American Dental Association hit by new Black Basta ransomware

bleepingcomputer.com/news/security/american-dental-association-hit-by-new-black-basta-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- April 26, 2022
- 02:42 PM
- 0

The American Dental Association (ADA) was hit by a weekend cyberattack, causing them to shut down portions of their network while investigating the attack.

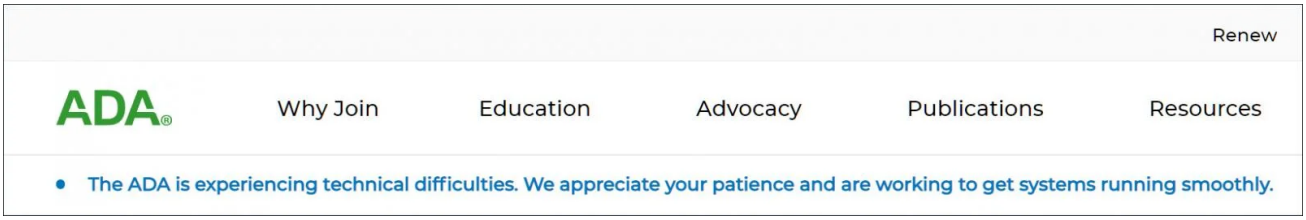
The ADA is a dentist and oral hygiene advocacy association providing training, workshops, and courses to its 175,000 members.

For many living in the USA, you will likely recognize the ADA Accepted seal on oral hygiene products, such as toothpaste and toothbrushes, indicating that the product is safe and contributes to oral health.

ADA suffers a weekend cyberattack

On Friday, the ADA suffered a cyberattack that forced them to take affected systems offline, which disrupted various online services, telephones, email, and webchat.

The ADA website now shows a banner stating that their website is experiencing technical difficulties, and they are working on getting systems running again.



Outage message on ADA.org

Source: BleepingComputer

This outage is causing online services to be inaccessible, including the ADA Store, the ADA Catalog, MyADA, Meeting Registration, Dues pages, ADA CE Online, the ADA Credentialing Service, and the ADA Practice Transitions. The company has also resorted to using Gmail addresses while its email systems are offline.

When BleepingComputer reached out to ADA for comment about the attack, we were told that they were just suffering technical issues and were investigating the cause of the disruption.

However, emails sent out to ADA members and seen by BleepingComputer paint a much grimmer picture.

Last night, the ADA began emailing its members, including state dental associations, practices, and organizations, with an update about the attack and information that can be shared with the recipient's members.

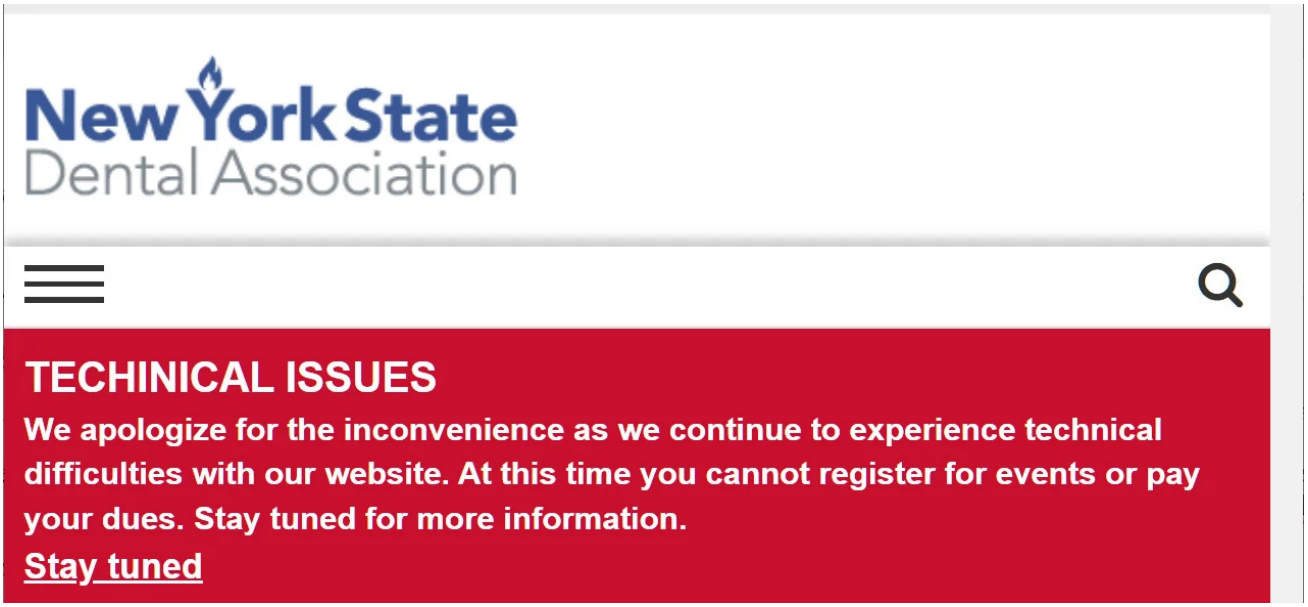
"On Friday, the ADA fell victim to a cybersecurity incident that caused a disruption to certain systems, including Aptify and ADA email, telephone and Web chat. Upon discovery, the ADA immediately responded by taking affected systems offline and commenced an investigation into the nature and scope of the disruption," reads an email sent to ADA members and seen by BleepingComputer.

