Tech | Hack Data Breach Israel

Hackers Claim 'Catastrophic' Internet Archive Attack

Published Oct 10, 2024 at 7:36 AM EDT

Updated Oct 11, 2024 at 4:39 AM EDT

By Marie Boran
Technology Reporter

A group linked to a pro-Palestinian hacktivist movement has launched a catastrophic cyberattack revealing the details of 31 million people, compromising their email

An account on X under the name SN_BlackMeta claimed responsibility for the attack on The Internet Archive, a nonprofit organization, and implied that further attacks were planned. The Internet Archive is known for its digital library and the Wayback Machine. SN_BlackMeta has previously been linked to an attack against a Middle Eastern financial institution earlier this year, and a security firm has linked it to a pro-Palestinian hacktivist movement.

Encrypted passwords were also exposed and although these are relatively safe, users have been advised to change their passwords. And one expert has told *Newsweek* people should avoid browsing or using any files obtained from the site until it has declared an "all clear."

More From Newsweek Vault: Best Internet Speed Tests | How Fast Is Your Internet

This breach was accompanied by a series of Distributed Denial-of-Service (DDoS) attacks that temporarily took down the organization's website, archive.org, on Wednesday and is continuing to affect the website currently. Wayback Machine is also inaccessible right now.

A pop-up warns of a system hack. The Internet Archive, the nonprofit that runs the Wayback Machine, suffered from a catastrophic hack exposing the details of 31 million users. **SOLARSEVEN/GETTY IMAGES**

Brewster Kahle, founder and digital librarian of the Internet Archive, confirmed the breach and acknowledged the ongoing DDoS attacks.

In a post on X (formerly Twitter), Kahle stated: "What we know: DDOS attack–fended off for now; defacement of our website via JS library; breach of usernames/email/salted-encrypted passwords. What we've done: Disabled the JS library, scrubbing systems, upgrading security. Will share more as we know it."

More From Newsweek Vault: Proton VPN Vs. NordVPN 2024: Which Is Best For You?

Newsweek reached out to Brewster Kahle via DM on X for further comment.

The Internet Archive digital library was founded in 1996 with the mission of providing "universal access to all knowledge." It preserves billions of webpages, texts, audio recordings, videos, and software applications.

China Unveils Quadruped Robot That Can Cross Rough Terrain at High Speeds

Judge Throws Out News Outlets' Case Against OpenAI

How Top X Rivals Fared Since Elon Musk Sparked Twitter Exodus

More From Newsweek Vault: Best Antivirus Software

Its most used service is the Wayback Machine, a tool that allows users to browse archived versions of websites as they appeared at different points in history, with snapshots of webpages dating back to the early days of the internet.

On October 9, visitors to the Internet Archive's website were met with a pop-up message indicating that the site had been hacked. The message read: "Have you ever felt like the Internet Archive runs on sticks and is constantly on the verge of suffering a catastrophic security breach? It just happened. See 31 million of you on HIBP!"

The reference to HIBP points to Have I Been Pwned?, a widely-used service that allows individuals to check if their personal data has been compromised in known data breaches.

Troy Hunt, founder of HIBP, confirmed to Bleeping Computer that he had received a database containing email addresses, screen names, bcrypt-hashed passwords, and other internal data for 31 million unique email addresses associated with the Internet Archive.

Hunt took to X to address the situation, confirming his communication with the Internet Archive regarding the breach. He wrote: "I've been in communication with the Internet Archive over the last few days re the data breach, didn't know the site was defaced until people started flagging it with me just now. More soon."

Hunt also mentioned that 54 percent of the compromised email addresses were already present in the HIBP database from previous breaches.

"Based on publicly available evidence, the site has been thoroughly compromised. Their database has been exfiltrated, indicating that the back-end infrastructure was accessible, and their pages have been defaced, suggesting that the attackers have some degree of control over the web content served to users," Jason Meller, VP of Product at 1Password, told *Newsweek*.

