DigiKnow

CYBER SECURITY DEPENDS ON YOU

THIS PHISH COST ONE CASINO $100 MILLION

October 2023| Issue 2023:8

WHY WE CONTINUE TO CARP ON PHISHING

It might appear that we spend an extraordinary amount of time and training on the topic of Phishing. We understand that some believe this is redundant. They would never disclose personal or work information in a phishing attempt.

Recent cyberattacks on international casino/hospitality organizations prove that the weakest link in the cybersecurity chain is very often us. Investigations into the MGM and Caesars attacks determined that in both cases, the chosen attack vector was phishing and Vishing, to be more specific. Vishing is using a voice call for the same goal as an email phish.

More than 90 percent of cyberattacks start with phishing, and it's one of the most common ways that organizations are penetrated as well. And vishing is a particularly effective avenue of attack: A 2022 IBM report found that targeted phishing attacks that included phone calls were three times more effective than those that didn't.

In the MGM case, it appears that the hackers found an employee's personal and employment information on LinkedIn. They used this to impersonate them in a call to MGM's IT help desk to obtain credentials to access and infect the systems.

How can you protect yourself and your organization? First, complete the annual cybersecurity training. To deflect attempts to Vish you personally, be careful what information you share by phone and with whom. Never give out

SPIDERS AND CATS LEAD THE CYBERATTACK AGAINST MGM RESORTS AND CAESARS ENTERTAINMENT

MGM Resorts confirmed hackers stole an unspecified amount of customers' personal information during a September cyberattack that will cost the hotel and casino giant an estimated $100 million.

The hotel and casino company first disclosed it had been targeted by a large-scale cyberattack on September 11. The cyberattack, which was days later claimed by hackers from ALPHV subgroup Scattered Spider, caused widespread disruption across MGM's properties - shutting down ATMs and slot machines and pulling the company's website and online booking systems offline.

MGM was not the only victim of a massive cyberattack. Caesars Entertainment announced a breach that was the result of a social engineering attack on an outsourced IT support vendor that led to unauthorized access to Caesars' network. The data exfiltration began on or about August 23, 2023, Caesars confirmed on September 7, 2023. The stolen personal data included names and driver's license numbers and/or identification card numbers. Caesars reportedly paid $15 million of $30 million ransomware demand.

A group known as Scattered Spider is believed to be responsible for the MGM breach, and it reportedly used ransomware made by ALPHV, or BlackCat, a ransomware-as-a-service operation. Scattered Spider specializes in social engineering, where attackers manipulate victims into performing certain actions by impersonating people or organizations with whom the victim has a relationship. The hackers are said to be especially good at "vishing," or gaining access to systems through a convincing phone call rather than phishing, which is done through an email.

Scattered Spider's members are thought to be in their late teens and early 20s, based in Europe and possibly the US, and fluent in English — which makes their vishing attempts much more convincing than, say, a call from someone with a Russian accent and only a working knowledge of English.

MGM reported that the private data of customers who used its services before 2019 were breached. This included contact information, gender, date of birth and driver's license numbers. A more limited number of Social Security and passport numbers were also breached. MGM said the hackers did not obtain customer bank account numbers or payment card information.

your login credentials and passwords. Be careful about where your personal and work data is publicly available as well, since attackers may use it against you (or to impersonate you to trick someone else). Verify that people are who they claim to be before engaging with them. Use different passwords across all of your accounts, so that if someone gets access to one of them, they aren't then able to get into others, and use multi-factor authentication for another layer of protection.

Solomon Adote
Chief Security Officer

The hacks have cast fresh spotlight on ransomware attacks - cyber intrusions that affect hundreds of companies every year, from healthcare providers to telecom firms. MGM and Caesars lost market value last week as stock prices fell, and MGM is yet to recover from various operations disrupted at the hotels and gaming venues it owns from Las Vegas to Macau. The FBI continues to investigate both breaches.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**