GuyCarpenter

MGM/CAESARS CYBER INCIDENT ANALYSIS

The cyber incidents targeting MGM Resorts (MGM) and Caesars Entertainment (Caesars) in September have been among the latest attention-grabbing headlines in cybersecurity, and for good reason.

The alleged attackers—Scattered Spider/APLHV—were able to damage networks of both companies severely and, in MGM's case, lead to operational outages lasting 10 days by some counts. Certainly, these breaches have been deserving of our attention and examination. However, when placed in the context of major cyber attacks of the last several years, they are similar to previously seen ransomware events—neither a catastrophic event nor a broadly market-impacting one.

In recent months, we have released a Guy Carpenter event bulletin on the attacks impacting MGM and Caesars, and prior to that, a report examining correlation between major cyber events and broad stock market index performance. Our intention is to provide a framework to place the MGM/Caesar's attacks within the context of larger, major cyber event analysis.

First, we will examine the fundamentals of the attacks on MGM and Caesars, and why they lack significant scale and contagion potential. Then, we will examine the financial market conditions around the attacks and why, at the very least, it is difficult to identify a causal connection between these attacks and any meaningful shift in broader markets.

Lack of Scale

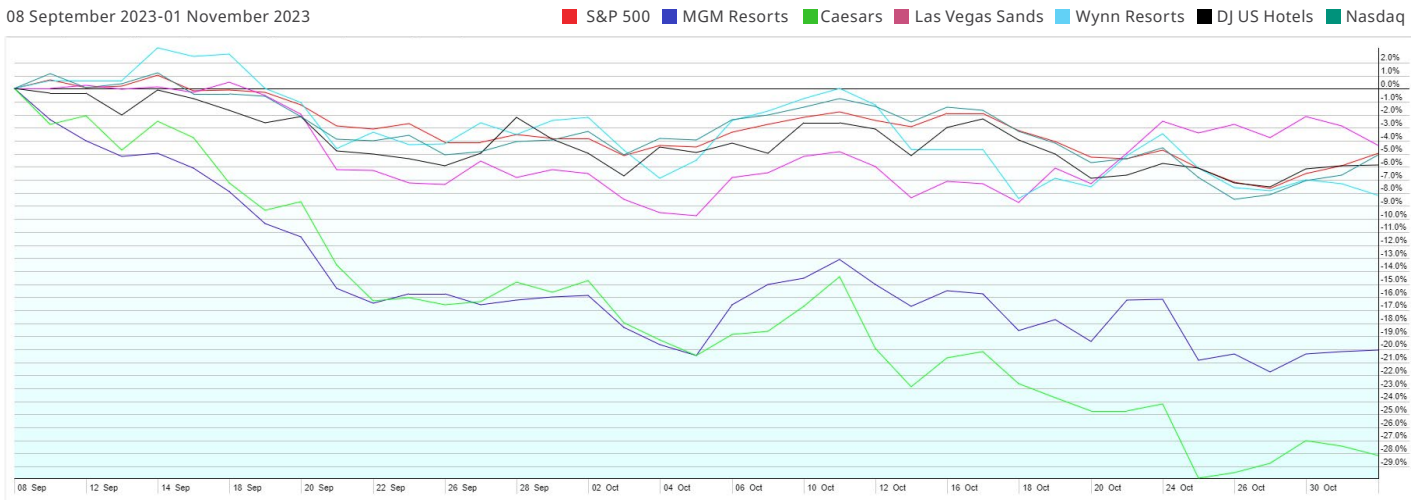
While the attacks were first reported on September 7 (Caesars)[1] and September 11 (MGM),[2] many believe in hindsight that Okta's advisory[3] on August 31 was actually the first indication of the malicious activity being performed by the attackers. This advisory warned of attackers using manual social engineering tactics to infiltrate company networks. This involved a combination of false personas on LinkedIn, combined with texting administrators and calling IT help desks. Compare this relatively high manual level of effort to a self-propagating malware incident such as NotPetya, which managed to infect hundreds of victims rapidly. While this attack was very effective against a handful of targets, it is easy to see why the attackers hit only 5 firms that Okta was able to detect[4] and were not able to scale easily to affect dozens or hundreds of victims.

Lack of Contagion

Casinos and hospitality are not in the federal Cybersecurity and Infrastructure Security Agency (CISA) list of Critical Infrastructure/Key Resources Sectors (CIKR). The impacts to MGM and Caesars are certainly significant to those firms, and the effects on employees and customers are very real, but there does not appear to have been much contagion from these attacks to other sectors of the economy, compared with an event such as Colonial Pipeline, for example. Additionally, even in cases in which CIKR has been impacted (such as with Colonial), we have seen quick rebounds and workarounds materialize to keep business running.

1. https://www.sec.gov/ix?doc=/Archives/edgar/data/0001590895/000119312523235015/d537840d8k.htm
2. https://www.cshub.com/attacks/news/a-full-timeline-of-the-mgm-resorts-cyber-attack
3. https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
4. https://www.reuters.com/technology/hackers-who-breached-casino-giants-mgm-caesars-also-hit-3-other-firms-okta-says-2023-09-19/

Figure 1: Stock and Index Prices: September 8-November 1, 2023



Source: Stockcharts.com

Standard Noise in the Markets

Figure 1 compares MGM and Caesars against the S&P 500, NASDAQ, DJ US Hotels index, and 2 other casino/hotel companies since the breaches were first announced. We can see that MGM and Caesars are clearly tracking a different path than the rest. The breaches have had significant short-term effects on the individual victim share prices, but do not appear to be dragging peers or the larger hospitality industry away from the rest of the market.

