ZEROFOX INTELLIGENCE

Flash

BreachForums and Notorious Actors Announce Re-emergence

F-2025-06-05a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

June 5, 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 June 5, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | BreachForums and Notorious Actors Announce Re-emergence

| Key Findings

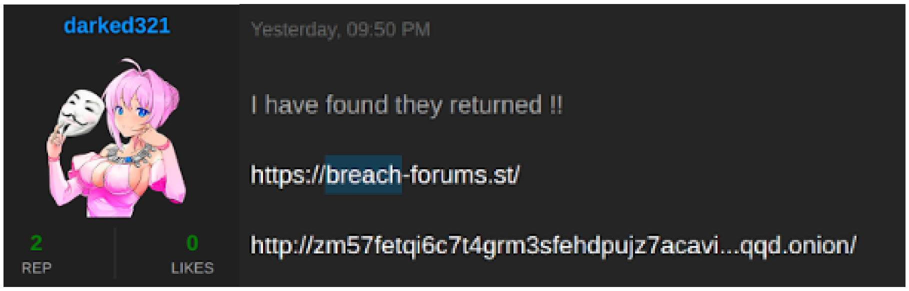
- On June 3, 2025, an actor using the alias "darked321" posted in the deep web forum DarkForums claiming its counterpart, BreachForums (another popular deep web hacking forum), has been relaunched.
- Darked321's DarkForums post quoted a longer message from actor "ShinyHunters", who provides an explanation as to the status of the original BreachForums domain and alleged plans for the new one. ZeroFox also observed activity from "IntelBroker".
- Given the presence of ShinyHunters and IntelBroker, there is a likely chance that breach-forums[.]st represents a relaunch effort led by actors in possession of digital infrastructure associated with the original domain.
- There is a very likely chance that breach-forums[.]st will quickly gain traction and restore functionality, though it is also likely that many users will remain active within peer domain DarkForums, where many actors migrated upon BreachForum's disruption.

Details

On June 3, 2025, an actor using the alias darked321 posted in the deep web forum DarkForums claiming its counterpart, BreachForums, has been relaunched. According to darked321, BreachForums is once again accessible via two separate domains: one clearnet domain (breach-forums[.]st) and one onion-based (zm57fetqi6c7t4grm3sfehdpujz7acavi4y7ubye3pugenyhktzxjqqd[.]onion/).

- On April 15, 2025, BreachForums became inaccessible, with the breachforums[.]st domain displaying an error code; at the time of this writing ZeroFox has confirmed that this domain remains inaccessible.
- Significant speculation surrounding this event took place within deep and dark web (DDW) forums and Telegram channels at that time, with many speculating law enforcement (LE) involvement.
- Discussion also centered around the possible arrest of IntelBroker—an actor prominent within the forum both for publishing numerous prominent data leaks and having previously carried out a moderator role.
- The hacktivist collective "Dark Storm" claimed responsibility for the BreachForums outage in its Telegram channel, though without any substantiation.

Darked321's DarkForums post quoted a longer message from actor ShinyHunters, who provides an explanation as to the status of the original BreachForums domain and alleged plans for the new one. According to the post, the newly launched breach-forums[.]st is the "new, official" domain, and efforts to restore legacy infrastructure and member ranks are ongoing—as is the rectification of security flaws identified during an "audit and rebuilding process." ShinyHunters also referred to the disruption of the previous domain, claiming a PHP vulnerability had been exploited. While the actor did not specify the identity of the alleged attacker, they did allude to attempts by "various agencies" to access a BreachForum database—almost certainly alluding to LE entities.



Yesterday, 09:50 PM

I have found they returned !!

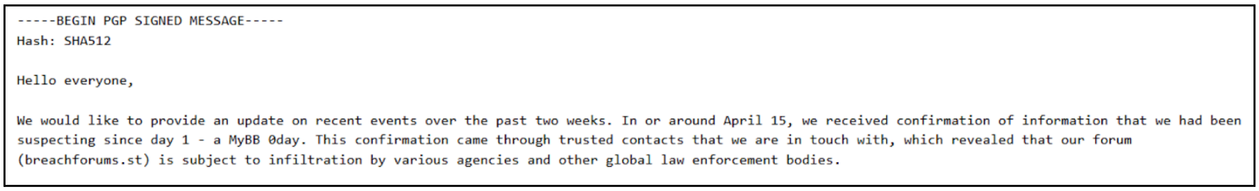
https://breach-forums.st/

http://zm57fetqi6c7t4grm3sfehdpujz7acavi...qqd.onion/

darked321's DarkForums post, quoting ShinyHunters' message

Source: ZeroFox Intelligence

Prior to this post, ZeroFox had not observed activity from ShinyHunters since April 28, 2025, when they posted a PGP-signed message to the front end of breachforums[.]st claiming that the disruption had been caused by a zero-day vulnerability affecting MyBB software. In this post, ShinyHunters also blamed unnamed LE entities, as well as warned BreachForums frequenters to avoid "clone" forums.

