# Internet Archive is Attacked and 31 Million Files Stolen

By Jeffrey Burt

Published: 2024-10-10 · Archived: 2026-04-02 12:07:37 UTC

The Internet Archive, the non-profit digital library to offer free access to a broad array of digitized materials like websites, books, and software applications, was attacked late last month in a data breach that exposed 31 million files that includes such information as email addresses and screen names.

Visitors to the Internet Archive website at one point this week were greeted with a message reading “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!”

HIBP refers to “Have I Been Pwned,” a breach notification site people can use to see if their data has been leaked because of a cyberattack. Both Brewster Kahle, who founded the Internet Archive, and Troy Hunt, who operates HIBP, confirmed the data breach

In a posting on X (formerly Twitter), Kahle wrote October 9 that his organization fought off a distributed denial-of-service (DDoS) attack that led to the defacement of the website. He also confirmed the breach of usernames, email addresses, and salted-encrypted password. In response to the attack, the Internet Archive disabled the JavaScript library, scrubbed systems, and upgraded its security, though no details were discussed.

In posts today, Kahle wrote that the Internet Archive site was again between hit with a DDoS attack and the site was knocked offline, adding that he was “being cautious and prioritizing keeping data safe at the expense of service availability.”

According to a BleepingComputer report, the 6.4GB SQL file was stolen from a user authentication database and the most recent timestamp among the stolen data was September 28.

## HIBP was Sent Data Last Week

Also on X, Hunt said someone had sent him the information from the breach on September 30, but because he was away, he didn’t look into it until October 5 and contacted the Internet Archive the next day. Hunt began loading the data onto HIBP on October 9, the same day that the Internet Archive was his with the DDoS attack and its site was defaced.

An X posting on the HIBP site said that 54% of the accounts from the Internet Archive breach had already been in the database from previous attacks.

“The timing on the last point seems to be entirely coincidental,” Hunt wrote, adding that “it may also be multiple parties involved and when we’re talking breach + defacement + DDoS, it’s clearly not just one attack.”

## Pro-Palestinian Threat Group Claims Credit

The threat group SN_Blackmeta is taking credit for the attack, posting on X that they did so because the Internet Archive "belongs to the USA" and that the U.S. government supports Israel in the fighting in the Middle East. However, as noted by many responding to the group's accusation, the Internet Archive is a nonprofit that is not owned by the United States.

According to cybersecurity company Radware, SN-Blackmeta rose up in the wake of Hamas' October 7, 2023, attack on Israel and that country's military response. In a report in July about a sustained six-day DDoS attack by the SN_Blackmeta on a financial institution in the Middle East, Radware researchers wrote that the threat group surfaced via a Telegram channel November 14, 2023.

"The initial content on this channel set the tone for its future endeavors, featuring updates on cyberattacks targeting Israeli and Palestinian infrastructure, primarily through distributed denial of service (DDoS) attacks," the researchers wrote. "These early posts laid a strong foundation for the group's operations and clearly indicated their ideological stance."

## An Active Threat Group

SN_Blackmeta's introduction on Telegram was followed by a surge of DDoS attacks that stretched into this year, with the victims including websites in Israel, Canada, and Saudi Arabia, as well as the International Airport of Azrael and the Saudi Ministry of Defense in January.

In March, the targets ranged from French infrastructure as Israel's Smart Shooter company, Israeli telecom companies, and the Tel Aviv Stock Exchange. April saw no decline in their fervor; instead, they focused on UAE's digital infrastructure, Israeli scientific and technological websites, and a range of Western entities. In May and June, the group launched campaigns against tech giants Microsoft, Yahoo, and Orange, and UAE infrastructure.

In addition, Radware researchers said the Internet Archive also was a target during those months.

In March, a user on X calling themselves Sn-darkmeta said they were the leader of SN_Blackmeta, reposting images and summaries of attacks that has been publicized don the Telegram channel and "crafting a persona that bolstered the group's visibility and ideological messaging," they wrote.

Recent Articles By Author

---