**Report of Investigation**

Brandon Luff

CYBR6800

April 25th, 2024

**Executive Summary**

The investigation into dark web drug trafficking on Dread's forums revealed an intricate environment where active vendors like WeAreAmsterdam and community members such as EmpBomb advocate for secure practices and safe drug usage. A forum user with the moniker NoseBeers raises questions about product quality and credibility, highlighting the challenges of the dark web marketplace and the difficulty markets have trying to regulate their communities safely. Community discussions on AI moderation and harm reduction initiatives reflect ongoing efforts towards safety. Overall, the findings display the importance of sustained investigation into the workings of dark web drug trafficking.

**Background**

The trafficking of drugs through the dark web has become a major concern to those in law enforcement as well as cybersecurity. The dark web offers excellent anonymity to those who access it most commonly through The Onion Router (TOR). The anonymity provides the perfect environment for criminals to bend and break the laws to sell or purchase illicit items. Additionally, the emergence of cryptocurrencies like Bitcoin allows transactions to be made in a nearly untraceable manner if done correctly. Drug trafficking is arguably the largest component of the dark web black market. The popularity grew as a result of the Silk Road, a major dark web marketplace. The Silk Road handled the sales of illegal goods in exchange for Bitcoin. It has since been taken down by the authorities, but new markets have filled its void. The marketplaces act just like legitimate sites such as Amazon. Some vendors sell products and consumers leave reviews and post on forum boards regarding various aspects of the site.

Law Enforcement has struggled to curb the popularity of such markets, largely because it’s no easy task. Operating Systems like Tails, and browsers like TOR, offer full encryption and anonymization of all actions. Users become difficult to track down and find. As an extra layer of protection, users will create monikers and fake personas to not expose their real identity. The most secure users completely sever their online persona from their real identity, leaving no trace at all. When law enforcement does take down a market, new ones emerge.

**Importance of Topic**

Drug trafficking on the dark web raises significant concerns in a variety of aspects. Dark web markets make obtaining harmful substances incredibly easy, and easy to get away with. The United States is currently in the midst of an opioid epidemic. Opioids are highly addictive and detrimental to users’ health if used incorrectly when not prescribed by medical professionals. Drugs are often laced and contain additional unlisted chemicals resulting in severe conditions or death. Those who become addicted pose risks not only to themselves but to those around them. Aside from taking the drugs, the possession of them often contributes to crime and violence, whether it be larger scale and gang-related, or smaller scale and simple theft on the street.

Many marketplace users view these markets as positives, however. The larger and well-known sites have made a collective effort to create a safe and secure environment where vendors have to gain trust within the community. Testing has become a large factor as well. Forums and markets will offer services to have vendors' drugs tested to ensure they are selling what they claim to be. Those who violate the rules will be banned from the forums. Consumers also take to the forums to review products and give future customers an idea of who to buy from for the best experience. The overall line of thought is that if people are going to do drugs, allow them to do it safely.

There are major implications to consider on both sides of the argument, many points of which are valid. There’s no doubt that dark web forums have likely caused many drug-related problems, yet at the same time, it very well may have saved some lives as well. Regardless, it’s imperative to study and analyze the current state of these marketplaces to be better able to protect and keep the world safe.

**Scope of the Investigation**

The scope of the investigation involved digging through the dark web to discover marketplaces and forums where drug-related activity was occurring. The goal is to find individuals of interest to develop and gain an understanding of how these sites function, how vendors conduct their business, how consumers interact with vendors and other consumers, and how users behave in general.

The full scope of the investigation was able to be achieved through the use of one online forum called Dread. Dread is one of the most popular forums currently available on the dark web. The forum is designed in nearly the same fashion as the popular clear website, Reddit. Users sign up for an account and there are ample sub forums and communities to browse through. Just like Reddit, there is a score system for those who are active. Each community has its own moderators and set of rules, while the site as a whole has its terms of service. Dread is run professionally.

