McMenamins breweries hit by a Conti ransomware attack

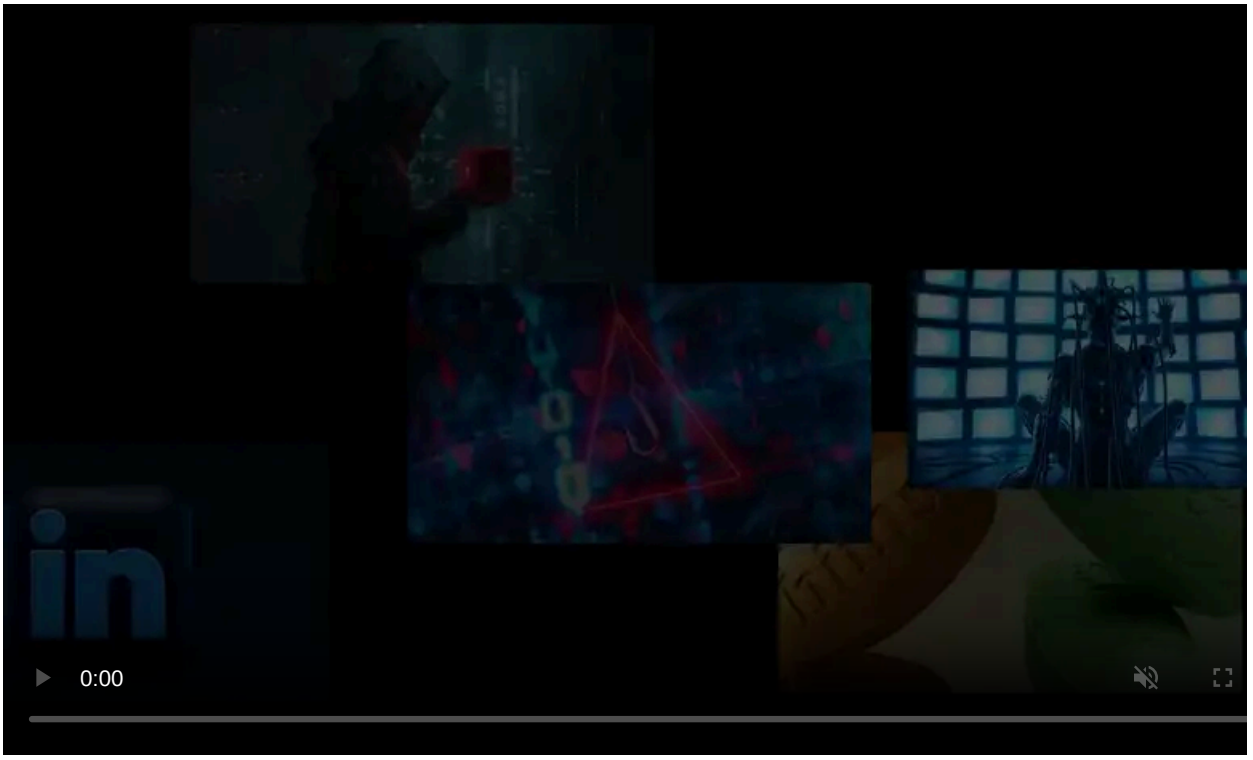
By Lawrence Abrams

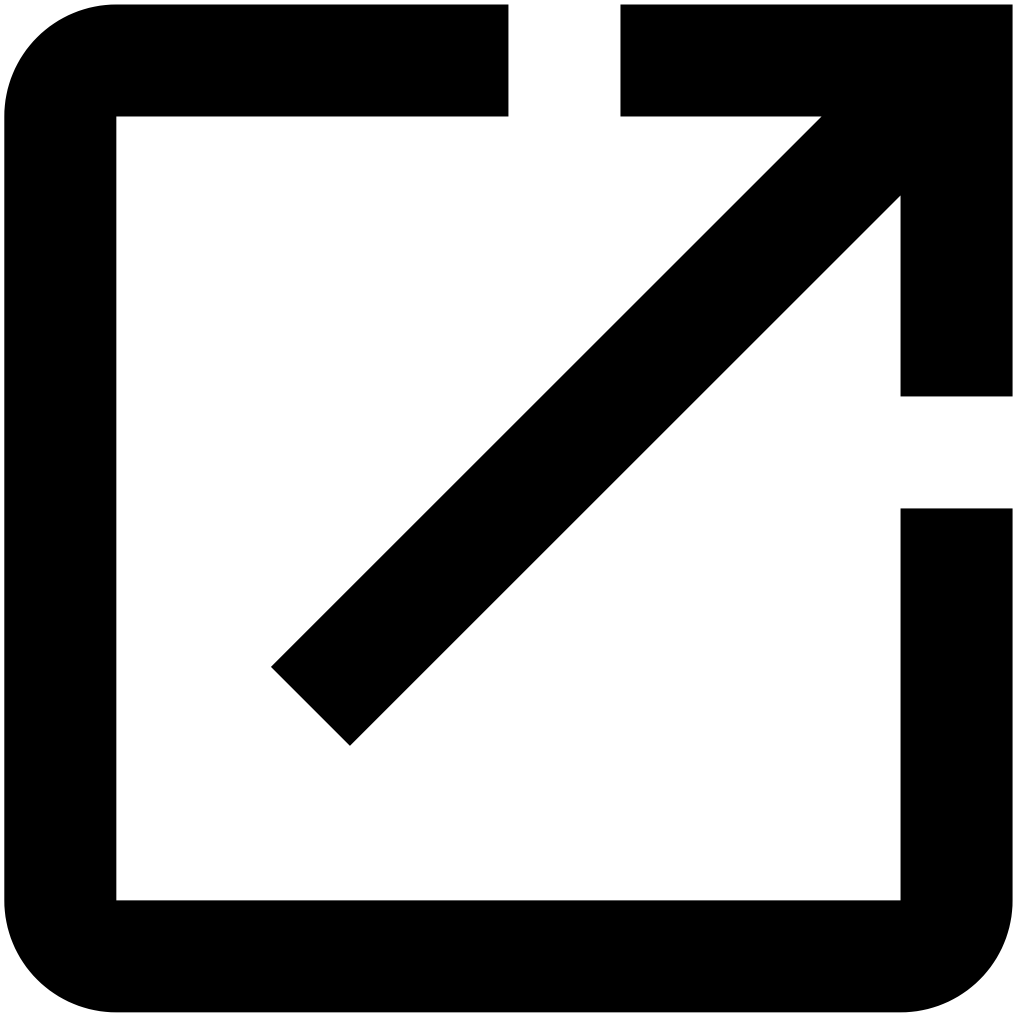
Published: 2021-12-16 · Archived: 2026-04-05 17:02:31 UTC

Portland brewery and hotel chain McMenamins suffered a Conti ransomware attack over the weekend that disrupted the company's operations.

McMenamins is a popular chain of restaurants, pubs, breweries, and hotels located in Oregon and Washington.

The ransomware attack occurred over the weekend, on December 12th, with sources telling BleepingComputer that the Conti gang conducted it.


0:00



Servers and workstations were encrypted as part of the attack, including point-of-sale systems.

While the attack did not cause locations to close, McMenamins was forced to shut down their IT systems, credit card point-of-sale systems, and corporate email to prevent the further spread of the attack.

After BleepingComputer emailed McMenamins, they issued a statement later that night confirming that they were hit by ransomware and are working with the FBI and a third-party cybersecurity firm to investigate the attack.

> "McMenamins today announced it has been the victim of a ransomware attack, which was identified and blocked on Dec.12. At this time, it appears that no customer payment data was impacted when cybercriminals deployed malicious software that locked the company's systems and prevented access to critical information. The family-owned company has reported the incident to the FBI and is also working with a cybersecurity firm to identify the source and full scope of the attack.
>
> It is possible that internal employee data may have been compromised, although it is not currently known whether that is the case. The following categories of employee information were potentially affected: names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, direct deposit bank account information, and benefits records. To provide employees with peace of mind, McMenamins will be offering employees identity and credit protection services, as well as a dedicated help line through Experian. Managers will provide this information to employees directly." - **McMenamins.**

