Internet Archive Data Breach and DDoS Attacks: What You Need to Know

Published: 2024-10-10 · Archived: 2026-04-05 15:05:08 UTC

[Update] October 21, 2024: "New Breach Hits Internet Archive, API Keys and Source Code Exposed"

The Internet Archive has come under spotlight in social platforms and the cybersecurity community as news of a data breach, exposing the personal information of **31 million users**, spread across the web. To make matters worse, the service has faced continuous Distributed Denial of Service (DDoS) attacks in the last two days, rendering many of its functions and the widely-used Wayback Machine inaccessible.

Notice: Wayback Machine is temporarily offline

The Internet Archive, established in 1996 as a non-profit organization, has long served as a digital library for researchers, historians, and general users. Its mission has been to provide access to a vast array of online resources for posterity. However, the recent breach and subsequent attacks have raised questions about its security and future.

In this article, we'll explore what led to this significant breach, how the DDoS attacks unfolded, and what users need to know in the wake of these incidents.

What Happened to the Internet Archive?

The Internet Archive's popular service, The Wayback Machine, has fallen victim to a significant data breach. A threat actor compromised the site, gaining unauthorized access to a user authentication database containing 31 million unique records.

After the site recovered from an initial wave of DDoS attacks on October 8, visitors began seeing a JavaScript alert left by the hacker. 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!**"

Alert shown on archive.org after breach

Data Is Currently Available on Have I Been Pwned

The threat actors behind the Internet Archive breach remain unidentified, but the stolen authentication database was shared with security researcher Troy Hunt nine days ago, according to BleepingComputer.

After verifying the data by contacting affected users, Hunt initiated a disclosure process with the Internet Archive, stating the breached data would be available on Have I Been Pwned (HIBP) within 72 hours.

According to HIBP's breach summary, the stolen database includes 31 million unique email addresses, bcrypt-hashed passwords, screen names, and other data.

Breach information on Have I Been Pwned (HIBP)

The database, a 6.4GB SQL file named "ia_users.sql," contains records with the most recent timestamp from September 28, 2024, likely marking when the breach occurred. However, it remains unclear how the threat actors breached the Internet Archive and whether any other sensitive data was compromised.

In light of such security breaches, leveraging tools like **SOCRadar's Breach Dataset** module can be a critical part of the response. By continuously monitoring compromised datasets across the dark web, you can quickly identify if any credentials, such as those exposed in the Internet Archive incident, have been leaked. Additionally, using **Dark Web Monitoring** services helps track threat actor activity surrounding data breaches, enabling a more comprehensive defense against cyberattacks.

SOCRadar's Breach Datasets module page

These modules, coupled with **SOCRadar's Alarm** systems, equip your organization with the intelligence needed to protect sensitive information, ensuring that unauthorized access is detected early and handled before it leads to greater compromise.

DDoS Attacks Start Targeting Internet Archive

The Internet Archive came under a Distributed Denial-of-Service (DDoS) attack on October 8, which has been claimed by the hacking group BlackMeta a day later. While it is suggested that the DDoS attack is unrelated to the recent security breach, the group has announced plans for additional attacks.

BlackMeta took to social platform X, claiming their success, stating, "We have been launching several highly successful attacks for five long hours and, to this moment, **all their systems are completely down**."

Tweet by BlackMeta threat group (X)

Who Is BlackMeta? Why Was Internet Archive Targeted?

BlackMeta, also known as **SN_BlackMeta** or **DarkMeta**, is a pro-Palestinian hacktivist group that emerged in November 2023. The group has previously claimed responsibility for cyberattacks targeting organizations in Israel, the United Arab Emirates, and the United States.

In an additional statement on X, BlackMeta cited political motivations for their DDoS attacks on the Internet Archive, protesting that it belongs to the United States. They accused the U.S. government of supporting actions by Israel, framing their attack as a protest in the ongoing Palestine-Israel conflict.

Despite their claims, it's important to note that the Internet Archive is a non-profit organization, independent of the U.S. government.

The Breach's Influence on Hacker Landscape

The Internet Archive breach has caught the attention of various hacker groups, sparking conversation on platforms like Telegram. Notably, **LulzSec** has shared messages from DarkMeta, about the claims of conducting successful DDoS attacks against the Archive.

In the forwarded messages, DarkMeta boasted about disabling services for hours during multiple attack waves. The first round of attacks reportedly lasted four hours on October 8, 2024, followed by a second wave on October 9, lasting six hours.

Telegram message forwarded by LulzSec threat group

The Archive's Response to Ongoing DDoS Attacks

Brewster Kahle, founder of the Internet Archive, addressed the ongoing incidents via social platform X, confirming the DDoS attacks and outlining the Archive's current actions.

Kahle noted that they managed to fend off the initial wave of attacks, which included the defacement of their website through a compromised JavaScript library and the breach of usernames, email addresses, and salted-encrypted passwords.

In response, the Archive disabled the affected JS library and began scrubbing systems while upgrading their security measures.

Tweet by Brewster Kahle briefly stating what they know about the breach (X)

However, in a follow-up tweet today, Kahle announced that the “DDoS folks are back,” leading to the offline status of archive.org and openlibrary.org. It is stated that they are prioritizing securing the data they host, at the cost of temporary service downtime.

A second tweet clarifies that the DDoS attacks are ongoing (X)

New Breach Hits Internet Archive, API Keys and Source Code Exposed

The Internet Archive has experienced another breach, with users recently receiving a concerning email from the hacker behind the incident. This email was sent through the Archive’s authorized Zendesk server, further proving the extent of the breach.

The hacker revealed that exposed API keys were not rotated despite the Archive being informed of the breach weeks prior. This includes a Zendesk token granting access to over **800,000** support tickets, dating back to 2018, affecting users who submitted removal requests or inquiries to **info@archive.org**.

Threat actor’s message (X)

According to reports, the breach began when the hacker found an exposed GitLab configuration file on one of the organization’s servers. This file, exposed since December 2022, allowed the hacker to download the Archive’s source code. Also, based on the hacker’s clarifications, it has been confirmed that the breach is unrelated to the DDoS attacks on the Archive, and were conducted by an entirely different threat actor.

The Archive posted an ‘insider report‘ two days ago, detailing their ongoing efforts to secure their systems, stating that teams are working tirelessly to prioritize user safety.

As the Internet Archive works to address these challenges, important updates on their efforts to secure data and restore services will be added to this article as they become available. Stay tuned for the latest developments.
