruptions in the casinos across all the resort hotels in Las Vegas. This incident is believed to be a ransomware attack. On September 12th, malware researchers from vx-underground revealed on X (previously Twitter) that the ALPHV ransomware group was responsible for this cyber attack. The threat actors allegedly obtained employee information from LinkedIn and then exploited helpdesk personnel through social engineering techniques to gain unauthorized access to MGM systems. It is worth noting that MGM has not confirmed these details or disclosed any plans regarding the ransom payment. Furthermore, as of now, MGM has not appeared on the ALPHV leak site. There have been unverified reports on social media suggesting that Caesars Palace in Las Vegas experienced a ransomware attack the week before and paid the ransom. However, the hotel has not officially confirmed these claims. As of September 12th, 2023, MGM has announced partial restoration of some systems. Given that this situation is still evolving, further updates will be provided in due course. It seems that targeting helpdesk employees, who typically possess elevated privileges, is becoming an increasingly popular approach for threat actors to infiltrate organizations through social engineering. Recently, Okta, a provider of identity and authentication services, issued a warning to its customers about an ongoing and sophisticated social engineering attack targeting IT service desk employees. Beginning in August 2023, multiple Okta customers reported falling victim to these attacks, which leveraged a technique known as vishing to deceive employees.
Key Social Engineering/OSINT Themes	• **Recon** - MGM employee and organizational information was harvested via LinkedIn (allegedly). The threat actor leveraged exposed employee information to conduct a social engineering attack.

	• **Vishing** - The threat actor targeted IT Help Desk personnel with high privileges with the purpose of gaining access.

Picnic's Recommended Remediations.
 	
For detailed remediations, see the Human Attack Surface Protection Framework (HASP).
	High Risk Employees
	• **HASP Framework 1.1 — Identify high value employee targets**
	  ◦ MITRE Alignment: T1589
	  ◦ NIST CSF Alignment: ID.RA-1
	• **HASP Framework 1.3 — Conduct social engineering risk assessments for high value employee targets**
	  ◦ MITRE Alignment: M1047
	  ◦ NIST CSF Alignment: ID.RA-5
	• **HASP Framework 1.5 — Establish and implement procedures for high value employee targets**
	  ◦ MITRE Alignment: M1056
	  ◦ NIST CSF Alignment: PR.IP-7
	• **HASP Framework 1.7 — Increase detection and monitoring for high value employee targets**
	  ◦ MITRE Alignment: M1040
	  ◦ NIST CSF Alignment: DE.CM-3
	
	Exposed Employee PII
	• **HASP Framework 2.1 — Identify exposed employee PII**
	  ◦ MITRE Alignment: T1589
	  ◦ NIST CSF Alignment: ID.RA-2
	• **HASP Framework 2.2 — Reduce exposed employee PII**
	  ◦ MITRE Alignment: M1056
	  ◦ NIST CSF Alignment: PR.IP-7
	
	Exposed Credentials
	• **HASP Framework 3.1 — Identify exposed work credentials**
	  ◦ MITRE Alignment: T1589.001
	  ◦ NIST CSF Alignment: ID.RA-2
	• **HASP Framework 3.7 — Restrict service account access**
	  ◦ MITRE Alignment: M1026
	  ◦ NIST CSF Alignment: PR.AC-4
	• **HASP Framework 3.8 — Monitor for account takeover (including real time alerts on exposed credentials)**
	  ◦ MITRE Alignment: DS0028
	  ◦ NIST CSF Alignment: DE.CM-3
	• **HASP Framework 3.9 — Monitor for MFA configuration changes**
	  ◦ MITRE Alignment: M1032
	  ◦ NIST CSF Alignment: DE.CM-3
	• **HASP Framework 3.10 — Monitor for new MFA registrations**
	  ◦ MITRE Alignment: DS0028
	  ◦ NIST CSF Alignment: DE.CM-3
	
	Exposed Remote Services
	• **HASP Framework 4.2 — Identify exposed shadow IT**

	◦ MITRE Alignment: T1133 ◦ NIST CSF Alignment: ID.AM-4 • **HASP Framework 4.4 — Manage shadow IT / remote access** ◦ MITRE Alignment: M1030 ◦ NIST CSF Alignment: PR.AC-3 **Indicators of Attack** • **HASP Framework 7.1 — Monitor for suspicious external accounts** ◦ MITRE Alignment: T1585.001 ◦ NIST CSF Alignment: DE.CM-7 • **HASP Framework 7.2 — Request takedowns for suspicious external accounts** ◦ MITRE Alignment: M1056 ◦ NIST CSF Alignment: PR.IP-7 • **HASP Framework 7.3 — Alert your organization about suspicious external accounts** ◦ MITRE Alignment: DS0021 ◦ NIST CSF Alignment: RS.MI-3 • **HASP Framework 7.4 — Monitor for suspicious domains** ◦ MITRE Alignment: T1583.001 ◦ NIST CSF Alignment: DE.CM-7 • **HASP Framework 7.5 — Block suspicious domains** MITRE Alignment: DS0038 NIST CSF Alignment: PR.AC-4 **Cyber Awareness** • **HASP Framework 8.1 — Train employees on social engineering attacks** ◦ MITRE Alignment: M1017 ◦ NIST CSF Alignment: PR.AT-1 • **HASP Framework 8.2 — Provide employees social engineering phishing simulation training** ◦ MITRE Alignment: M1017 ◦ NIST CSF Alignment: PR.AT-1 • **HASP Framework 8.4 — Build and establish social engineering policies, processes, and procedures** MITRE Alignment: N/A NIST CSF Alignment: PR.IP-1
Industry	Hospitality
Actor	Suspected to be ALPHV ransomware group
Motivations	Financial
Related Hacks	Marriott (2022) / IHG (2022), Luna Hotels & Resorts (2023)
Breach Notice/Company Notice	MGM Resorts on Twitter MGM Resorts on Twitter
Other Sources	vx-underground on Twitter

	MGM Resorts shuts down IT systems after cyberattack MGM Resorts Suspends IT Systems Following Cyber Incident MGM cyberattack claimed by ALPHV/BlackCat ransom gang | Cybernews Hotel giant Marriott confirms another data breach IHG attackers phished employee to deploy destructive wiper | Comput... Luna Hotels & Resorts Cyber Attack Highlights Threat to Hospitality Industry Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum