Caesars Entertainment confirms ransom payment, customer data theft

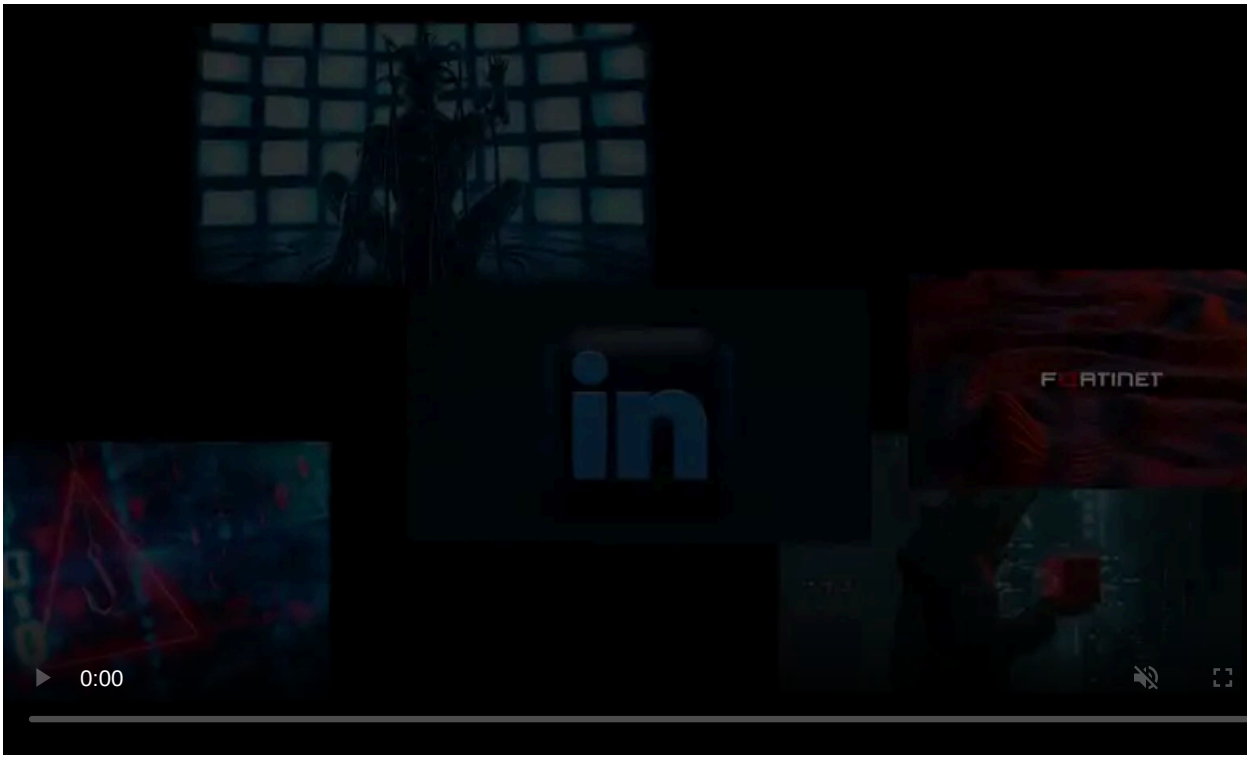
By Sergiu Gatlan

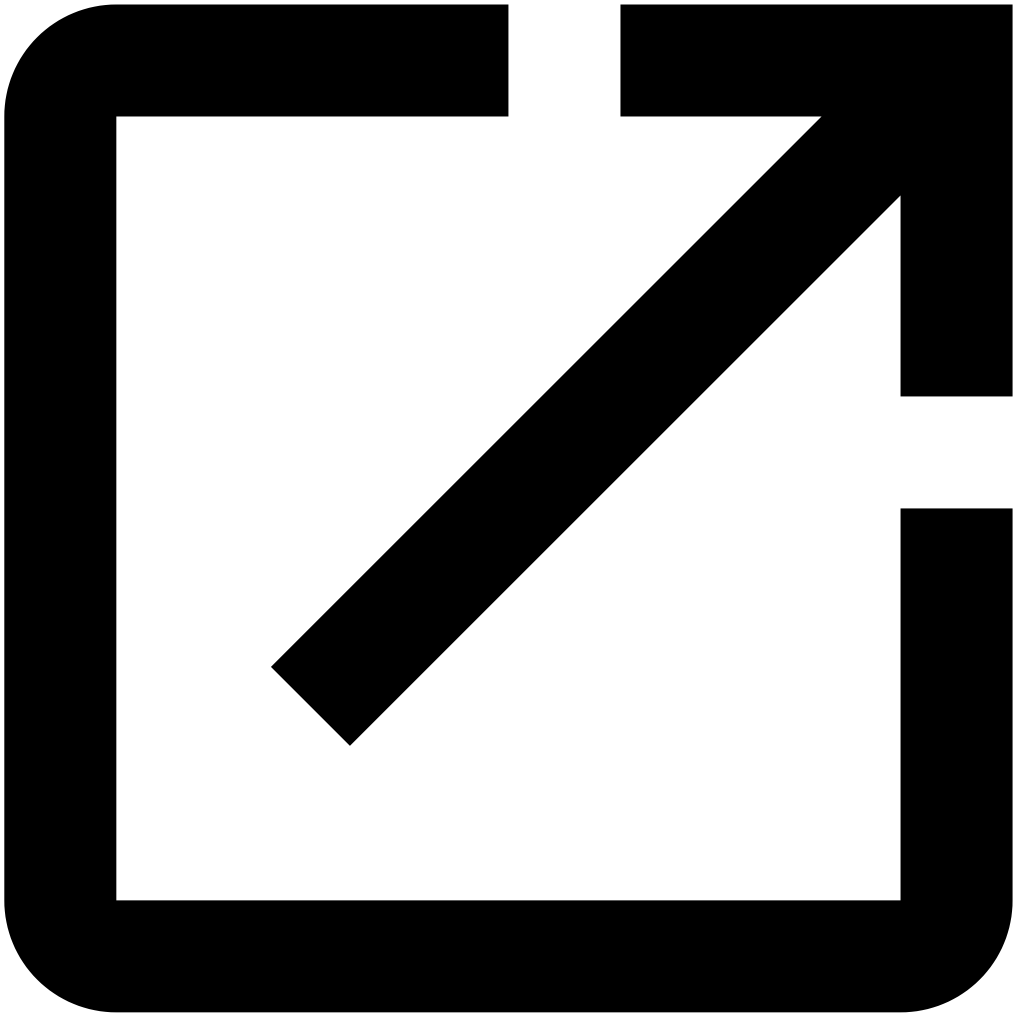
Published: 2023-09-14 · Archived: 2026-04-05 20:20:54 UTC

Caesars Entertainment, self-described as the largest U.S. casino chain with the most extensive loyalty program in the industry, says it paid a ransom to avoid the online leak of customer data stolen in a recent cyberattack.

Caesars discovered on September 7th that the attackers stole its loyalty program database, which stores driver's license numbers and social security numbers for many customers.

"We are still investigating the extent of any additional personal or otherwise sensitive information contained in the files acquired by the unauthorized actor," says an 8-K form filed by Caesars with the U.S. Securities and Exchange Commission on Thursday.


0:00



"We have no evidence to date that any member passwords/PINs, bank account information, or payment card information (PCI) were acquired by the unauthorized actor."

Caesars' 8-K also implies that a ransom demanded by the attackers was paid to prevent the leak of the stolen data online—a Wall Street Journal report says the hotel and casino entertainment company paid roughly $15 million, half of the attackers' initial $30 million demand.

Nonetheless, Caesars made it clear that it cannot provide any assurances regarding the potential actions of the threat actors responsible for the incident, including the possibility that they might still sell or leak the customer's stolen information.

"We have taken steps to ensure that the stolen data is deleted by the unauthorized actor, although we cannot guarantee this result," Caesars said.

"We are monitoring the web and have not seen any evidence that the data has been further shared, published, or otherwise misused."

While Caesars didn't link the attack to a specific cybercrime gang or threat actor, a Bloomberg report published on Wednesday claims the attack was conducted by a group known as Scattered Spider.

Also tracked as UNC3944 and 0ktapus, this financially motivated threat group has been active since at least May 2022.

It uses a combination of social engineering, multi-factor authentication (MFA) fatigue, and SMS credential phishing attacks to steal user credentials and breach targets' networks.

Data breach impacts only loyalty program members

According to Caesars, customers not enrolled in Caesars' loyalty program were not impacted by the data breach. The company will notify all affected individuals over the coming weeks.

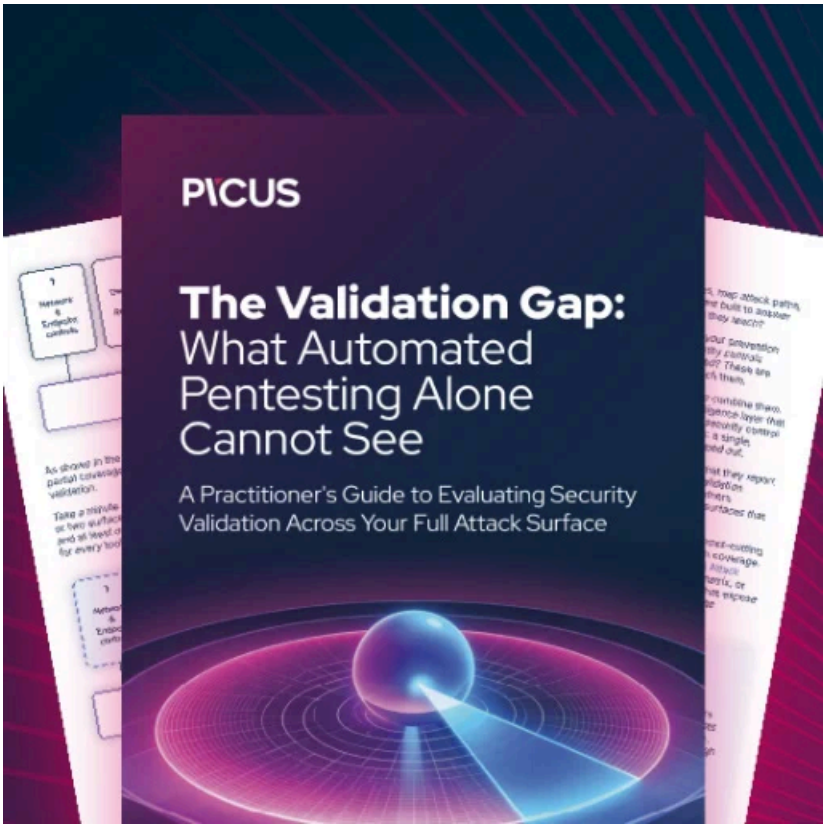
The company said in a separate data breach notification with additional details that it reported the incident to law enforcement.

It also added that the attack has not impacted its customer-facing operations, including online/mobile gaming apps and physical properties, as they operate without disruption.

Caesars is the second casino chain impacted by a cyberattack recently, with MGM Resorts International disclosing on Monday that it was forced to take its IT systems offline following a cyberattack that affected its websites, reservation systems, and casino services (i.e., ATMs, slot machines, and credit card machines).

In 2020, MGM Resorts also disclosed a 2019 cyberattack that led to the breach of its cloud services, allowing the hackers to steal over 10 million customer records.

Update: Added more info on Scattered Spider.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-payment-customer-data-theft/