



| Flash |

BreachForums Marketplace Seized By Law Enforcement

F-2024-05-15a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Threat Actor, Deep and Dark Web

May 15, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 AM (EDT) on May 15, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | BreachForums Marketplace Seized By Law Enforcement

› Key Findings

- On May 15, 2024, the popular English-language deep and dark web (DDW) forum BreachForums was seized by law enforcement agencies in an operation likely coordinated by multiple international law enforcement agencies.
- Since mid-2023, BreachForums has been one of the most popular DDW marketplaces hosting discussions surrounding malicious network access and exploitation, as well as the trading of associated goods such as personally identifying information and personal financial information.
- ZeroFox can neither independently confirm nor deny that a spate of recent posts on the forum advertising the sale of highly sensitive information initiated the law enforcement activity.
- ZeroFox notes the possibility that the law enforcement operation is ongoing, with the potential for further disruption to occur.

Details

On May 15, 2024, the popular English-language DDW forum BreachForums was seized in an operation likely coordinated by multiple international law enforcement agencies. At the time of writing, both clearnet and onion domains display a banner stating that the

sites are under the control of the United States' Federal Bureau of Investigation (FBI) and Department of Justice (DoJ). ZeroFox notes the possibility that the law enforcement operation is ongoing, with the potential for further disruption to occur.

- The FBI and DoJ have allegedly taken control of the domain hosted at breachforums[.]st. Former BreachForum domains hosted at [.]cx, [.]is and [.]vc were not operational at the time of the disruption.
- The FBI has also seized control of the BreachForums Telegram channel, announcing to users via a message that a review of the backend data will be conducted.
- There are unconfirmed reports that an alleged BreachForum's moderator, Baphomet, has been arrested.



Banner Displayed on BreachForums[.]st Stating the Domain is Under FBI Control

Source: ZeroFox Intelligence

Since mid-2023, BreachForums has been one of the most popular DDW marketplaces hosting discussions surrounding malicious network access and exploitation, as well as the trading of associated goods such as personally identifying information and personal financial information.

- A previous version of BreachedForums was run from March 2022 – March 2023 before being seized by law enforcement following the arrest of the forum’s creator, an individual known as “Pompompurin.”¹
- The forum’s predecessor, Raidforums, was also disrupted by law enforcement in April 2022.

In April 2024, BreachForum’s surface web domain became unusable for a short period of time. The site’s administrator, Baphomet, posted a subsequent PGP-encrypted message to the forum’s Telegram channel announcing the suspension of BreachForums[.]cx and added that the forum’s [.]onion domain was still functioning. The disruption was claimed by the threat actor R00TK1T in a Telegram post.

- R00TK1T’s involvement was quickly disputed by Baphomet, who instead blamed “the five eyes network, and various other large nations.” Baphomet also announced the resumption of the forum on the [.]st Top Level Domain (TLD). As of the time of writing, this site is fully functional.
- Many of R00TK1T’s historical targets are those perceived to be acting against the interests of Russia and Israel. As a primarily English-speaking forum, BreachForums is regularly frequented by actors discussing cyberattacks against both Russia and Israel, which R00TK1T almost certainly perceives as justification for its alleged involvement.
- However, given the forum’s short downtime and the lack of subsequent information posted by R00TK1T as threatened, it is unlikely that R00TK1T was involved in the site’s disruption.

ZeroFox can neither independently confirm nor deny that activity conducted by well-regarded threat actor “IntelBroker” initiated law enforcement’s disruption to BreachForums. A spate of recent posts on the forum advertised data breaches allegedly composed of highly sensitive information.

- In April 2024, IntelBroker claimed to advertise a leaked database associated with “Space Eyes”—a geospatial intelligence company that almost certainly works with the U.S. government. Posts of this nature are not uncommon from IntelBroker;

1

[hXXps://www.justice\[.\]gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-forums-and-disruption](https://www.justice.gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-forums-and-disruption)

however, they are not usually advertised in clear web forums such as BreachForums[.]st.

- In May 2024, IntelBroker claimed to have breached a European intelligence agency and was selling sensitive personal data pertaining to its employees. This data was reportedly sold by Intelbroker.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%