



| Flash |

First Potential BreachForums Successor Announced

F-2024-05-20a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep & Dark Web, Threat Actor

May 20, 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 PM (EDT) on May 20, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | First Potential BreachForums Successor Announced

› Key Findings

- On May 16, 2024, threat actor “USDoD” announced on X (formerly, Twitter) their intent to launch a new, open-source data breach forum named Breach Nation.
- USDoD stated their intent for Breach Nation to serve as a successor to BreachForums, which was severely disrupted on May 15, 2024, by a law enforcement (LE) operation that seized the forum’s [.]st domain, a [.]onion domain, and a Telegram channel.
- There is a roughly even chance that Breach Nation will become a popular tool for threat actors seeking to discuss techniques, tactics, and procedures (TTPs) related to data breach attacks, publicize results, and sell stolen information.
- It is likely that, in the coming months, other BreachForums members, moderators, and staff will seek to capitalize upon its disruption by creating and advertising new forums.

Details

On May 16, 2024, threat actor USDoD announced on X their intent to launch a new, open-source data breach forum named Breach Nation. USDoD claimed that Breach Nation will use two separate domains, breachnation[.]io and databreached[.]io, with a planned launch date of July 4, 2024.

- USDoD has previously been referred to as “NetSec” in malicious forums and has allegedly been responsible for data breaches targeting numerous, primarily Western organizations.
- The actor had previously announced their retirement from cybercriminal activities in an April 21, 2024, deep and dark web (DDW) post.

My goal is to revive the community and provide opportunities for everyone. I am not affiliated with the old staff, but I promise to do a better job and keep the legacy alive.

I am not concerned with who is in charge at the Department of Justice or who the FBI director is. My focus is on keeping the system running.

Regarding the CDN with all databases, I have a plan. I cannot promise to have a full CDN at launch, but I am working on it.

At present, I am the sole admin and staff member. I am aware of individuals who were active previously, but for now, I do not plan to appoint anyone as staff for security reasons and due to a limited circle of trust.

I appreciate all the support and feedback. If a significant portion of the community dislikes the domain, I am open to providing a new one. Your feedback is crucial in every decision.

To make things right, I need the community on my side. You don't need to be staff to have a voice or to help us in this new phase. It will be a process, and everyone is welcome.

Best Regards, USDoD, a perpetual Threat Actor

USDoD announces the launch of Breach Nation

Source: [hXXps://x\[.\]com/EquationCorp/status/1791077909999886503](https://x[.]com/EquationCorp/status/1791077909999886503)

