UNDER ATTACK

MGM Resorts and Caesars Entertainment were just the two latest gaming companies to become targets of digital blackmail. How can the industry fight these cybercriminals?

BY ANDY GOLDBERG

As just about everybody knows by now, the two largest casino operators in the United States, Caesars Entertainment and MGM Resorts International, were both recently victimized by a malicious computer network intrusion. Although it is impossible to fully verify any of the reports and rumors surrounding these incidents, it does appear that both attacks were perpetrated by the same group, known by security insiders as UNC3944, or more commonly, "Scattered Spider."

Who exactly is Scattered Spider?

This is a difficult question to answer definitively, but they are believed to be an English-speaking group (as opposed to Russian or Eastern-European) that began intrusion campaigns in May or June 2022, according to reports from security firms CrowdStrike and Trellix.

Wikipedia claims the group members range in age from 19 to 22. Singapore-based cybercrime defender Group-IB appears to have been the first organization to connect cyberattacks at Twilio, Cloudflare and its own client base as all coming from the same group, which it dubbed "Oktapus," based on the victims' common reliance on Okta, a separate company, to handle secure authentication and access management. Group-IB published its report in August 2022, claiming the group had already compromised 130 organizations at that point.

Who else have they attacked?

Twilio and CloudFlare both published post-mortems of the attacks against their networks on August 7 and 9, 2022, respectively. The Group-IB report on August 22 noted the similarities in these two incidents as well as others it was monitoring. Then in January and February 2023, incident reports from video game publisher Riot Games, discussion forum Reddit, and cryptocurrency exchange Coinbase all identified similar attacks that were linked to Oktapus (which by then was more commonly referred to as Scattered Spider).

Riot Games confirmed that some source code of its popular game *League of Legends* was stolen, while Reddit and Coinbase prevented the attackers from gaining access to any customer data, though they both acknowledged that some employee contact information and internal documents were likely compromised.

Did they really break in via a 10-minute phone call with an employee?

A widely circulated X.com post by @vxunderground claimed the attackers simply needed to "hop on LinkedIn, find an employee, then call the Help Desk," and were inside after 10 minutes. This is consistent, in fact, with the earlier attacks, which all relied heavily on "phishing," that is, fooling a privileged employee into unwittingly providing credentials to an attacker, through a variety of methods.

However, the tweet ignores a large amount of prep work the attackers performed ahead of time to gather details about each company, including the names of key personnel, and a lot of work developing and placing malware inside of associated service providers. The tweet also glosses over the attackers' persistence. They might target dozens of employees, all of whom correctly refuse to interact, until finding one who gets fooled.

So how does the attack work?

While we don't know exactly how Caesars and MGM's networks were initially compromised, earlier attacks relied on fake SMS messages sent to targeted insiders. Twilio produced screenshots of seemingly urgent text messages sent to employees with links to twilio-sso.com and twilio-okta.com.

Similarly, Coinbase suggested that domains combining the company name with -sso.com or -dashboard.com were originated by the attackers. Upon clicking these links, employees were redirected to login pages that

The bottom line is that customers of either company should assume that their private information will probably be sold to adverse actors on black markets, if it hasn't been already.

appeared identical to their legitimate sites. And because many of these companies rely on Okta, all of these login pages look very similar, perhaps with just the company logo swapped out, making it relatively easy for the attackers to reuse a fake login page on many different target domains.

When the employee submits his or her credentials, the server immediately transmits that information to the attackers, including two-factor codes (those annoying SMS message or Google Authenticator digits), which the attackers use in real time to easily gain secure access to the legitimate site. Additionally, threat intelligence service Mandiant notes that the group also tries persistent calls to company help desks to initiate password resets that it can intercept. Once inside, the attackers launch a number of infiltration tools to breach additional systems and get closer to the most valuable data and assets.

Okta keeps being mentioned. What is it, and should it be avoided?

Okta is a cloud service company that handles login and identity management. Many companies use it internally for employee login and authentication—in short, Okta handles login screens, password management, application permissions.

