

Booze and cruise providers are the latest to be hit by ransomware scourge

reader comments

13 with 9 posters participating

Share this story

Ransomware operators are continuing their blitz on corporations with deep pockets, with Jack Daniel's distiller Brown-Forman and cruise line behemoth Carnival being two of the latest to be hit.

In a statement, Brown-Forman officials wrote:

Brown-Forman was the victim of a cybersecurity attack. Our quick actions upon discovering the attack prevented our systems from being encrypted. Unfortunately, we believe some information, including employee data, was impacted. We are working closely with law enforcement, as well as world class third-party data security experts, to mitigate and resolve this situation as soon as possible. There are no active negotiations.

The statement came after Bloomberg News reported that it had received an anonymous tip of a ransomware attack. A Dark Web site that claims to be run by members of the REvil strain of ransomware says it has obtained 1 terabyte of data from Louisville, Kentucky-based Brown-Forman. (In addition to producing Jack Daniel's, Brown-Forman also owns Finlandia

vodka and other spirits.)

The site, which Ars isn't linking to, said that stolen data included contracts, financial statements, credit histories, and internal correspondence of employees. Also included were screenshots of file structures and documents purportedly taken during the heist.

Ars was unable to confirm the authenticity of the data. The Brown-Forman statement didn't comment on the Dark Web site claims or the purported evidence. A Brown-Forman spokeswoman didn't answer questions posed by Ars.

Meanwhile, the world's biggest cruise operator, Carnival Corporation, reported on Monday that it was hit by a ransomware attack that provided unauthorized access to personal data of passengers and employees. Company officials learned of the infection on Friday, but when the infection started or how long it lasted before it was caught remain unclear.

The company didn't identify the ransomware strain or say if data is already circulating. Company officials have also yet to identify which of its numerous subsidiary cruise lines was breached. Carnival disclosed the attack in a regulatory filing with the Securities and Exchange Commission. Part of the filing read:

Based on its preliminary assessment and on the information currently known (in particular, that the incident occurred in a portion of a brand's information technology systems), the Company does not believe the incident will have a material impact on its business, operations or financial results. Nonetheless, we expect that the security event included unauthorized access to personal data of guests and employees, which may result in potential claims from guests, employees, shareholders, or regulatory agencies. Although we believe that no other information technology systems of the other

Company's brands have been impacted by this incident based upon our investigation to date, there can be no assurance that other information technology systems of the other Company's brands will not be adversely affected.

Ransomware has emerged as one of the key forms of attack by financially motivated hacking groups. After initially gaining access, members often spend days or weeks mapping machine topology and obtaining passwords in an attempt to maximize the damage that can be done. To add a new line of revenue, many ransomware groups in recent months have begun selling the confidential data they steal. Payments are made through bitcoin and occasionally other types of digital coin.

A recent ransomware attack on GPS device and services provider Garmin cause outages that shut down many of its services for more than four days. There were no reports of outages affecting either Brown-Forman or Carnival.
<https://arstechnica.com/?p=1699855>