Upon exploring the Dread forums, a variety of vendors and consumers were identified as people of interest, and research was conducted on them. The vendor brands that were identified were “WeAreAmsterdam,” and “AbascusMarket.” The admins of Dread were identified as “HugBunter,” “Paris,” and “Solar.” Additionally, there is a Dread moderator that was identified as “Shakybeats”. Furthermore, the users and vendors that were identified go by the monikers of “EmpBomb,” “NoseBeers,” and “dontlaugh.”

**Analysis of the Evidence**

Upon arriving on Dread’s forums, the first vendor found was WeAreAmsterdam, which owns their sub-forum within Dread for them to conduct their business. On their home page [Exhibit A] they provide general information about the vendor and how to conduct business with them. They provide mail addresses for direct contact and encourage encryption through their PGP public key [Exhibit B] which they provide. The vendor boasts fifteen years of experience and claims to be professional. Links to additional markets where they can be found are also provided. Overall, their posts on their forum do not get very much engagement and there are very sporadic posts with the latest being three weeks ago, followed by three months ago, and then five ago. However, Dread has tagged them as a high-quality vendor. Periodically, the vendors host giveaways, “LOTTERY2 GUESS NUMBER 1 - 100 || WIN 200 EURO WORTH OF PRODUCT OF CHOICE. EVERY MONTH WINNER!” Users pick numbers in the replies to find a winner. The winner of this particular contest was EmpBomb, who was the closest picking sixty-nine while the number was seventy.

While this contest was conducted four years ago, the user EmpBomb is still active on the forum, and most active on the drug-related forums. Their involvement in communities comes mostly from replies as opposed to starting threads of their own. While reviewing their account it was found that EmpBomb is a sub-forum mod, different and lower than a Dread mod, and is a premium member of the site. Additionally, their PGP key is attached to the profile [Exhibit C]. In a sub-forum called /d/CafeDread, a community for general discussion about the site, EmpBomb was found discussing the dangers the Telegram app poses to dark web users. Telegram is a communication app and can be used in browsers or through a mobile app. Many vendors are now utilizing the app to conduct business. However, EmpBomb warns against this as they state law enforcement will use the app to span the bridge between the clear web and the dark web and bust vendors and then their consumers. People often use their dark web personas on Telegram and due to the app being a clear web application, it can leave an unwanted trail. Instead, EmpBomb encourages the usage of TOR, PGP, and burner accounts.

Within /d/CafeDread, there was a recent posting about a new AI that was launched on the forum to serve as a moderator to relieve some of the responsibilities of the admins. The posting was very lighthearted as the AI has not been functioning as intended and needs significant improvement. Many of the Dread admins and Dread mods were found in this post discussing the future of this AI. Shakybeats, HugBunter, and Paris’ PGP keys can be found in [Exhibit D]. An important note about all found PGP keys is that none of them display version or device information within their key indicating good operational security. Investigating further into the admins, they posted a harm reduction page detailing their efforts to create a safe environment with trusted vendors selling safe products [Exhibit E]. This line of action is seemingly accepted across the dark web with users wanting a pro-drug world where drugs can be done safely.

Browsing through the site, the top donators page was found with the top all time donators being a user called NoseBeers. This raised the question as to why this user donated so much and what his connection to Dread is. In a post, NoseBeers was found stating, “Who are we? a long time vendor who worked with partyisland 8 years ago the top vendor of all time, since then we have supplied Australia with pure cocaine then changed to making our own designer drug of cocaine as we knew how it was ruining people's lives plus always cut/toxic chemicals added for the end users. We didn't agree and went our own way making top sales for cocaine in Australia for last 2 years, but we've been a vendor since dream market on and off for the last 8 years We are number 1 donators for dread we support health and safety.” This post was taken from the middle of a dispute between NoseBeers and another user dontlaugh. Both users are vendors for a larger network of vendors. The community is very suspicious of NoseBeers because a user named wilsonone tested his product and found that it is not cocaine being sold. NoseBeers denies the claims [Exhibit F]. NoseBeers claims to be a part of AbascusMarket, but is not listed on their homepage as a member. Overall, NoseBeers claims to have existed on DreamMarket, another forum, eight years ago under a different name, held Bitcoins when the site went down, and using the Bitcoins has re-emerged on Dread as a vendor selling questionable Cocaine to Australians. This is an interesting character that would likely require more investigation. Their PGP key [Exhibit G], indicated their prior alias was Snow Nose, which matches the claims of being on DreamMarket.

