CRYTICA SECURITY

If you can't detect, you can't protect.™

MGM BREACH

CASE STUDY

Date of Attack: Unknown at this time, but the attack was identified on September 10, 2023

Malware Type: Ransomware levied against more than 100 ESXi hypervisors.

Cost of Breach: $110m

Attack Mechanism/Name:

Perpetrators: ALPHV (aka BlackCat)

The hackers were able to install multiple versions of remote monitoring and management tools. These provided them with several distinct access vectors to the infected systems.

It has been reported that at least some access was gained using social engineering. ALPHV sent messages to targeted help desk employees claiming the need to reauthenticate their identities or update account information.

Damage Caused: The incident impacted MGM's website, casinos, and systems used for email, restaurant reservations, and hotel bookings, and even digital hotel room keys.

Defenses Defeated: Cybersecurity Defenses: All of the malware detection systems in place. Help Desk: End-user authentication/verification processes.

Defenses Defeated By:

- A manifest lack of any malware detection systems that can detect, at the time of infection, malware such as the "multiple versions of remote monitoring and management tools."
- A lack of malware detection systems that can detect the ALPHV malware.
- A lack of Stringent Helpdesk authentication/verification procedures.

HOW CRYTICA WOULD HAVE HELPED

Crytica would have, IMMEDIATELY upon injection, detected the remote monitoring and management ransomware, the ALPHV malware. The ransomware would then not have been permitted to remain in the infected systems to be launched at will. Upon detection, steps could have been taken to remove the ransomware before it launched. Remediation could have begun immediately, and not after the critical systems were locked up. Thus, having Crytica installed could have provided early enough detection to thwart the MGM attack; and also thwart the Caesars attack, which was perpetrated by the same group using the same MO.

info@cryticasecurity.com | 877-614-9300