Because security and authentication are difficult problems, outsourcing is often a good idea because their experts, who are entirely focused on this one area, are certain to have a more secure authentication flow than one you'd build in-house. The problem is, because Okta is so widely used, any tiny exploit is a master key into hundreds of company networks, so adversaries spend enormous amounts of time and effort into finding any flaw in Okta's systems.

Still, because these attacks relied initially on obtaining legitimate credentials via social engineering, it would not be accurate to say that Okta itself was compromised, but more that some of the enterprise configurations were not optimized for maximum protection against these types of attacks.

What could the casino operators have done to prevent these attacks?

Clearly, after more than a year of attacks by the same group using similar methods, knowledge about Scattered Spider and its methods was available. Whether anyone in infosec at Caesars, MGM or their partners was familiar with the group is unknown, but it demonstrates the importance of monitoring threats across all industries and never assuming an attack won't evolve to come after you, especially when one of your primary assets is a very large and detailed patron database.

Importantly, as I wrote in *GGB* in 2020, the casino industry must end its practice of keeping silent about any and all cyberattacks. The detailed reports produced by Twilio, CloudFlare, Coinbase and Reddit certainly helped other companies recognize similar attacks, allowing them to fend off, or reduce the severity of, those attacks.

By contrast, Caesars didn't produce any report or public statement, and its hack was a secret until journalists began speaking to sources as a result of the MGM disruption. It is entirely plausible to believe that had Caesars published a comprehensive report detailing the attack on its network, MGM could have amplified its security to be on high alert for specific social engineering tactics, and possibly prevented its hack altogether.

Although Caesars and MGM are competitors, professional ethics dictate sharing information about external threats. Casinos share information among security teams about individual criminals, cheaters and fraud schemes, and their credit departments share information about bad debtors. Refusing to share information about cyberthreats is simply irresponsible.

What is the impact on customers?

Truthfully, it's unlikely any of us will ever know. Because the casinos won't speak out, we really don't know what data the attackers were able to access or steal. Casinos require customers to offer up their driver's licenses (with photo, birthdate, address, height, weight, etc.) and private PIN numbers (which often match the customer's banking PIN) to participate in their loyalty programs. In return, they should owe those customers full transparency when such information has been breached or stolen.

Unfortunately, no state gaming regulators have held the casinos accountable. As of writing of this article, the Nevada Gaming Control Board has not released any public statement about either incident, except to say on X.com that it is "monitoring the cybersecurity incident with MGM Resorts." The bottom line is that customers of either company should assume that their private information will probably be sold to adverse actors on black markets, if it hasn't been already.

How should the different responses from Caesars and MGM be evaluated?

While most information surrounding these incidents is unverified, the widespread belief is that Caesars quickly paid a large ransom (supported by reporting from Bloomberg) while MGM did not. And because Caesars'

customer experience was largely unaffected while MGM's operations were clearly disrupted, many industry observers wrote that Caesars made the "smart" decision.

Ignoring the ethical implications of paying off a ransom demand, this viewpoint seems short-sighted. Even if business insurance will cover the cost of the ransom in this incident, Caesars future premiums are sure to skyrocket, its credit rating may drop (increasing borrowing costs) according to Moody's Investor Service, and the company has set itself up as a popular, profitable target for future attacks.

In addition, Caesars received nothing of substance for its payment, as it indicated in its SEC filing: "We have taken steps to ensure that the stolen data is deleted by the unauthorized actor, although we cannot guarantee this result."

In my 2020 article I wrote, "A ransomware attacker's dream victim is one who pays up and who stays silent," and that is exactly what Caesars has become. Caesars' silence doesn't just threaten a future attack on itself, but because all of these cyberattacks across many industries are interconnected, funding these criminals, giving them time and money to produce more exploits, it enhances the threat to companies in every industry.

And MGM?

It isn't entirely fair to compare the Caesars and MGM attacks, because it is unlikely the cybercriminals were able to infiltrate the two networks equally, and further, much of the MGM disruption was self-inflicted, shutting down its own systems as a preventative measure, according to a press release it submitted to the SEC.

It is also possible that Scattered Spider failed to access MGM's player database, and chose to resort to operational disruption as a secondary tactic in order to coerce the company to pay a ransom.