**Findings of the Fact**

* WeAreAmsterdam: WeAreAmsterdam operates a dedicated sub-forum on Dread's forums, offering drug-related services. Their forum page provides contact information, including a PGP public key for encrypted communication. Despite sporadic engagement, WeAreAmsterdam is recognized as a high-quality vendor. Periodic giveaways are used as promotional tactics, with winners like EmpBomb emerging from these contests.
* EmpBomb: EmpBomb, an active participant and sub-forum moderator on Dread, advocates for secure communication practices such as TOR, PGP, and burner accounts. They caution against the use of Telegram due to potential law enforcement surveillance risks.
* Dread's AI Moderator: Dread administrators and moderators discuss the introduction of an AI moderator, expressing skepticism about its efficacy. Key figures involved include Shakybeats, HugBunter, and Paris.
* Harm Reduction Efforts: Dread administrators prioritize harm reduction initiatives, creating a dedicated page outlining efforts to foster a safe environment with trusted vendors selling quality products.
* NoseBeers: NoseBeers, a significant donor to Dread, faces scrutiny regarding the quality of their products. Allegations of misrepresentation and disputes surrounding their offerings raise questions about their credibility and potential implications for Dread's community.

**Conclusion**

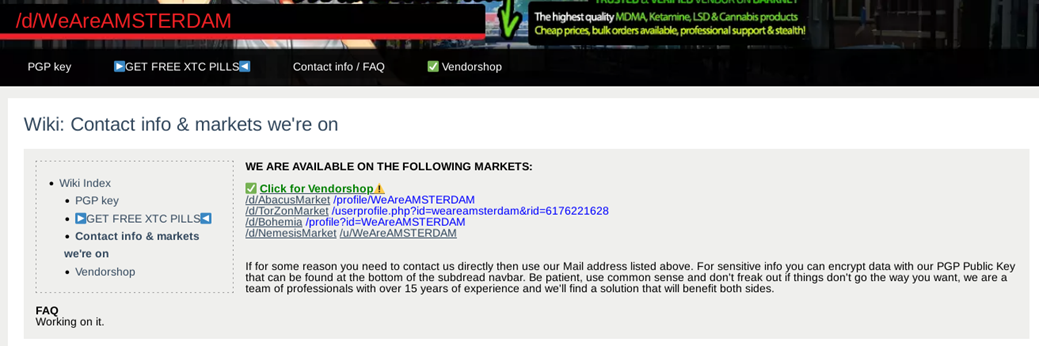
