

BreachForums Returns Under the Control of ShinyHunters Hackers

Published: 2023-06-13 · Archived: 2026-04-05 20:23:25 UTC

The return of BreachForums was announced by Baphomet on Telegram, one of the administrators of the original forum.

BreachForums, the well-known cybercrime and hacking forum that was shut down months ago, has reemerged under new management. The notorious hacking group ShinyHunters has assumed control of the revived platform, raising alarm among cybersecurity experts and law enforcement agencies worldwide.

Confirmation of BreachForums' return under the management of [ShinyHunters](#) came through Baphomet, one of the administrators of the original forum. Baphomet, who remains an active figure within the hacking community, announced the resurgence of BreachForums in a PGP-signed message, leaving little room for doubt about its authenticity (It could still be a honeypot).

(Editor's note: You have been warned – use the forum at your own risk.)

Furthermore, a Telegram account using the alias ShinyHunters (@shinycorp) has emerged alongside Baphomet, taking charge of addressing the previous users of BreachForums. The account has already begun disseminating information and updates related to the forum's operations, attracting attention from both potential members and concerned individuals.

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

Hello.

This is Baphomet confirming not only myself, but the official forum: breachforums.vc

This is our only domain, no other domains are to be trusted. Including any old Breached domains.

Please be patient as we work through some expected issues related to email verification and downtime. Members who held rank on BF can PM me on the forum (or telegram) to restore their account on our forum. If you do not receive a verification email please let me know and we can make sure your account gets activated.

Sent from my tiny boating vessel.

-- Baph

-----BEGIN PGP SIGNATURE-----

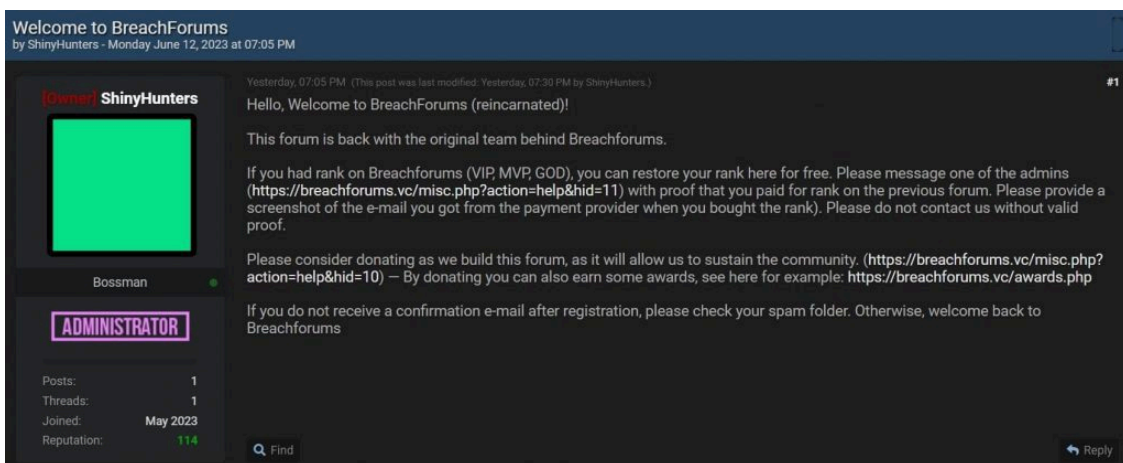


Baphomet's PGP-Signed message and ShinyHunters on Telegram (Hackread.com)

BreachForums, in its previous incarnation, served as a notorious hub for cybercriminals to exchange stolen data, discuss hacking techniques, and orchestrate illicit activities. The return of the forum, now under the auspices of ShinyHunters, has sent shockwaves through the cybersecurity community.

ShinyHunters, a hacking group infamous for their involvement in several high-profile data breaches, has consistently targeted organizations to steal sensitive information for monetary gain by [selling user data](#) on Clear and the dark web.

The resurgence of BreachForums under ShinyHunters' control has raised concerns about the potential implications for global cybersecurity. Law enforcement agencies and cybersecurity experts fear an upswing in cyberattacks, data breaches, and the facilitation of illegal activities on the platform.



The reincarnation of BreachForums as posted by ShinyHunters (Image: Hackread.com)

As news of the forum’s return spreads, organizations and individuals are urged to remain vigilant regarding their online security. It is crucial to implement strong security measures, regularly update passwords, and exercise caution when sharing personal information or engaging in online discussions.

What Happened to Old BreachForums?

