ZEROFOX INTELLIGENCE

Flash

Prominent Threat Actors Reportedly Arrested

F-2026-06-26b

Classification: TLP:CLEAR

Criticality:LOW

Intelligence Requirements: Threat Actor, Deep and Dark Web

June 26, 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 26, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

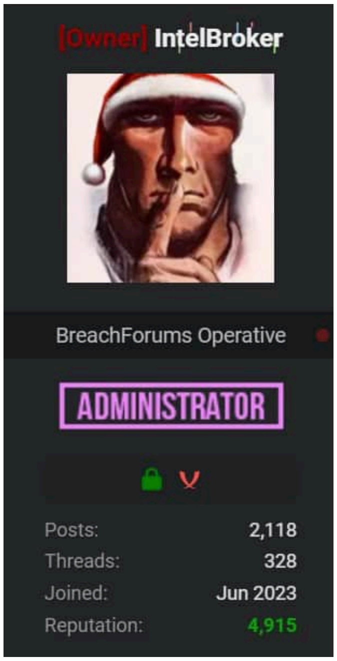
| Flash | Prominent Threat Actors Reportedly Arrested

| Key Findings

- Reporting on June 25, 2025, indicated that an individual thought to be behind the prominent deep and dark web (DDW) handle "IntelBroker" had been arrested by a law enforcement operation that occurred in France in February 2025.
- Earlier on the same day, separate reporting suggested that four key members of the popular hacking forum BreachForums, who are known by the aliases "ShinyHunters", "Hollow", "Noct", and "Depressed", had also been arrested on June 23, 2025.
- Both IntelBroker and ShinyHunters are prominent threat actors that are heavily associated with the popular deep web hacking forum BreachForums, which remains inactive as of the writing of this report.
- BreachForums is unlikely to make a successful comeback or relaunch, regardless of the presence of IntelBroker and ShinyHunters. Despite once being one of the most popular and prominent deep web hacking forums, there is a very likely chance that many members perceive a higher risk from using the forum, which is likely exacerbated significantly following the recent arrests.

Details

Reporting on June 25, 2025, indicated that an individual thought to be behind the prominent DDW handle IntelBroker had been arrested by law enforcement in an operation that took place in France in February 2025.[1] Earlier on the same day, separate reporting suggested that four key members of the popular hacking forum BreachForums known by the aliases ShinyHunters, Hollow, Noct, and Depressed had also been arrested on June 23, 2025.[2]



[Owner] IntelBroker

BreachForums Operative

ADMINISTRATOR

Posts:	2,118
Threads:	328
Joined:	Jun 2023
Reputation:	4,915

IntelBroker's BreachForums profile

Source: ZeroFox Intelligence

IntelBroker is a prominent threat actor and data broker who is best known for high-profile cyberattacks targeting well-known entities across the globe. IntelBroker is closely associated with the popular deep web hacking forum BreachForums, where they assumed a moderator role in mid-2024 following the forum's severe disruption by a law enforcement (LE) collaboration that resulted in the alleged arrest of previous moderator, "Baphomet".

[1] hXXps://www.securityweek[.]com/british-man-suspected-of-being-the-hacker-intelbroker-arrested-charged/

[2] hXXps://siliconangle[.]com/2025/06/25/breachforums-leaders-including-shinyhunters-intelbroker-arrested-france/

- On April 5, 2024, IntelBroker claimed responsibility for the alleged data breach of U.S. multinational home improvement company Home Depot, advertising a download of the data for free on BreachForums.[3]
- On January 18, 2025, IntelBroker posted on BreachForums advertising the sale of data related to Hewlett Packard Enterprise (HPE) following an alleged data breach. IntelBroker claimed that they had exfiltrated HPE's source code, private GitHub repositories, and certificates (both public and private keys).[4]

In March 2025, a lack of activity from IntelBroker led to speculation amongst DDW forums that they had been arrested. No further posts or comments by IntelBroker were observed, however the actor's name was present within a list of proposed moderators for a relaunched BreachForums domain, which would very likely have required the handle to log in to the platform.

There is a roughly even chance this activity was associated with LE's possession of the login credentials, obtained following the actor's arrest. However, there is a more likely chance that the IntelBroker handle has historically been used by more than one person and could therefore still be accessed, though this is now unlikely to occur.

