



**| Flash |**

# **Dark Web Discussion Centers on BreachForums Outage**

**F-2025-04-17a**

**Classification: TLP:CLEAR**

**Criticality: MEDIUM**

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

**April 17, 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 9:00 AM (EDT) on April 17, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **| Flash | Dark Web Discussion Centers on BreachForums Outage**

**| Key Findings**

- On April 15, 2025, ZeroFox observed that the popular deep web hacking forum BreachForums was no longer online, with the domain breachforums[.]st displaying an error code which remains as of the writing of this report.
- On the same day, the hacking collective “Dark Storm” posted to its Telegram channel seemingly claiming responsibility and providing a check-host URL which confirmed the forum's outage.
- Conflicting information has also been circulating amongst threat actors, with many instead claiming that the Federal Bureau of Investigation (FBI) is behind BreachForums’ closure.
- ZeroFox observed discussions taking place in deep and dark web (DDW) forums and Telegram channels surrounding the alleged arrest of notorious threat actor “IntelBroker”, who is known for publishing prominent data leaks and previously fulfilling an administrator role within BreachForums.
- As of the writing of this report, it is unclear whether a law enforcement (LE) operation or a hacktivist group such as Dark Storm (who has not indicated any specific motive) is responsible for the BreachForums outage.

## Details

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 code which remains as of the writing of this report.

- BreachForums experienced several outages during 2024. Notably, in April, hacking collective “R00TK1T” claimed responsibility for the disruption of the forum’s .cx surface web domain, and LE entities claimed responsibility for taking down a related .st domain in May.



### **Dark Storm Telegram post claiming responsibility for BreachForums outage**

*Source: Telegram*

On the same day, the hacking collective Dark Storm posted to its Telegram channel seemingly claiming responsibility and providing a check-host URL which confirmed the forum's outage. As of the writing of this report, the post has received several “reactions” but no written responses.

- Dark Storm, first observed in approximately mid-2023, is a vocally pro-Palestine hacking collective that primarily engages in politically and ideologically motivated malicious cyber activities.

- On March 10, a post on the collective's Telegram channel alluded to responsibility for a global outage of the social media platform X (formerly Twitter).
- Dark Storm has also been implicated in attacks against various government and critical infrastructure entities, such as Finland's Central Bank, the Hungarian Defense Ministry, airports, and the North Atlantic Treaty Organization (NATO).<sup>12</sup>

Conflicting information has also been circulating amongst threat actors, with many instead claiming that the FBI is behind BreachForums' closure. Moderator "Tanaka"—who has a positive reputation in the forum—posted in Telegram stating that BreachForums had been "taken over", a claim that was reiterated in the Breachforums V4 Telegram channel.

- ZeroFox notes the absence of any evidence linking BreachForums' outage to LE activity, as well as any official statement from the FBI.
- ZeroFox also observed an allegedly leaked, protectively marked document circulating within online forums which claimed that, among other things, an international LE collaboration had achieved "persistent backend access" to BreachForums in March 2025, leading to a successful "operation". This document is unlikely legitimate, however.



## Tanaka Telegram post alluding to BreachForums outage

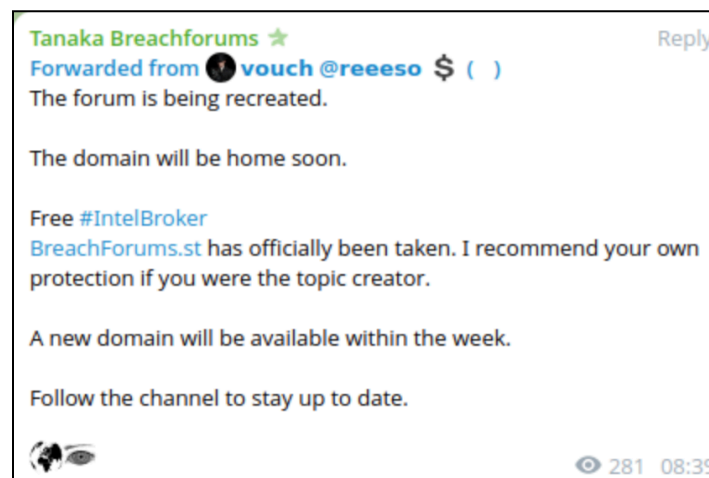
Source: Telegram

<sup>1</sup> [hXXps://thecyberexpress\[.\]com/dark-storm-team-announces-cyberattack/](https://thecyberexpress[.]com/dark-storm-team-announces-cyberattack/)

<sup>2</sup> [hXXps://cybernews\[.\]com/news/breachforums-dark-storm-ddos-cyberattack-fbi-hackers/](https://cybernews[.]com/news/breachforums-dark-storm-ddos-cyberattack-fbi-hackers/)

Tanaka's post also alluded to the alleged arrest of notorious threat actor IntelBroker, known for publishing prominent data leaks and previously fulfilling an administrator role within BreachForums. Similar claims were being heavily discussed across DDW forums and Telegram channels, though ZeroFox observed no evidence that these claims are either legitimate or linked to the forum's outage.

- IntelBroker assumed a moderator role within BreachForums in mid-2024, following the forum's severe disruption by a LE collaboration that resulted in the alleged arrest of moderator "Baphomet".
- In January 2025, IntelBroker resigned from BreachForums, citing a lack of available time to dedicate to the forum. The actor became more active in other hacking communities such as cracked[.]io and nulled[.]to, shortly before their targeting by international LE entities.



## Tanaka Telegram post alluding to BreachForums outage

Source: Telegram

Tanaka's post further specified that a new BreachForums domain will soon be available, with some actors speculating it will be online within several days. ZeroFox also observed the creation and advertisement of numerous domains appearing to masquerade as a BreachForums replacement, such as breachforums[.]cc. There is a very likely chance that these are being deployed by opportunistic, financially motivated threat actors seeking to capitalize upon the BreachForums outage by extracting cryptocurrency from users wishing to register with the "new domain."



## Breachforums[.]cc domain “registration” page

Source: Telegram

As of the writing of this report, it is unclear whether an LE operation or a hacktivist group such as Dark Storm (which has not indicated any specific motive) is responsible for the BreachForums outage. While the check-host URL provided by Dark Storm seemingly indicates denial-of-service activity has taken place, this does not eliminate the possibility of an ongoing LE operation.

There is a likely chance that a new BreachForums domain will be launched and moderated by familiar pseudonyms. While it will likely gain popularity quickly, the forum’s reputation is very likely to have wavered—causing frequenting actors to exhibit security concerns surrounding registration, as well as buying and selling processes. Threat actors are very likely to continue using malicious imitation domains to conduct opportunistic targeting of those seeking a relaunched BreachForums domain.

## Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                          | Amber                                                                                                                                                                                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | Sources may use <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. | Sources may use <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.                                                                                                           |
| HOW MAY IT BE SHARED?   | Recipients may NOT share <b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | Recipients may ONLY share <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. |
|                         | Green                                                                                                                                                                                        | Clear                                                                                                                                                                                                                                                                                                              |
| WHEN SHOULD IT BE USED? | Sources may use <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.              | Sources may use <b>TLP:CLEAR</b> 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 <b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | Recipients may share <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%         |