When looking at how major markets and indices have performed following these attacks, we must recognize that these attacks did not occur in a vacuum. Around the same time as the attack disclosures, markets grappled with the potential of a US government shutdown, multiple strikes in the transportation and healthcare industries, and the emergence of war in the Middle East.

In any given week or month in global markets, there are many factors at play. This is why in our *Double Whammy* analysis, we sampled more than a dozen major cyber events from across various timelines in the financial markets, to remove the effects of individual economic or financial cycles. It is possible that the casino breaches added some volatility in the immediate aftermath, but it is very unlikely that the discrete financial impacts of these breaches have singularly caused a material change in broader investor behavior or economic activity. Put another way, were these breaches (or similar ones) to occur during different economic or financial conditions, it is unlikely that they would have altered the course of the markets.

Looking Back—2021 Ransomware Events

In 2021, several high-profile ransomware attacks grabbed headlines. Most notable, of course, was the Colonial Pipeline attack in May 2021—which, while impactful, is hard to evaluate for market damage because of multiple private ownerships of the pipeline. The larger pipeline industry remained unaffected, however, and comparable stocks actually rose after the attacks.[5]

When looking at publicly traded firms that were hit by major ransomware events in 2021, we can examine Accenture, Kronos, and JBS, the meat processing company. Accenture announced in August 2021 that it had suffered a breach—and later in October, confirmed that the attackers had indeed stolen and leaked proprietary data. From August 2021 to the end of December, Accenture's share price rose roughly 30%, with no discernible effects visible to the stock after either the announcement of the breach or the confirmation of leaked data.

In December of 2021, workforce management company Kronos suffered a ransomware attack just before Christmas.[6] Multiple Kronos customers reported having to move to paper-based time tracking and other emergency measures due to the breach, as well as suffering impacts to paychecks. However, a month later, Kronos' shares had outperformed the S&P 500 over the same period, gaining roughly 3% even as the market went down 2%.

5. https://www.marketwatch.com/story/pipeline-stocks-broadly-higher-after-colonial-pipeline-ransomware-attack-2021-05-10
6. https://www.nbcnews.com/tech/security/ransomware-attack-threatens-paychecks-just-christmas-rcna8795

Finally, the attack on JBS has perhaps the most in common with recent incidents, in that it involved a confirmed shutdown of operations. In June of 2021, JBS USA suffered an attack attributed to the REvil ransomware gang, and reportedly paid the USD 11 million ransom demanded.[7] The attack disrupted US operations for the firm, shutting down 9 facilities across the US for a day while the company recovered.[8] The share price for JBS SA took a brief dip in June, but by the end of July had gained roughly 5% from the price the day of the attack notification. By October 2021, the price had risen over 11%—outperforming the S&P 500 over the same period.

Conclusions and Analysis: A Shift in the Impact of Ransomware Attacks

While notable, previous ransomware attacks and campaigns have not driven material changes in market activity beyond the short- and medium-term financial results of their victims. What we can gather from the MGM/Caesars attacks is a move toward more engaged social engineering by malicious actors. Controls such as increased multi-factor authentication (MFA) enforcement and the removal of default macros from Microsoft Office documents, for example, may have forced attackers to move away from previous tried and true attack vectors. Thus far, it appears that the recent casino and hotel breaches are simply the latest chapters in the continuing story of ransomware operations.

Recent changes in reporting timelines and transparency may be responsible for the increased public profile of these incidents. The victims in this case have made efforts to file reports in accordance with new federal Securities and Exchange Commission (SEC) rulings. This has possibly increased investor awareness of the attacks, as well as the timing and damage details. Victims of previous ransomware campaigns had more control over messaging (or omitting) the impact of incidents, perhaps dampening the short-term market reactions.

We have seen evidence of short-term reputational reactions to highly public cyber events, and we have seen some short- to medium-term reactions to extremely impactful one-time losses. However, if these types of attacks caused material long-term damage to the profitability of impacted firms, those results would show in persistent, long-running share price effects, which we have not seen.

Contacts

Anthony Cordonnier
Global Co-Head of Cyber
anthony.cordonnier@guycarp.com

Erica Davis
Global Co-Head of Cyber
erica.davis@guycarp.com

Zain Hussain Awan
International Cyber ILS Lead
zain.awan@guycarp.com

Additional contributors:

Matt Berninger

Jess Fung

How Guy Carpenter Can Help

The Guy Carpenter team will continue to monitor evolving attack methods and the effect they have on not only the global cyber market, but the wider financial market as well. Understand the origins, motivations and quantum of these events is critical to long-term portfolio management. We will support our clients as this risk evolution guides their cyber underwriting tactics, contract wordings and reinsurance strategies.

7. https://www.cnn.com/2021/06/09/business/jbs-cyberattack-11-million/index.html
8. https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with 3,500 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 over 130 countries. With annual revenue of $23 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 X.