The email says that they are working with "third-party cybersecurity specialists" and law enforcement to investigate the attack.

"Federal law enforcement has been notified and we are cooperating with them in this active investigation, so we ask for your understanding that we must limit the amount of detail that we can share at this time. In the meantime, we understand you may receive questions about the incident from members," continues the email sent by ADA to its members.

"It is important that we provide members with accurate information regarding this incident. It is equally important that we respond with accurate information while also being cognizant that this is an active investigation."

The ADA's cyberattack is not only affecting their website, but also state dental associations, such as those in New York, Virginia, and Florida, who rely on ADA's online services to register an account or pay dues.



Outage message on New York's Dental Association website
Source: BleepingComputer

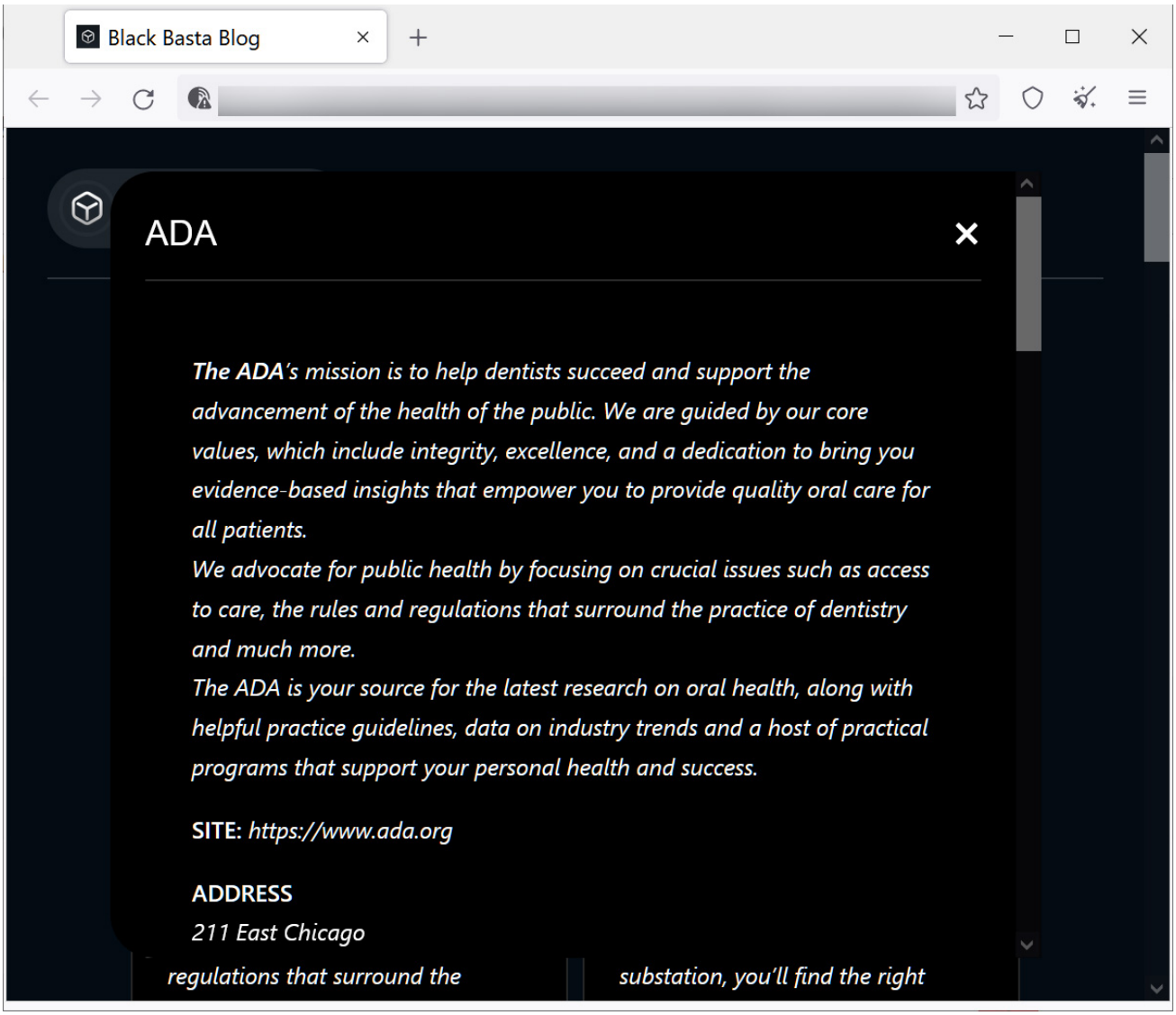
The ADA says that preliminary investigations do not indicate that member information or other data has been compromised. However, the description of this attack sounds like a ransomware attack, and almost every initial press statement says the same thing, with stolen data later published by threat actors.

BleepingComputer has contacted the ADA with further questions about the attack but has not heard back.

Black Basta ransomware gang leaks ADA's data

A new ransomware gang known as Black Basta has claimed responsibility for the attack on the American Dental Association.

Soon after publishing this story, security researcher MalwareHunterTeam told BleepingComputer that the threat actors had begun leaking data allegedly stolen during the attack on ADA.