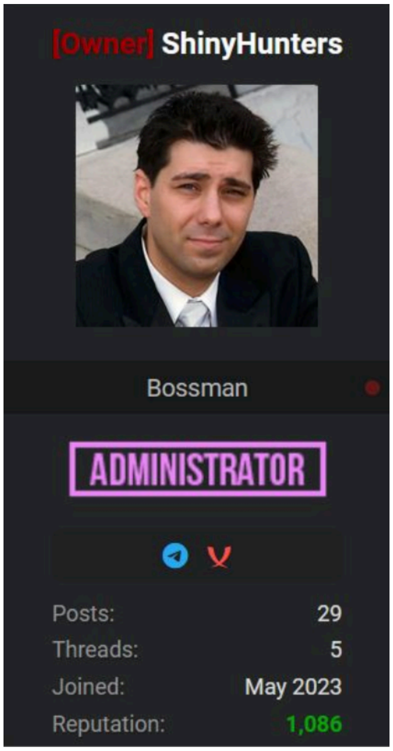
- In January 2025, IntelBroker resigned from BreachForums, citing a lack of available time to dedicate to the forum. The actor became more active in other hacking communities such as cracked[.]io and nulled[.]to, shortly before their targeting by international LE entities.

ShinyHunters is an English-speaking threat actor or collective that has been operational in DDW forums since approximately 2020. The actor 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 a previous moderator, "Pompompurin."

- On June 27, 2024, ShinyHunters posted on BreachForums advertising the sale of data related to Neiman Marcus, a U.S. department store chain. The data set allegedly provided personally identifiable information (PII) that included full names, dates of birth, phone numbers, and personal addresses.[5]
- On May 29, 2024, ShinyHunters advertised customer data stolen from

[3] hXXps://hackread[.]com/intelbroker-home-depot-employees-data-breach/
[4] hXXps://hackread[.]com/hackers-claim-hewlett-packard-data-breach-sale/
[5] hXXps://hackread[.]com/shinyhunters-twilio-authy-phone-neiman-marcus-truist-bank/

Ticketmaster, an American ticket sales and distribution company, in BreachForums for a cost of USD 500,000.[6]



[Owner] ShinyHunters

Bossman

ADMINISTRATOR

Posts:	29
Threads:	5
Joined:	May 2023
Reputation:	1,086

ShinyHunters' BreachForum profile
Source: ZeroFox Intelligence

ZeroFox had not observed activity from ShinyHunters since April 28, 2025, when they posted a PGP-signed message to the front end of the now-defunct breachforums[.]st, claiming that a recent disruption to the domain had been caused by a zero-day vulnerability affecting MyBB software. No further activity was observed until June 3, 2025, when a ShinyHunters post claimed that the newly launched breach-forums[.]st is BreachForums' "new, official" domain and that efforts to restore legacy infrastructure and member ranks were ongoing—as was the rectification of security flaws identified during their "audit and rebuilding process."

- While ShinyHunters did not claim to know which actor or entity had compromised the breachforums[.]st domain, they did allude to attempts by "various agencies" to access a BreachForums database—almost certainly alluding to LE entities.

[6] hXXps://www.reuters[.]com/technology/cybersecurity/live-nation-probing-ticketmaster-hack-amid-user-data-leak-concerns-2024-06-01/

On April 15, 2025, the breachforums[.]st domain displayed an error code and has since remained inaccessible. As a result, significant speculation surrounding the outage underpinned discussion within DDW forums and Telegram channels, with many speculating LE involvement.

- 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.
- BreachForums was allegedly relaunched on June 3, 2025, within a new domain: breach-forums[.]st. However, the domain did not gain traction, and a frontend message stating that BreachForums is for sale appeared within a few days of the "relaunch." The domain is inaccessible as of the writing of this report.