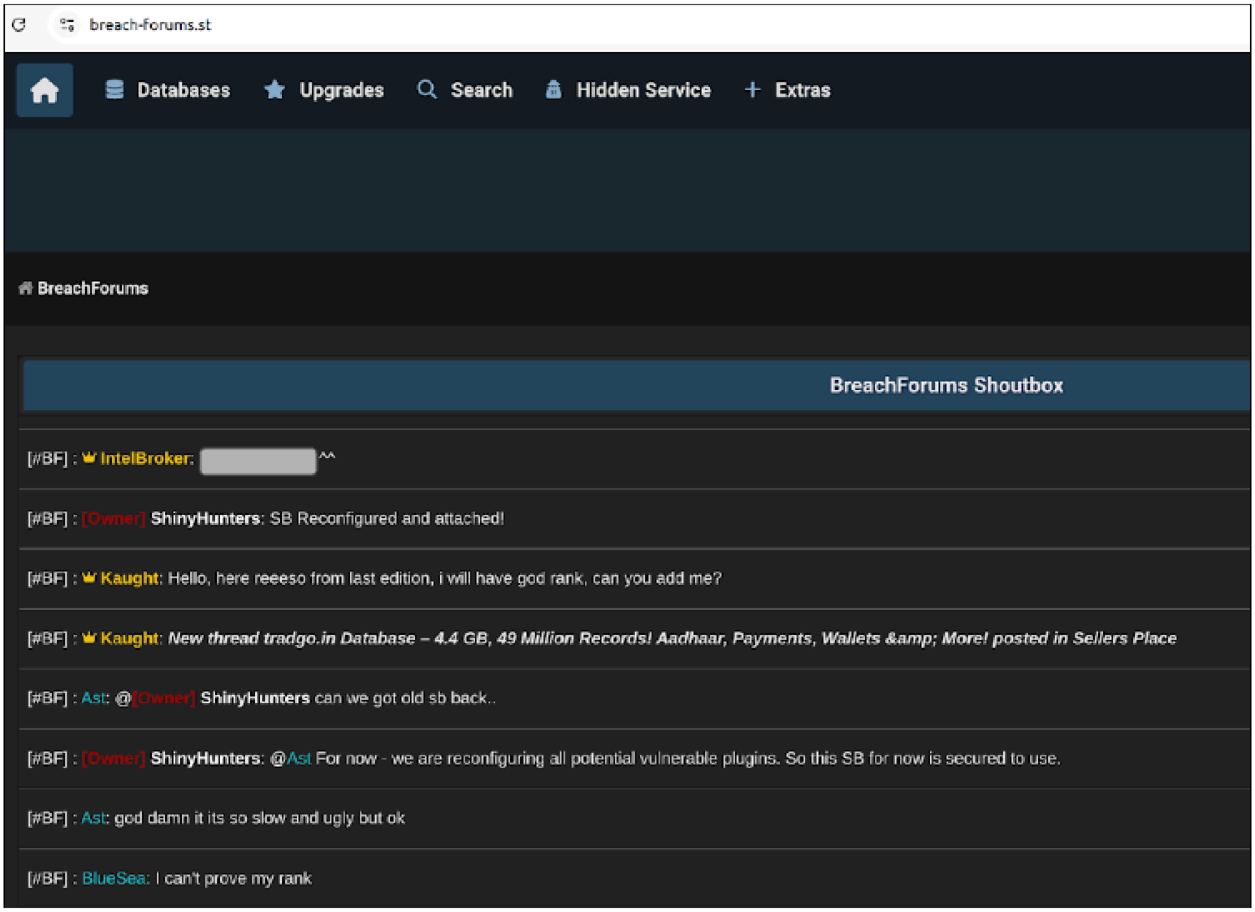


```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Hello everyone,

We would like to provide an update on recent events over the past two weeks. In or around April 15, we received confirmation of information that we had been
suspecting since day 1 - a MyBB 0day. This confirmation came through trusted contacts that we are in touch with, which revealed that our forum
(breachforums.st) is subject to infiltration by various agencies and other global law enforcement bodies.
```

Portion of ShinyHunters' statement posted to BreachForums front end on April 28, 2025

Source: ZeroFox Intelligence

- ShinyHunters is an English-speaking threat collective that has been operational in DDW forums since approximately 2020. The group has since been responsible for numerous data breaches and has also been widely viewed as the owner of BreachForums since the March 2023 arrest of previous moderator "Pompompurin."
- In addition to ShinyHunters, ZeroFox also observed posts within breach-forums[.]st's new Shoutbox feature from IntelBroker—the first activity observed from the actor since April 15, 2025.