ADA on Black Basta ransomware data leak site

Source: BleepingComputer

The data leak site claims to have leaked approximately 2.8 GB of data, which the threat actors state is 30% of the data stolen in the attack.

This data includes W2 forms, NDAs, accounting spreadsheets, and information on ADA members from screenshots shared on the data leak page.

The leaking of dentists' information can be particularly damaging, as small dental practices typically do not have dedicated security or network admins.

This lack of dedicated IT personnel typically causes their networks to be less secure than larger corporations with a significant security budget.

Due to the potential leak of ADA members' information to other threat actors, it is strongly advised that all ADA members be on the lookout for targeted spear-phishing emails that attempt to steal login credentials or other sensitive information.

Dental practices should also ensure they are not exposing any remote desktop services or other potential avenues for initial access to their networks and should place them behind a VPN instead.

Update 4/26/22: Added information about Black Basta ransomware claiming the attack on ADA.

Related Articles:

New Black Basta ransomware springs into action with a dozen breaches

The Week in Ransomware - May 13th 2022 - A National Emergency

Costa Rica declares national emergency after Conti ransomware attacks

Conti, REvil, LockBit ransomware bugs exploited to block encryption

The Week in Ransomware - April 29th 2022 - New operations emerge

- ADA
- American Dental Association
- Black Basta
- Cyberattack
- Dentist
- Outage
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: