Drug distributor AmerisourceBergen confirms security breach

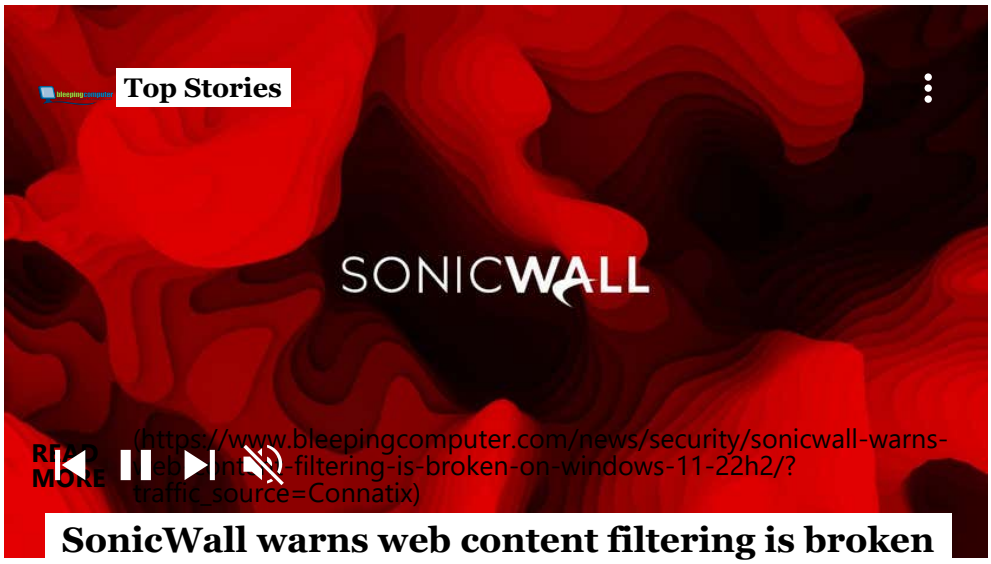
By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

February 8, 2023 09:59 AM **0**

Pharmaceutical distributor AmerisourceBergen confirmed that hackers compromised the IT system of one of its subsidiaries after threat actors began leaking allegedly stolen data.

AmerisourceBergen is a pharmaceutical product distributor, medical business consultant, and patient services provider. The company is a giant in the healthcare industry, employing 42,000 people and operating multiple distribution centers in the United States, Canada, and the UK, with 150 offices worldwide.

As first reported by security researcher Dominic Alvieri (https://twitter.com/AlvieriD), the Lorenz ransomware gang ended a lengthy period of silence by listing AmerisourceBergen and their allegedly stolen data on its extortion site.



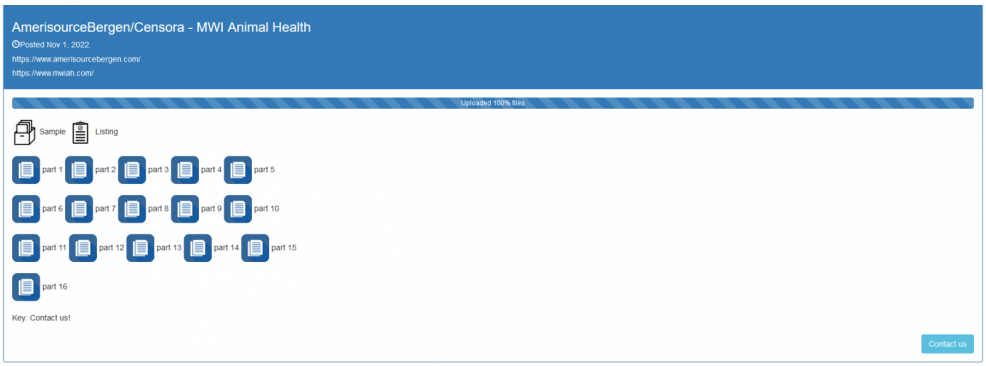
AmerisourceBergen confirmed the attack to BleepingComputer, stating that the intrusion was contained and they are investigating whether the incident has resulted in the compromise of sensitive data.

The complete statement from AmerisourceBergen is shared below:

> *"AmerisourceBergen's internal investigation quickly identified that a subsidiary's IT system was compromised. We immediately engaged the appropriate teams to limit the intrusion, contained the disruption and took precautionary measures to ensure all systems were and are now clear of any intrusions."*
>
> *"This was an isolated incident and we are in the process of investigating to determine whether any sensitive data was compromised. We take our responsibility to protect data very seriously and continue to secure and strengthen our networks to prevent any future issues." - AmerisourceBergen.*

The Lorenz ransomware group has posted all files allegedly stolen from AmerisourceBergen and MWI Animal Health, presumably the subsidiary that was breached.

The threat actors set the post date to November 1, 2022, even though the files were published just now, which might indicate that the breach happened a couple of months back.



AmerisourceBergen listed on Lorenz *(BleepingComputer)*

It is important to note that while the leaked files appear genuine, AmerisourceBergen has not yet confirmed these files were stolen from its networks.

Lorenz ransomware operators were recently observed using critical flaws in Mitel (https://www.bleepingcomputer.com/news/security/lorenz-ransomware-breaches-corporate-network-via-phone-systems/) telephony systems to gain access to corporate networks. The threat actors then lay low for several months (https://www.bleepingcomputer.com/news/security/lorenz-ransomware-gang-plants-backdoors-to-use-months-later/) until they are ready to use the deployed backdoor for data exfiltration and encrypt files.

Although Lorenz isn't the most prolific threat group in the ransomware space, its attacks have a major impact due to targeting large firms.

A notable example from last year was an attack against the multinational defense contractor Hensoldt (https://www.bleepingcomputer.com/news/security/defense-contractor-

hensoldt-confirms-lorenz-ransomware-attack/) that resulted in the exfiltration of internal documents.

Related Articles:

Arnold Clark customer data stolen in attack claimed by Play ransomware (https://www.bleepingcomputer.com/news/security/arnold-clark-customer-data-stolen-in-attack-claimed-by-play-ransomware/)

The Week in Ransomware - January 13th 2023 - LockBit in the spotlight (https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-13th-2023-lockbit-in-the-spotlight/)

Vice Society ransomware claims attack on Australian firefighting service (https://www.bleepingcomputer.com/news/security/vice-society-ransomware-claims-attack-on-australian-firefighting-service/)

Lorenz ransomware gang plants backdoors to use months later (https://www.bleepingcomputer.com/news/security/lorenz-ransomware-gang-plants-backdoors-to-use-months-later/)

Rackspace: Customer email data accessed in ransomware attack (https://www.bleepingcomputer.com/news/security/rackspace-customer-email-data-accessed-in-ransomware-attack/)

AMERISOURCEBERGEN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/AMERISOURCEBERGEN/)

DATA BREACH (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DATA-BREACH/)

LORENZ (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/LORENZ/)

PHARMACEUTICAL (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHARMACEUTICAL/)

RANSOMWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RANSOMWARE/)