FBI seize BreachForums hacking forum used to leak stolen data

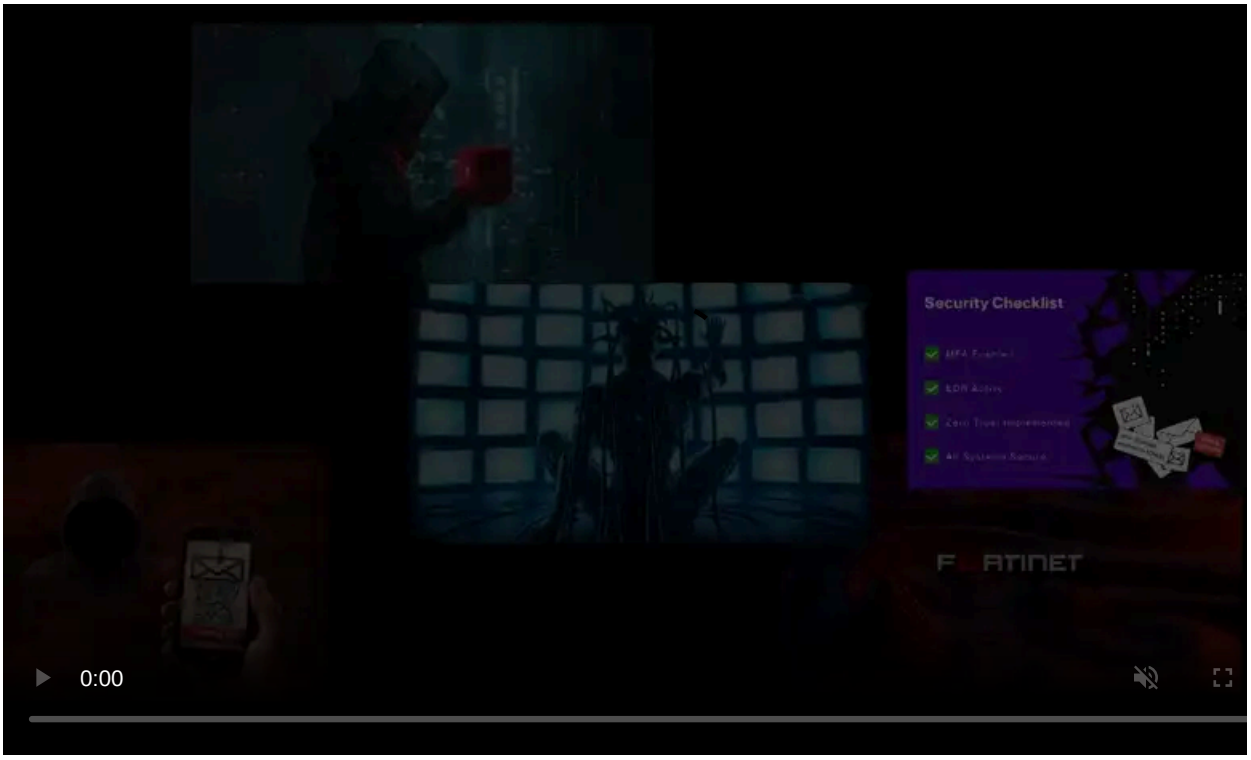
By Lawrence Abrams

Published: 2024-05-15 · Archived: 2026-04-06 15:27:20 UTC

The FBI has seized the notorious BreachForums hacking forum that leaked and sold stolen corporate data to other cybercriminals.

The seizure occurred on Wednesday morning, soon after the site was used last week to leak data stolen from a Europol law enforcement portal.

The website is now displaying a message stating that the FBI has taken control over it and the backend data, indicating that law enforcement seized both the site's servers and domains.


Security Checklist
0:00

"This website has been taken down by the FBI and DOJ with assistance from international partners," reads the seizure message.

"We are reviewing this site's backend data. If you have information to report about cyber criminal activity on BreachForums, please contact us," continues the seizure banner.

The seizure message also shows the two forum profile pictures of the site's administrators, Baphomet and ShinyHunters, overlaid with prison bars.