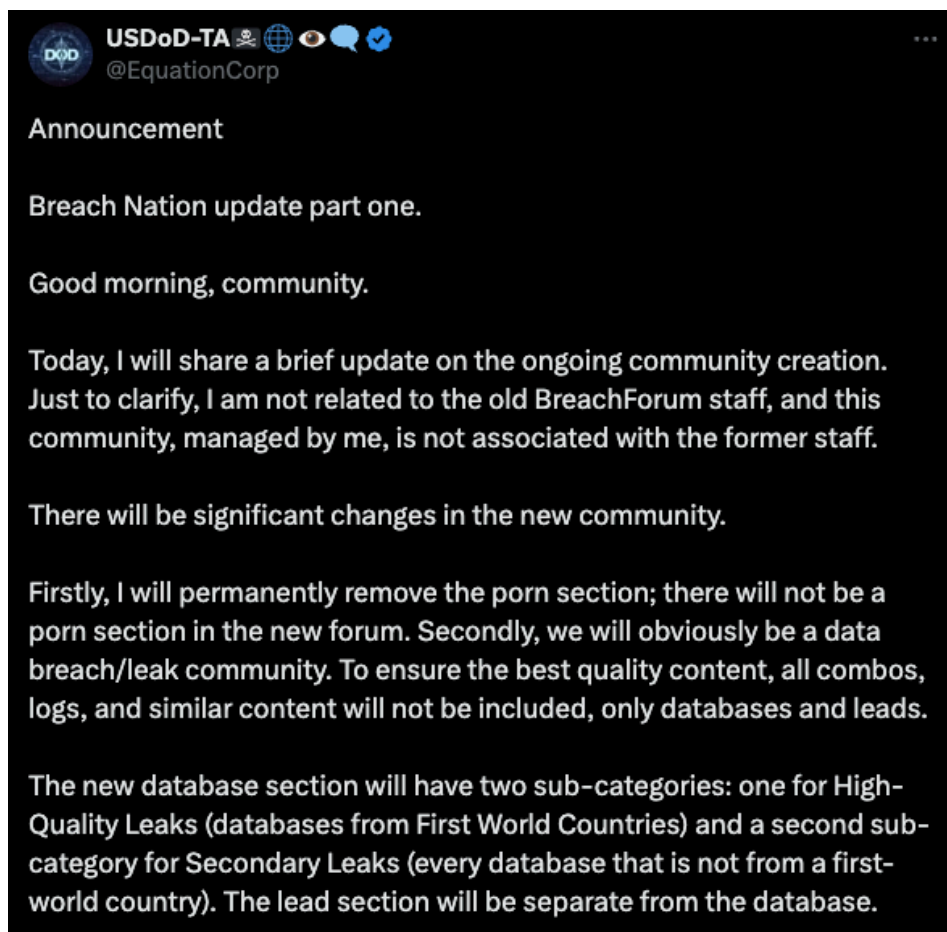
USDoD stated their intent for Breach Nation to serve as a successor to BreachForums, where USDoD was almost certainly a prominent figure—despite denying any affiliation with BreachForum moderators.

- BreachForums was a popular forum consisting of open source and DDW domains, as well as an instant messaging platform. It was severely disrupted on May 15, 2024, by a LE operation that seized the forum's [.]st domain, a [.]onion domain, and a Telegram channel.
- ZeroFox observed unconfirmed reports that the platform's moderator, known as "Bapohmet", was arrested.

USDoD claims to be working alone on the production of the new forum, stating that they are not currently seeking to recruit moderators or other staff due to "a limited circle of trust." This is very likely a reflection of uncertainty amongst DDW communities stemming from recent LE activity, as well as USDoD's likely limited trusted network.

Further detail surrounding the structure, intent, and use of Breach Nation was provided in a second post on May 20, 2024. USDoD detailed two changes that they deemed significant. The post claimed that regular updates as to the forum's status will be provided in subsequent X posts.

- Unlike BreachForums, Breach Nation will not include a pornography section.
- To ensure the "best quality" content, "combos, logs, and similar content" will not be allowed—only databases and "leads." The data breach/leak section will be broken down into two sub-categories: one for high-quality leaks associated with first-world victims and one for all other victims.
- A market section will also be available once an escrow system is established, as well as a threat intelligence section that will reportedly use XenForo software.



USDOD provides insight as to intended Breach Nation features

Source: [hXXps://x\[.\]com/EquationCorp/status/1792571853904511048](https://x.com/EquationCorp/status/1792571853904511048)

USDOD stated that the first 200,000 individuals to become members will receive an upgraded member rank. It is not clear what privileges this will enable. Once the site has a “good amount” of users, the community will transition to an invite-only model. The criteria for granting a member this privilege is unclear at the time of writing.

There is a roughly even chance that Breach Nation will become a popular tool for threat actors seeking to discuss TTPs related to data breach attacks, publicize results, and sell stolen information. It is likely that, in the coming months, other BreachForums members, moderators, and staff will seek to capitalize upon its disruption by creating and advertising new forums.

Recommendations

- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of ransomware and digital extortion (R&DE) threats and their associated TTPs and Indicators of Compromise (IOCs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system and ensure all business IT assets are updated with the latest software as quickly as possible.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Configure ongoing monitoring for Compromised Account Credentials.

| 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%