BreachForums Returns Just Weeks After FBI Seizure - Honeypot or Blunder?

By The Hacker News

Published: 2024-05-29 · Archived: 2026-04-05 16:30:08 UTC

The online criminal bazaar BreachForums has been resurrected merely two weeks after a U.S.-led coordinated law enforcement action dismantled and seized control of its infrastructure.

Cybersecurity researchers and dark web trackers Brett Callow, Dark Web Informer, and FalconFeeds revealed the site's online return at breachforums[.]st – one of the dismantled sites – by a user named ShinyHunters, who has since offered for sale a 1.3 TB database containing details of allegedly 560 million Ticketmaster customers for $500,000.

This includes full names, addresses, email addresses, phone numbers, ticket sales and event information, and the last four digits of credit cards and their associated expiration dates.

However, in an interesting twist, visitors of the site are now being asked to sign up for an account in order to view the content.

The development follows a joint law enforcement action that seized all the new domains belonging to BreachForums (breachforums[.]st/.cx/.is/.vc), while also hinting that the site administrators Baphomet and ShinyHunters may have been arrested.

The operation also resulted in the seizure of the Telegram channel operated by Baphomet, with the U.S. Federal Bureau of Investigation (FBI) noting that it's reviewing the site's backend data.

It's not currently clear if the individual(s) using the ShinyHunters persona on BreachForums is the original ShinyHunters hacker. Also unknown is the manner how they came to be in possession of one of the clearnet sites seized by the FBI, although Hackread.com reported that they reclaimed the domain from domain registrar NiceNIC.

However, the possibility that it may be a honeypot has not been lost among members of the cybersecurity community.

BreachForums emerged in March 2022 in the aftermath of the shutdown of RaidForums and the arrest of its owner "Omnipotent." It was dismantled in mid-June 2023, after which it was revived by Baphomet and ShinyHunters to launch a new site under the same name.

Both the U.S. Department of Justice (DoJ) and the FBI have yet to comment on the takedown, or the re-emergence of the forum for that matter.

Ticketmaster Confirms Breach

Ticketmaster's parent Live Nation confirmed on May 31, 2024, that it suffered a breach after its data was stolen from a third-party cloud database environment. Although the name of the provider was not disclosed, it's suspected to be Snowflake, based on a report published by Hudson Rock.

The Israeli cybersecurity firm said that a Snowflake employee's ServiceNow credentials were stolen via a Lumma Stealer campaign on October 5, 2023, allowing the threat actors to gain access to the employee's ServiceNow account in a manner that bypassed two-factor authentication (2FA) protections.

"Info-stealer infections as a cybercrime trend surged by an incredible 6,000% since 2018, positioning them as the primary initial attack vector used by threat actors to infiltrate organizations and execute cyberattacks, including ransomware, data breaches, account overtakes, and corporate espionage," Hudson Rock said.

It further said that the credentials were used by the threat actors behind the attack to break into other companies, including Santander. Earlier this month, the bank confirmed it had been compromised, and said it affected customers of Santander Chile, Spain, and Uruguay.

Snowflake has since acknowledged that it's "investigating an increase in cyber threat activity targeting some of our customers' accounts" and that it became of unauthorized access on May 23, 2024. The malicious activity is

said to have commenced around mid-April 2024.

The company said it has also notified all customers, urging them to review their account settings and enable 2FA to secure their data. It, however, refuted assertions that the activity was caused by any vulnerability, misconfiguration, or breach of the product.

That said, Snowflake noted that a former employee's demo account was accessed through stolen credentials, but said it did not contain sensitive data. Nor is it connected to any production or corporate systems, it added.

(The story was updated after publication to include information about the Ticketmaster breach.)

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2024/05/breachforums-returns-just-weeks-after.html