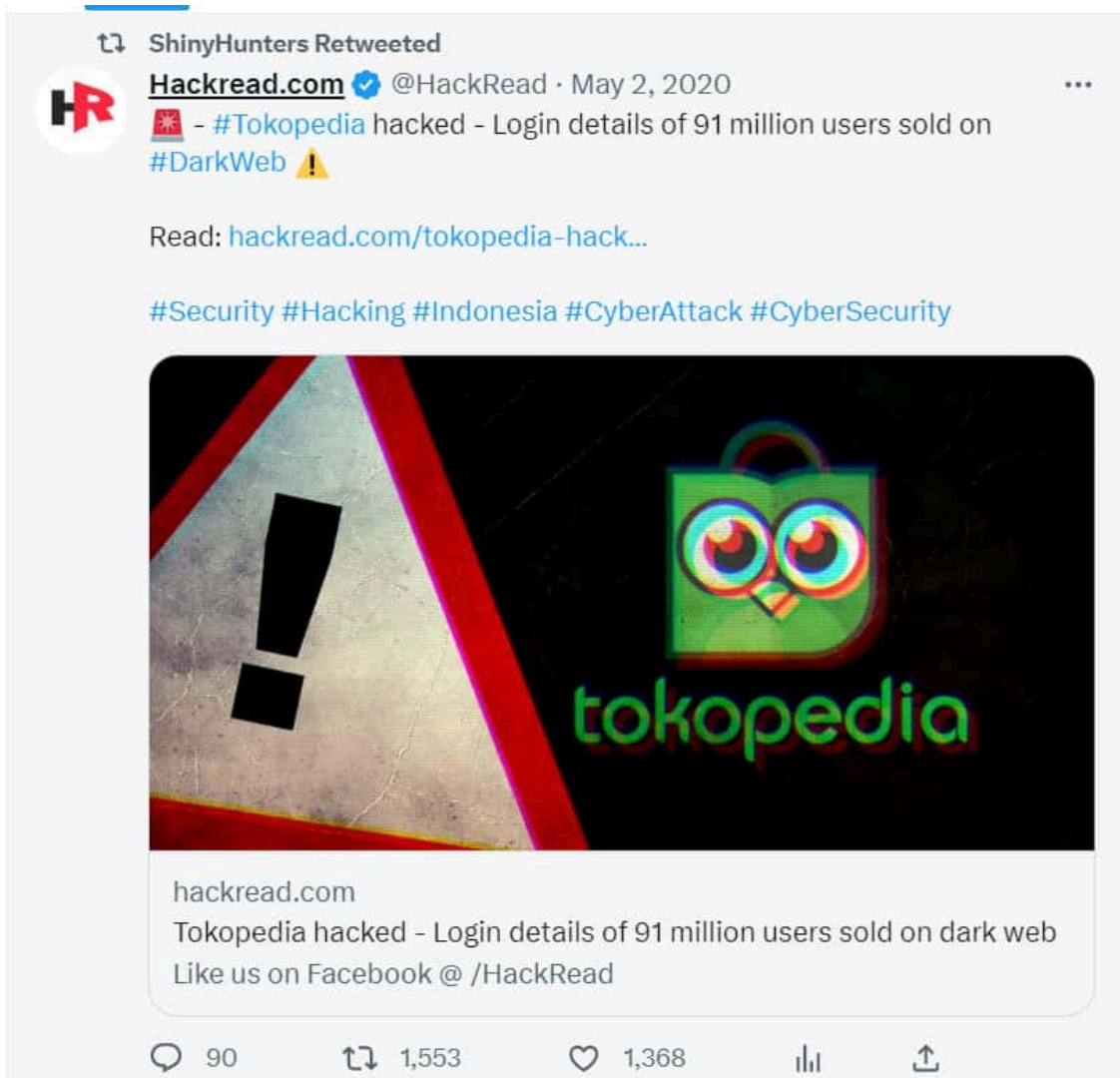
The original BreachForums emerged as an alternative to the [seized RaidForums](#) but was compelled to cease operations following the arrest of its owner, Conor Brian Fitzpatrick, also known as Pompompurin or Pom. Fitzpatrick, a 2021 graduate of Peekskill High School, was apprehended by the FBI.

Subsequently, the forum remained offline, prompting its members to convene in a Telegram group named “The Jacuzzi” to discuss the forum’s future. It is important to highlight that the FBI was unable to access the forum’s domain, preventing its seizure.

About ShinyHunters

ShinyHunters have gained prominence for their involvement in high-profile data breaches. They are known for targeting various organizations, including large corporations and popular websites.

ShinyHunters first gained attention in 2020 when they were linked to a series of data breaches, such as the [breaches of Tokopedia](#), a popular Indonesian online marketplace, and [Microsoft’s GitHub repository](#). In these incidents, they reportedly accessed and leaked millions of user records.



The group gained further notoriety by selling stolen data on underground hacking forums and dark web marketplaces. They typically target organizations with large user bases and sensitive data, including personally identifiable information (PII), login credentials, and financial details.

While the exact identity of ShinyHunters remains unknown, their activities and the scale of the breaches they have been associated with have raised concerns about cybersecurity and data protection.

The Arrest and Extradition of Alleged ShinyHunters Member

In June 2022, [Hackread.com reported](#) how authorities made an arrest at the Rabat international airport. The detainee was identified as Sébastien Raoult, a 21-year-old French citizen from Epinal City, France. Raoult is believed to be a member of the notorious hacking group known as ShinyHunters.

However, in January 2023, [reports emerged](#) stating that Raoult, also known by the alias Sezyo, had been extradited to the United States. He appeared in a Seattle federal court and pleaded not guilty to the charges against him.

Despite Raoult's arrest, concerns persist regarding the resurgence of cyber threats associated with the ShinyHunters group. One significant cause for worry is the return of BreachForums, a platform previously

exploited by the group to trade stolen data. This development poses a substantial cybersecurity threat to unsuspecting users and businesses.

In light of the past activities of ShinyHunters, organizations that have been targeted by this group must take immediate action to fortify their security systems. Strengthening security measures and implementing robust protocols are crucial steps to safeguard user data and prevent future attacks.

RELATED ARTICLES

1. [ShinyHunters Hack Google-funded delivery service Dunzo](#)
2. [ShinyHunters selling 368m users records stolen from 26 firms](#)
3. [ShinyHunters Hack Image stock site 123RF Leak 8.3m user data](#)
4. [ShinyHunters leak database of Indian wedding site WedMeGood](#)
5. [Raidforums Database Leak: Data of 460,000 Users Dumped Online](#)

Source: <https://www.hackread.com/breachforums-returns-with-shinyhunters-hackers/>