As credit card scanners have been taken offline, McMenamins is being forced to change its payment processing at some locations. Unfortunately, these changes also prevent customers from purchasing or redeeming gift cards.

While our source has said that corporate data and documents appear to have been stolen during the attack, it is unknown if customer data was included. McMenamins says that their initial investigation does not indicate that any customer information was compromised as it was managed, collected, and stored by a third-party payment processing company.

However, as the hackers likely had access to the corporate network for some time, it is possible that the threat actors installed point-of-sale malware to steal credit cards, as has been done in previous ransomware attacks.

Whether this has happened will not be known until the third-party cybersecurity firm completes its investigation.

Who is Conti?

Conti ransomware is a ransomware operation believed to be run by a Russian-based hacking group known for other notorious malware infections, such as TrickBot.

The ransomware gang usually gains access to a network through BazarLoader or TrickBot malware infections installed via phishing attacks or by the threat actors exploiting vulnerabilities in Internet-exposed devices, such as VPN or firewalls.

Once the attacks gain access to an internal system, they will spread through the network, steal data, and deploy their ransomware.

Conti is considered a top-tier ransomware operation that has previously breached high-profile organizations, such as Ireland's Health Service Executive (HSE) and Department of Health (DoH), the City of Tulsa, Broward County Public Schools, FatFace, Advantech, and Sangoma.

Due to the increased activity by the cybercrime group, the US government recently issued a warning to corporations about an increased number of Conti ransomware attacks.

Source: https://www.bleepingcomputer.com/news/security/mcmenamins-breweries-hit-by-a-conti-ransomware-attack/