Certainly, the ensuing chaos and offline systems, whether self- or externally inflicted, were embarrassing and cost MGM quite a lot of revenue, and its credit rating may also be negatively affected, but if it avoids paying a ransom, it would probably recover confidence among analysts more rapidly, and be less likely to be targeted going forward, as the profit motive is severely lessened. If it is eventually learned that attempts to steal MGM's customer data were not successful, that should restore confidence among gaming customers as well.

What can other casinos learn from these incidents?

The most obvious thing would be to study the social engineering tactics used by Scattered Spider and ensure all infosec and IT personnel are fully aware of proper procedures for evaluating and reporting suspicious phishing tactics, rather than falling victim to them.

Seeing that Okta has been a common vendor in numerous attacks, any casino using its services should be in constant communication regarding its response and strategy. It is also essential to stop putting off difficult conversations about internal configurations and vendor selection. Still running SQL Server 2012? Time to upgrade. Still supporting Internet Explorer because a vendor's UI requires it? Get a new vendor. Internal networks using obsolete TLS protocols? Might as well not be using any security at all.

Have your backup and recovery procedures been tested recently? Are your databases encrypted at rest? Are all operating systems fully patched, and hardware drivers updated? Can external partners get access to high-value resources? Does your work-from-home solution introduce additional attack vectors (according to security rating firm Bitsight, remote-office networks are 3.5 times more likely to have malware installed)?

Have your backup and recovery procedures been tested recently? Are your databases encrypted at rest? Are all operating systems fully patched, and hardware drivers updated? Can external partners get access to high-value resources?

Further, these attacks demonstrate that there is no reliable way to outsource threat assessment and prevention to an external firm. Other hard conversations revolve around accurately assessing the quality of IT personnel, and whether compensation packages are adequate to attract and retain talented, motivated network engineers and technology experts.

It is easy to spend millions on consultants and services, and perhaps they can help identify some threats or disclose weaknesses within your network, but there is no substitution for in-house expertise and constant vigilance and education. As an example, Palo Alto Networks published a 2021 case study on its website, claiming that Caesars is protected by Palo Alto's "Prisma Access" solution. Whether Palo Alto was still working with Caesars in August 2023 is not known, but it is a certainty that enterprise-scale products such as these are not inexpensive. A Forrester Total Economic Impact Study estimated $13.3 million in costs over three years to deploy a comprehensive Palo Alto solution.

Are cloud servers more secure than in-house?

Every network deployment is unique, and therefore, generalizations don't apply to everyone. Mandiant, however, noted that Scattered Spider "is particularly adept at using privileged access to cloud environments to establish persistent access to victim environments," noting access to Azure cloud identity providers placing malware in victim-owned AWS S3 buckets. Okta, which we've discussed, is a cloud service. Alarmingly, the Group-IB report states that other cloud service platforms such as Mailchimp were breached, allowing cybercriminals to create password reset emails from legitimate Mailchimp addresses and servers, making it extremely difficult even for cautious, guarded infosec operators to recognize a malicious message.

Final takeaways?

Threats against widespread computer networks like those at casino resorts are constant and ever-evolving. Just when cybersecurity teams build up defenses against the methods and the tools used by the Scattered Spider group, a new attack with a different methodology is likely to arise.

Monitoring cybersecurity incidents across many industries is vital, as is employing engineers and technologists with demonstrated expertise. Coinbase and Twilio and most of the others largely fended off similar attacks without prior warning or knowledge of these attacks, while a year later, even after Scattered Spider's tactics were widely circulated, both casino companies failed to defend themselves.

The industry also needs regulators to take cybersecurity and personal information as seriously as they do gaming operations. The NGCB, to its credit, adopted new regulations in December 2022 which, in part, require disclosure of cyberattack investigations. However, the new rules do not specifically state whether such disclosures will be made public. It is strongly recommended that the board insists on public disclosure, and that regulators in other states follow this lead.

Andy Goldberg (andy@cfnine.com) is a database, technology and analytics consultant dedicated to making casinos smarter and more efficient. He specializes in database marketing automation, custom API programming, building innovative reporting tools and dashboards, revenue forecasting, and reducing VIP player churn. His consultancy, Centerfield Nine, is at cfnine.com.