[#BF] : ♛ IntelBroker: [redacted] ^^

[#BF] : [Owner] ShinyHunters: SB Reconfigured and attached!

[#BF] : ♛ Kaught: Hello, here reeeso from last edition, i will have god rank, can you add me?

[#BF] : ♛ Kaught: *New thread tradgo.in Database – 4.4 GB, 49 Million Records! Aadhaar, Payments, Wallets &amp; More! posted in Sellers Place*

[#BF] : Ast: @[Owner] ShinyHunters can we got old sb back..

[#BF] : [Owner] ShinyHunters: @Ast For now - we are reconfiguring all potential vulnerable plugins. So this SB for now is secured to use.

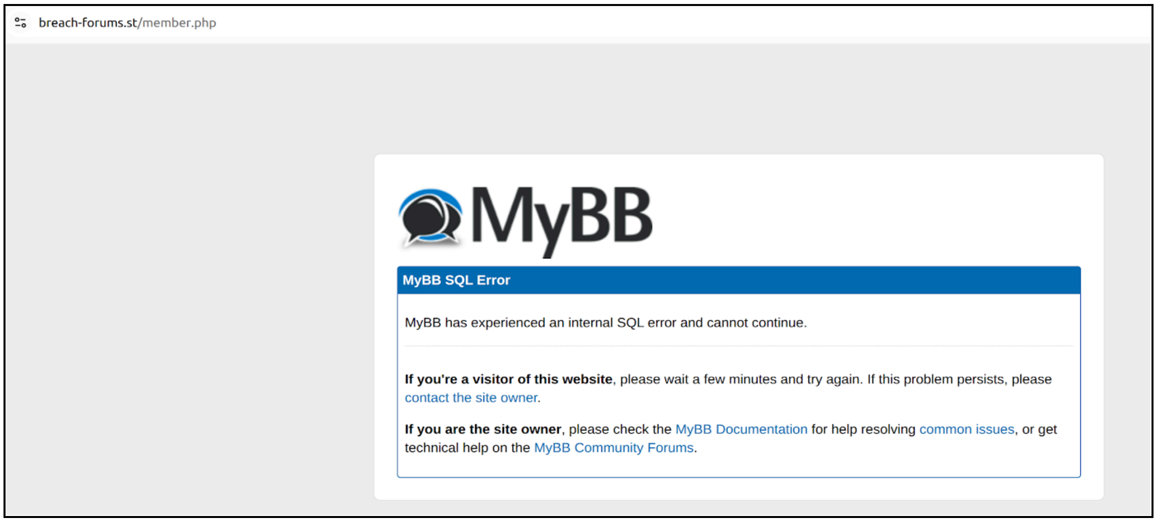
[#BF] : Ast: god damn it its so slow and ugly but ok

[#BF] : BlueSea: I can't prove my rank

Front page of BreachForums[.]st, with profanities redacted

Source: ZeroFox Intelligence

ZeroFox's attempts to register an account on breach-forums[.]st were unsuccessful due to a MyBB SQL error. This likely indicates that the forum is unable to connect to its user SQL database, suggesting configuration efforts remain in progress. Despite this, the forum search feature appears to be functional, with new discussions and topics appearing from users that have successfully registered. Notably, the new domain appears to have undergone a significant overhaul, with many features redesigned.



MyBB SQL Error

MyBB has experienced an internal SQL error and cannot continue.

If you're a visitor of this website, please wait a few minutes and try again. If this problem persists, please contact the site owner.

If you are the site owner, please check the MyBB Documentation for help resolving common issues, or get technical help on the MyBB Community Forums.

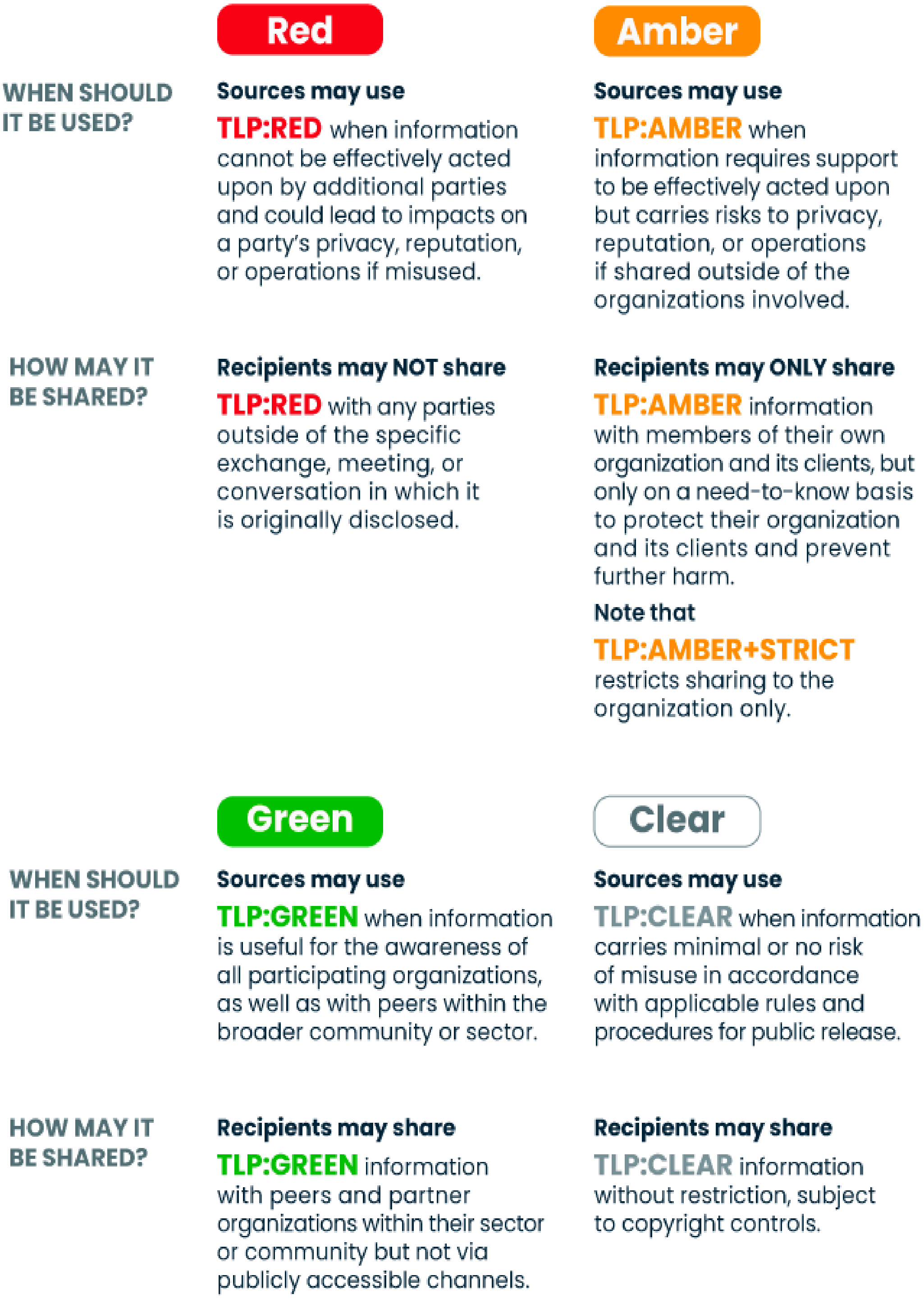
Breach-forums[.]st registration error

Source: ZeroFox Intelligence

Since the outage of BreachForums[.]st, numerous other forums have surfaced, with some claiming to offer a like-for-like replacement and others attempting to scam users wishing to register new accounts by masquerading as an "official" replacement. ZeroFox previously reported on the launch of BreachForums[.]fi, announced by actors "Normal" and "Anastasia" (the latter has previously fulfilled a moderator role within the original forum). This domain likely reflected attempts to offer a replacement but was seemingly unable to gain traction and remains inaccessible as of the writing of this report.

Given the presence of ShinyHunters and IntelBroker, there is a likely chance that breach-forums[.]st represents a relaunch effort led by actors in possession of digital infrastructure associated with the original domain. This is further supported by the presence of historic content within the new domain, much of which dates back to as early as 2023. There is a very likely chance that breach-forums[.]st will quickly gain traction and restore functionality, though it is also likely that many users will remain active within peer domain DarkForums—where many actors migrated upon BreachForum's disruption.

Appendix A: Traffic Light Protocol for Information Dissemination

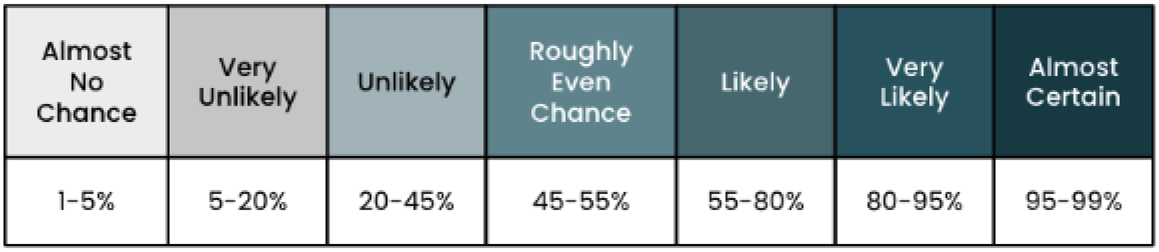


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively 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%