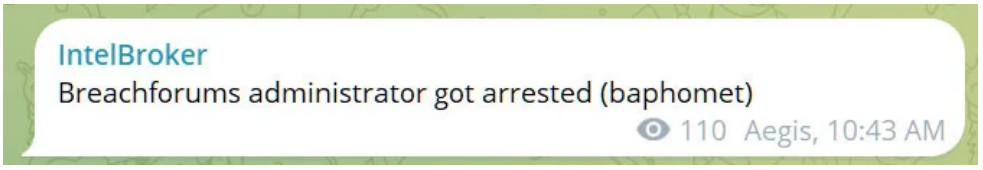
If law enforcement has gained access to the hacking forum's backend data, as they claim, they would have email addresses, IP addresses, and private messages that could expose members and be used in law enforcement investigations.

The FBI has also seized the site's Telegram channel and other channels owned by Baphomet, with law enforcement sending messages stating it is under their control.

Some of the messages posted to the seized Telegram channels by law enforcement came directly from Baphomet's account, likely indicating that the threat actor was arrested and his devices are now in the hands of law enforcement.

Seized BreachForums Telegram channel
Source: BleepingComputer

In a Telegram message shared with BleepingComputer, the threat actor known as IntelBroker is also claiming that Baphomet was arrested in the law enforcement operation.



The FBI is requesting victims and individuals contact them with information about the hacking forum and its members to aid in their investigation.

The seizure messages include ways to contact the FBI about the seizure, including an email, a Telegram account, a TOX account, and a dedicated page hosted on the FBI's Internet Crime Complaint Center (IC3).

"The Federal Bureau of Investigation (FBI) is investigating the criminal hacking forums known as BreachForums and Raidforums," reads a dedicated subdomain on the FBI's IC3 portal.

"From June 2023 until May 2024, BreachForums (hosted at breachforums.st/.cx/.is/.vc and run by ShinyHunters) was operating as a clear-net marketplace for cybercriminals to buy, sell, and trade contraband, including stolen access devices, means of identification, hacking tools, breached databases, and other illegal services."

"Previously, a separate version of BreachForums (hosted at breached.vc/.to/.co and run by pompompurin) operated a similar hacking forum from March 2022 until March 2023. Raidforums (hosted at raidforums.com and run by Omnipotent) was the predecessor hacking forum to both version of BreachForums and ran from early 2015 until February 2022."

This IC3 subdomain hosts a form that victims and other individuals can use to share information about BreachForums and its members.

When contacted by BleepingComputer about the seizure, both the FBI and the Department of Justice declined to comment.

The notorious BreachForums

BreachForums was the successor of a string of hacking forums used to trade, sell, and leak stolen data, as well as sell access to corporate networks and other illegal cybercrime services.

The first of these sites was known as RaidForums, which initially launched in 2015 and became the largest site for distributing stolen data, and was commonly used by ransomware and extortion groups.

The site was eventually seized by law enforcement, with the police arresting the owner known as "Omnipotent".

Soon after, one of its more active members, Pompompurin, created a new forum called 'Breached' to fill the void left behind by RaidForums.

The site quickly grew in popularity and was used by thousands of members to brag about their cybercrime activities and to leak and sell stolen data.

However, the site soon drew the ire of law enforcement after one of its members, IntelBroker, leaked the stolen data of D.C. Health Link, a healthcare provider for U.S. House members, their staff, and their families.

Soon after, Breached was seized by law enforcement, and its admin, Conor Fitzpatrick (aka Pompompurin), was arrested.

Once again, those in this cybercrime community were left without a home, so one of Breached's previous admins, known as Baphomet, teamed with ShinyHunters, a notorious seller of stolen data, to launch a new site named BreachForums.

Like the other sites, BreachForums quickly became popular with stolen corporate data being leaked from new breaches, including those on AT&T, 23andMe, Hewlett Packard Enterprise, Home Depot, Dell, PandaBuy, and The Post Millenial.

Today's seizure message indicates that law enforcement has had access to the site's servers, potentially for a long time, as they monitored threat actors' activities.

However, the breach that went too far may have been the recent leak of data stolen from Europol's Platform for Experts (EPE) portal by a threat actor known as IntelBroker, forcing law enforcement to take action.

Source: https://www.bleepingcomputer.com/news/security/fbi-seize-breachforums-hacking-forum-used-to-leak-stolen-data/