



**| Flash |**

# **BreachForums Allegedly Relaunched With New Domain**

**F-2025-04-24B**

**Classification: TLP:CLEAR**

**Criticality: MEDIUM**

**Intelligence Requirements: Threat Actor, Hacking Forum, Deep Web**

**April 24 , 2025**

## 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 09:00 AM (EDT) on April 24, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

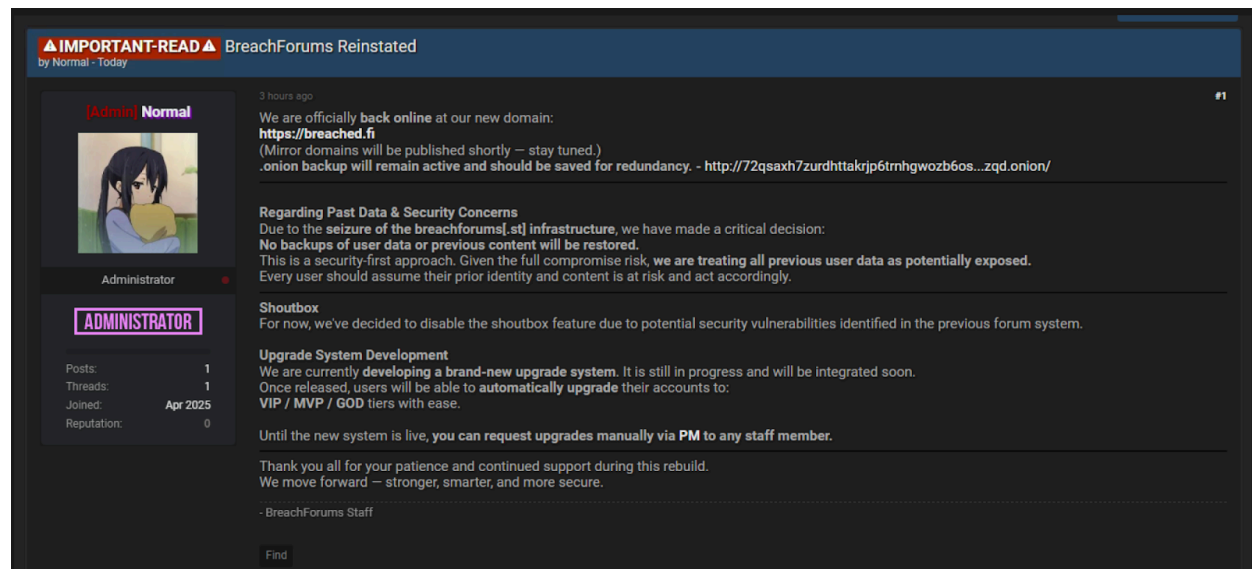
# | Flash | BreachForums Allegedly Relunched With New Domain

## | Key Findings

- On April 23, 2025, ZeroFox observed an announcement posted to the allegedly relaunched BreachForums site, breached[.]fi—made by the user “Normal”, stating that the forum is “officially back online”.
- Administrators of the previous [.]st BreachForums domain appear to have launched the new domain and have publicized efforts to reinstate the existing reputations of previous users.
- It is likely that BreachForums will have suffered reputational damage as a result of the April 15, 2025 outage. Returning users will very likely approach the [.]fi domain with increased caution, due to circulating speculation on deep and dark (DDW) forums regarding the potential involvement of law enforcement (LE).
- As of the writing of this report, ZeroFox has observed some users reporting difficulties in registering for accounts, which is likely attributed to initial launch issues. It is very likely that it will take some weeks before a fully functioning user interface is restored.

## Details

On April 23, 2025, ZeroFox observed an announcement posted to the allegedly-relaunched BreachForums site, breached[.]fi-made by the user Normal, stating that the forum is “officially back online”, accompanied by further details and plans.