"The website has also been repeatedly knocked offline, indicating that the attackers have gained dominance at the network layer. This is undoubtedly a difficult and challenging time for the Archive, a resource many of us rely on," he added.

"Given the severity of this breach and until they have had time to fully investigate, my strong recommendation is to avoid browsing or using any files obtained from the site until they have declared an 'all clear'," said Meller.

Involvement of Hacker Group SN_BlackMeta

SN_BlackMeta, who claimed responsibility for the attack, has previously been linked to other cyberattacks, including a record-breaking DDoS attack against a Middle Eastern financial institution earlier this year.

The hacktivist group, who emerged in November 2023 and previously targeted the Internet Archive with a DDoS attack in May 2024, battered the Middle Eastern financial institute for six days with attacks using a new DDoS-for-hire service called InfraShutdown.

Cybersecurity firm Radware connected SN_BlackMeta to a pro-Palestinian hacktivist movement that utilizes DDoS-for-hire services like InfraShutdown.

In posts on X from October 9, SN_BlackMeta stated: "The Internet archive has and is suffering from a devastating attack. We have been launching several highly successful attacks for five long hours and, to this moment, all their systems are completely down."

The account added, " "second round | New attack. 09/10/2024 Duration 6 hours," linking to a series of status reports on check-host.net, showing multiple connection timeouts for the Internet Archive.

people might want to know. This group claims they took down the Internet Archive because it "belongs to the USA ... who support Israel" which is not true. The Archive is not U.S. government, it is a nonprofit that includes many resources about Palestine, which we can't now access because of this attack."

"Sophisticated DDoS attacks, like the one just suffered by The Internet Archive, are often politically motivated," Meller said.

Although SN_BlackMeta has openly claimed responsibility for the latest Internet Archive DDoS attack, Meller says: "While SN_BlackMeta has implied involvement in the data breach that occurred more than a week earlier, it's currently unclear if they were actually responsible for that attack or the website defacement which occurred on the same date as the DDoS attack."

Newsweek reached out to SN_BlackMeta via X for comment.

Details of the Internet Archive Data Breach

Internet Archive users subscribed to Have I Been Pwned were made aware of the data breach late on Wednesday evening when they received an email titled 'You're one of 31,081,179 people pwned in the Internet Archive data breach'.

In the email, they were told that "In September 2024, the digital library of internet sites Internet Archive suffered a data breach that exposed 31M records. The breach exposed user records including email addresses, screen names and bcrypt password hashes."

The compromised data appears to have been obtained through the exploitation of a JavaScript library used by the Internet Archive, which allowed the attacker to deface the website and display the pop-up message.

The database, a 6.4GB SQL file named "ia_users.sql," contains records up to September 28, 2024, suggesting the breach occurred around that time.

Cybersecurity researcher Scott Helme confirmed the validity of the data after matching his own account information with the details in the leaked database. Helme noted that the bcrypt-hashed password in the data matched the hashed password stored in his password manager, and the time-stamps aligned with his records.

using the bcrypt algorithm. This method makes it extremely difficult for anyone who obtains the hashed passwords to determine what the original passwords were, thereby keeping your actual password safer.

What This Means for Internet Archive Users

The breach is a significant concern for users who have registered accounts with the Internet Archive. Exposed information includes email addresses, screen names, and bcrypt-hashed passwords.

While bcrypt is a strong hashing algorithm, users are advised to change their passwords as a precautionary measure, especially if they use the same password on other sites.

As a result of the DDoS attacks, the Internet Archive's website is experiencing significant downtime, with services being temporarily offline. The organization directed users to its social media accounts for updates during the outage.

The Internet Archive has been the target of cyberattacks in the past. In May, the same group claimed responsibility for DDoS attacks aimed at disrupting the Archive's services. Jason Scott, an archivist and software curator at the Internet Archive, commented on the attacks, noting that they appeared to be conducted "just because they can."

Update on 10/10/2024 at 11:01 a.m.: This story has been updated to include expert comment from Jason Meller, VP of Product at 1Password.