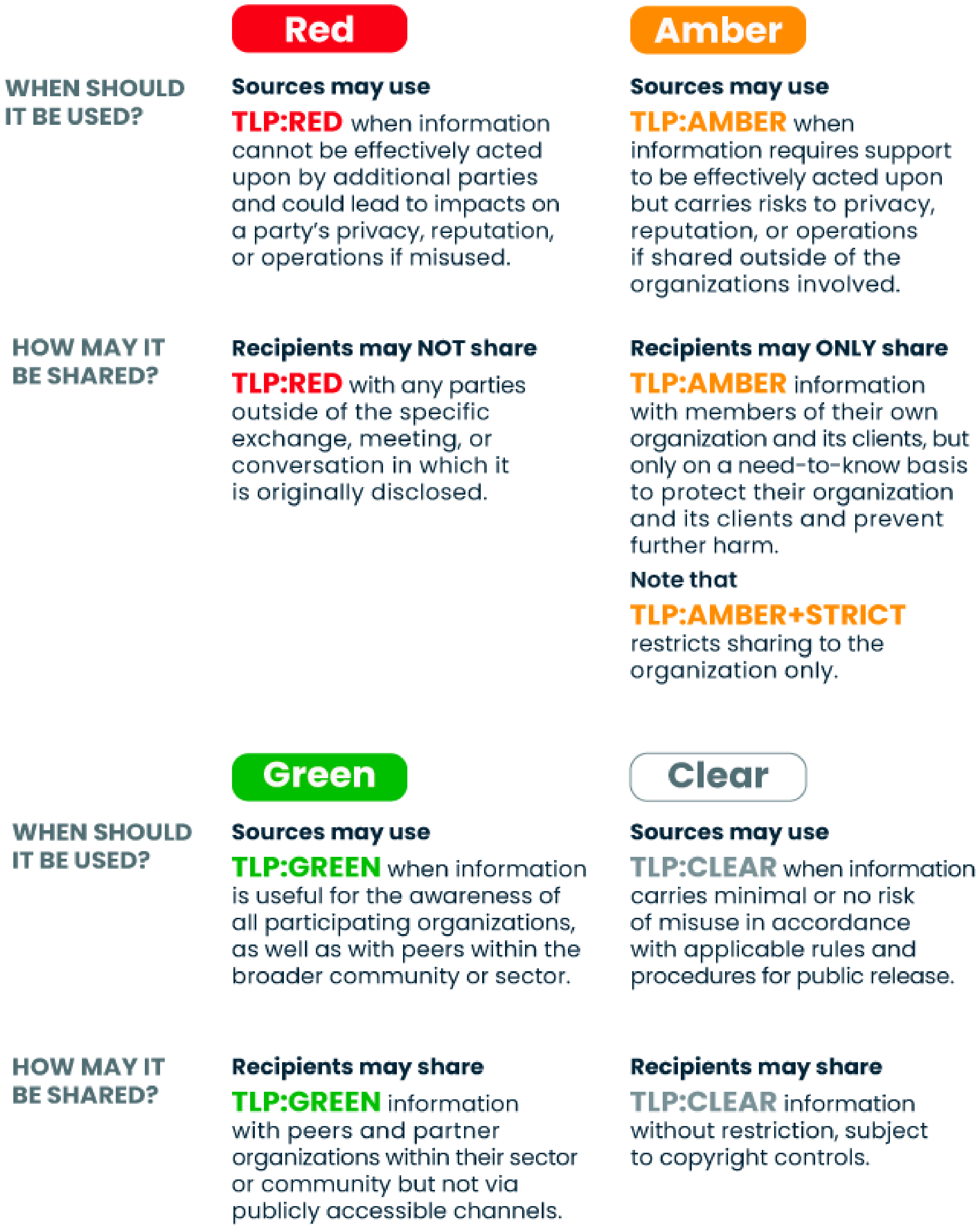
BreachForums is unlikely to make a successful comeback or relaunch, regardless of the presence of IntelBroker and ShinyHunters. Despite once being one of the most popular and prominent deep web hacking forums, there is a very likely chance that many members perceive a higher risk from using the forum, which is likely exacerbated significantly following the recent arrests. Peer hacking forum DarkForums is very likely to continue growing in popularity amongst BreachForums members, with many perceiving it as the closest and most convenient alternative.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi-factor authentication (MFA), establish secure and complex password policies, and ensure the use of unique and non-repeated credentials.

- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

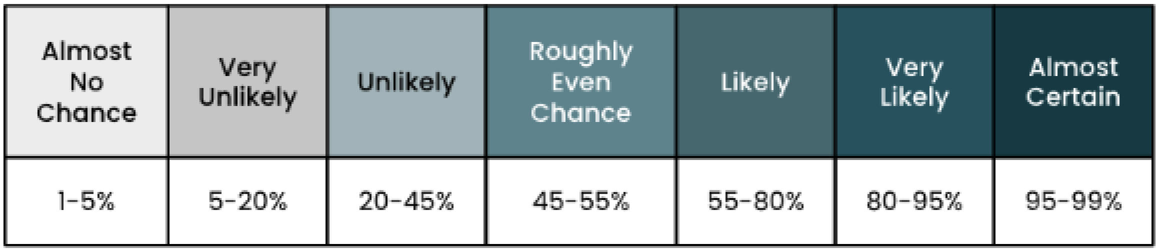


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively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