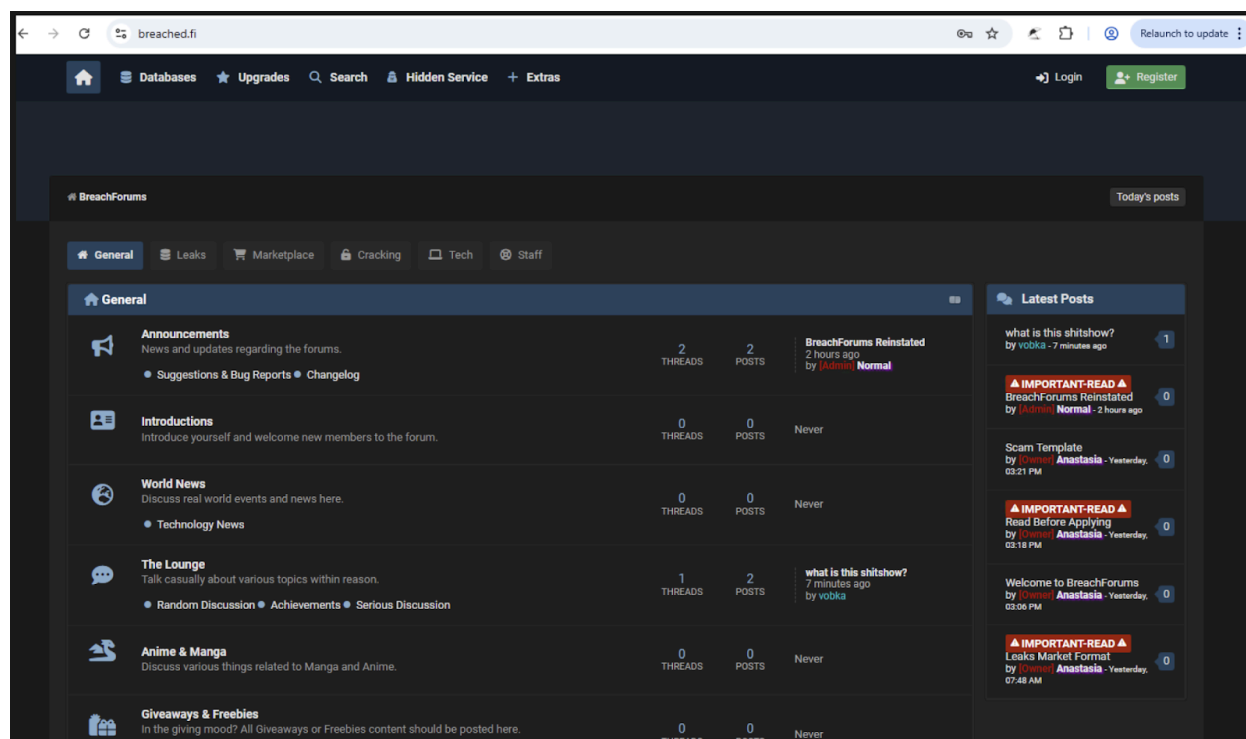
### Normal's post on Breached[.]fi

Source: ZeroFox Intelligence

- On April 15, 2025, ZeroFox observed that popular deep web hacking forum BreachForums was no longer online, with the domain breachforums[.]st displaying an error message.
- Conflicting information has also been circulating amongst threat actors, with many instead claiming that the Federal Bureau of Investigation (FBI) is behind BreachForums' closure.
- As of the writing of this report, it remains unclear whether a LE operation or a hacktivist group, such as Dark Storm (who has not indicated any specific motive), is responsible for the BreachForums outage.

The [.]fi domain referenced in Normal's post was launched on April 19, 2025, with a user interface notably similar to the previous [.]st domain. On April 20, 2025, an update was

posted on the [.]fi domain site by positive reputation actor “Anastasia”, to say that they were doing “everything they could to restore the forum as quickly as possible”. On April 23, 2025, Anastasia announced on breached[.]fi that they have successfully completed upgrades to the infrastructure and management procedures of the forum, stating that it would undergo a restart before launching with additional functionality.



Homepage of breached[.]fi

Source: ZeroFox Intelligence

There is ongoing speculation within DDW forums surrounding what caused the unexpected outage of BreachForums, and whether any relaunched domain can be trusted.

- On April 18, 2025, well-regarded and established threat actor “Rey” took to the social media platform X (formerly Twitter), posting a series of messages that alleged BreachForums had been seized by the FBI.
- On April 23, 2025, Rey posted on X stating “I don’t vouch for breached[.]fi, It’s fake”.<sup>1</sup> Notably, some of the original moderators from breachforums[.]st such as “Loki”,

<sup>1</sup> hXXps://x[.]com/ReyXBF/status/1915119801082499189

"Tanaka", "Addaka", and "888", have not yet been observed in the new domain breached[.]fi.

A separate post by Anastasia offered to restore the ranks of users that were held on the previous BreachForums site, should they send proof of payment to the admins of the new domain. This is very likely an attempt to lend credibility to the site, attract previous BreachForums users, and gain traction.



### Post by Rey on X

Source: [hXXps://x\[.\]com/ReyXBF/status/1913116530658705661](https://x[.]com/ReyXBF/status/1913116530658705661)

On 20 April, 2025, the Telegram-based hacktivist collective "Dark Storm" seemingly claimed responsibility for a distributed denial of service (DDoS) attack targeting the [.]fi domain, which they allegedly conducted between April 19–20, 2025. In the post, Dark Storm claimed they had taken down the site temporarily, also providing a check-host URL which seemingly confirmed the forum's outage.<sup>2</sup> As of the writing of this report, it remains unclear whether Dark Storm carried out this attack.

- On April 15, 2025, Dark Storm posted to its Telegram channel, seemingly claiming responsibility for a previous DDoS attack against the [.]st domain.

As BreachForums is a popular and highly-frequented hacking forum, it is very likely that many of its previous users will seek to register accounts at the new domain, in order to

---

<sup>2</sup> [t\[.\]me/DarkStormTeam3](https://t.me/DarkStormTeam3)

restore their previous reputations. While other deep web hacking forums exist, none are likely perceived as a legitimate alternative to BreachForums.

It is likely that BreachForums will have suffered reputational damage as a result of the April 15, 2025 outage. Returning users will very likely approach the [.]fi domain with increased caution, due to circulating speculation on DDW forums regarding the potential involvement of LE.

It is very likely that numerous threat actors will seek to capitalise on the uncertainty surrounding the new domain by creating alternative forums, whether intended as a replacement or created for the purposes of scamming visitors seeking to register. As of the writing of this report, ZeroFox has observed some users reporting difficulties in registering accounts, which is very likely attributed to initial launch issues. It is likely to take some weeks before a fully functioning user interface is restored.

## **| Appendix A: Traffic Light Protocol for Information Dissemination**

|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> 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%         |