GuyCarpenter

Cyber Event Analysis

RANSOMWARE WINS BIG IN VEGAS

Incident	Revealed	Victims	Responsible Parties	Intent
Targeted Ransomware	September 13, 2023	MGM Resorts, Caesars Entertainment	Scattered Spider, ALPHV	Financial Gain

Facts and Context

Last week, gaming and hospitality titan MGM Resorts International disclosed that an ongoing cybersecurity incident had paralyzed its information technology (IT) and casino operations. In addition to public statements, the USD 15 billion company reported to the US Securities and Exchange Commission (SEC) that it viewed the incident as a material risk.

Reportedly, threat actor Scattered Spider, working as an affiliate of the ALPHV ransomware group, carried out the attack using social engineering techniques as the initial entry point. In the past, Scattered Spider has impersonated IT personnel, often leveraging LinkedIn for its social engineering schemes, to convince legitimately credentialed employees to provide access by running remote monitoring and other tools. Scattered Spider accessed the MGM Resorts network as early as September 8. Once inside, the threat actor quickly captured user credentials and gained global administrative rights.

The MGM Resorts cyber incident followed closely on the heels of a similar incident where Scattered Spider targeted Caesars Entertainment. Caesars acknowledged that its attackers stole its loyalty program database, which included customer driver's license numbers and Social Security numbers. In its own SEC filing, Caesars implied that it paid an extortion demand, when it acknowledged that it took action "to ensure that the stolen data is deleted by the unauthorized actor." Notably, Caesars stated in the filing that they have found no evidence of any member passwords/PINs, bank account information, or payment card information being extracted in this breach.

While Caesars did not report any interruption to its casino operations, MGM was not able to avoid that peril. According to a statement from ALPHV, MGM attempted to evict ALPHV by taking down certain network infrastructure, which caused ALPHV to widely deploy ransomware in the network. That attack affected slot machines, automated teller machines, websites and reservation systems, and even cardkey systems, leaving some guests locked out of their rooms. In addition to pervasive encryption, ALPHV claimed to also have exfiltrated personal data. All told, the Scattered Spider hack allegedly caused 6 terabytes of combined data loss from the 2 casino and resort giants.

Key Takeaways

Ransomware Groups are Tenacious. ALPHV is a notorious ransomware operation known for providing affiliates with highly customizable malware that can encrypt a wide range of network environments. ALPHV is also a confirmed successor to the DarkSide ransomware group, which shuttered operations in May 2021 in the face of intense law enforcement pressure following its widely publicized attack

on Colonial Pipeline. DarkSide's re-emergence as ALPHV, which has never shied away from targeting large operations for high demands, reminds industry and government how difficult it is to prevent malicious activity.

Ransomware is Still a Major Peril for Insurers and Insureds. After a wave of ransomware activities starting in 2019, cyber insurance companies responded swiftly with major price hikes, as evidenced by Guy Carpenter cyber client group's average 183% cumulative rate increase since 2020. The improvement in rate adequacy and cyber hygiene have restored confidence to the cyber insurance industry and attracted new capacity. However, ransomware activity has escalated since the start of 2023, with ransom payments spiking to near the level of fourth quarter 2021. The recent headline-grabbing attacks on these Las Vegas casino resorts will again heighten the industry's attention to the ongoing threat from ransomware groups. Resulting losses for many insurers participating in the MGM and Caesars cyber towers could also lead to a more cautious approach on pricing and terms.

Need for Insurers to Address Aggregation and Volatility. While the cyber insurance industry confronts systemic risk through quantification and policy wording, insurers and insureds should view the Vegas attacks as garden-variety cybercrimes that are financially motivated. Despite the fact that Caesars and MGM Resorts fell victim to the same threat actor, which used the same ransomware and similar social engineering tactics, early evidence indicates these incidents may be classified as 2 separate events rather than a single cyber catastrophe event. Unlike systemic ransomware attacks where a self-propagating malicious code spreads across networks, the Vegas attacks involved, through individual targeted reconnaissance efforts, the compromise of separate systems owned and controlled by different entities. However, for insurers seeking to address portfolio volatility, losses from the MGM and Caesars claims should be considered holistically to address overall aggregation risk. Using live cases such as the Vegas attacks, Guy Carpenter is working with various stakeholders in the cyber insurance industry to strengthen the product for insureds and support the cyber market's long-term sustainable growth.

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with 3,400 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. The Company's more than 85,000 colleagues advise clients in 130 countries. With annual revenue of over $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses including Marsh, Mercer and Oliver Wyman. For more information, visit www.guycarp.com and follow us on LinkedIn and Twitter.