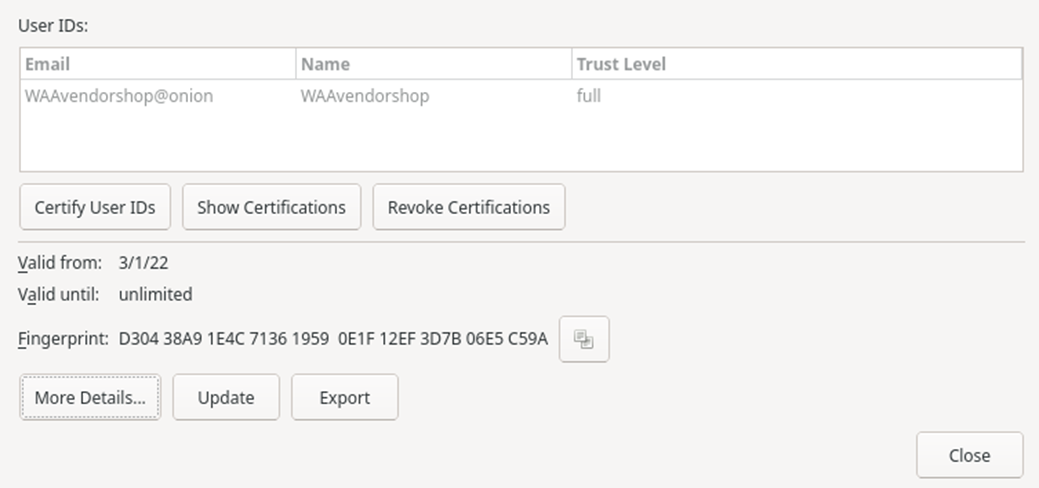
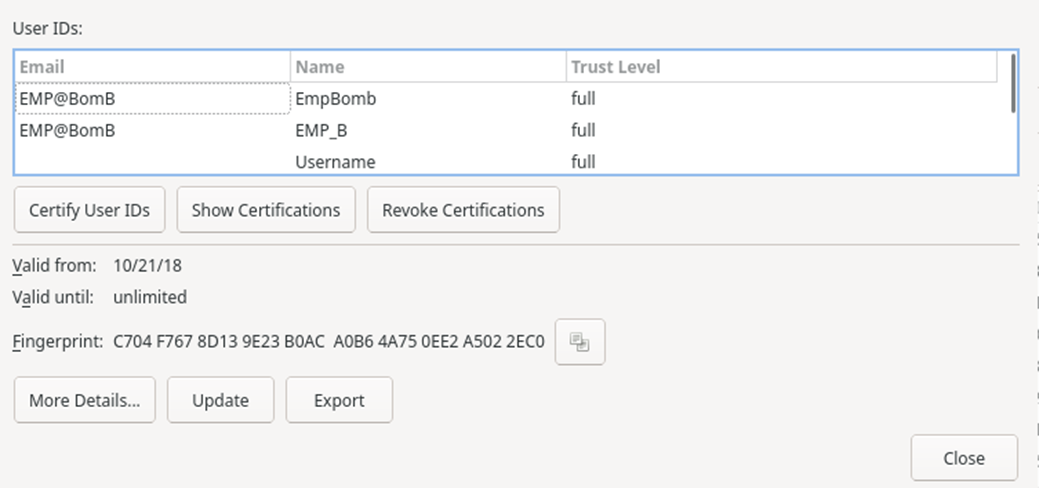
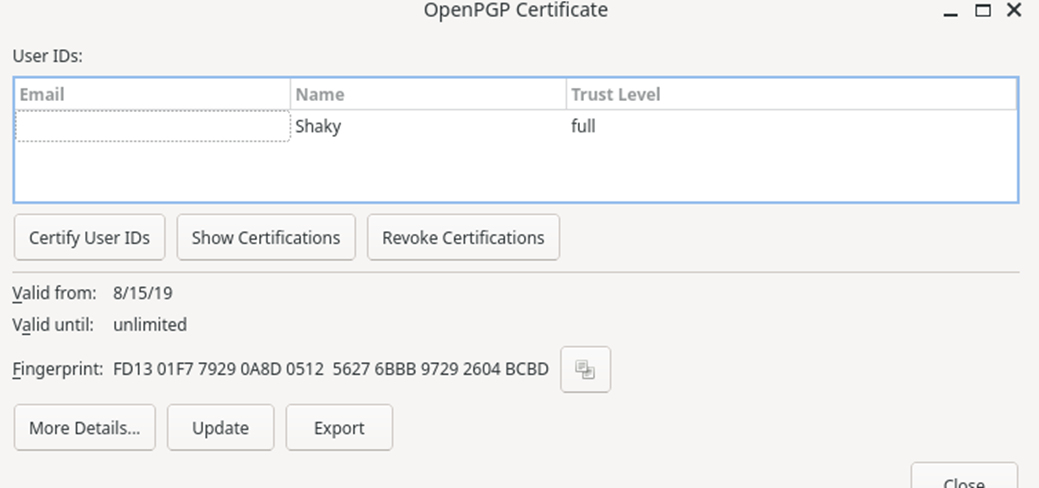
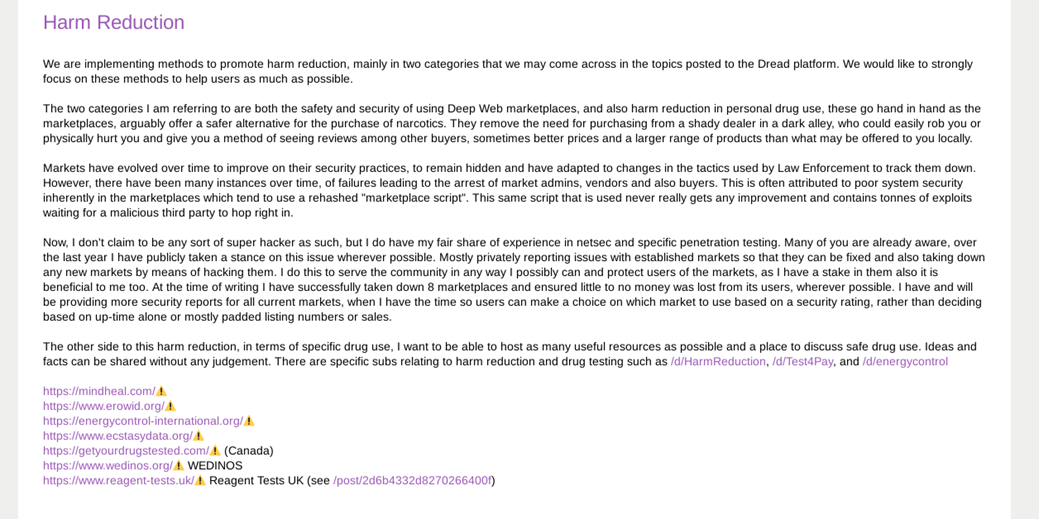
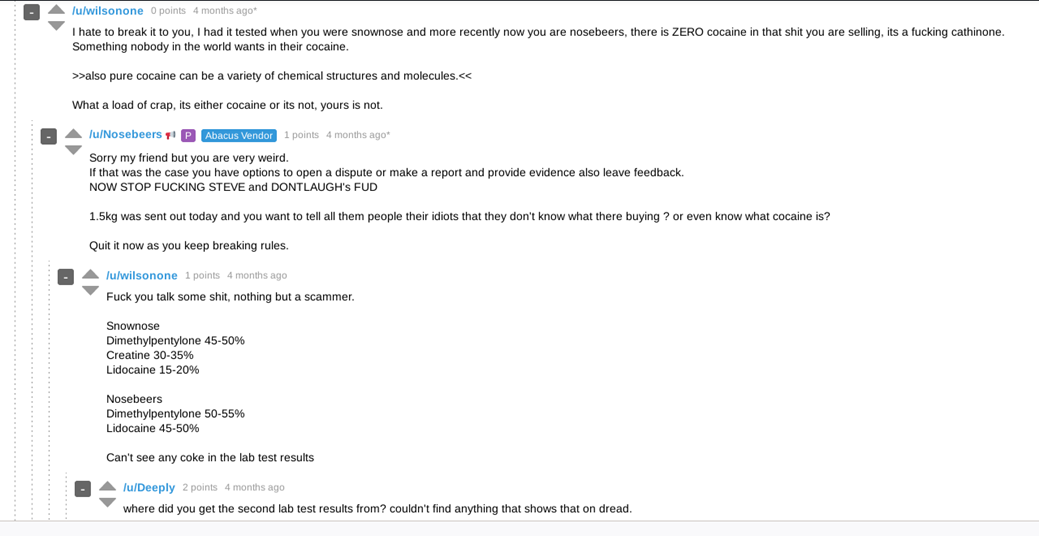
In conclusion, the findings reveal a diverse landscape within Dread's forums, characterized by active vendor engagement, community discussions on security measures, skepticism towards AI moderation, and ongoing efforts towards harm reduction. NoseBeers has been identified as a particularly interesting figure, displaying the complexities and controversies inherent in the dark web drug trade.

**Link Analysis Chart**

**A diagram of a network

Description automatically generated**

**Exhibits**

1. 
2. 
3. 
4. 
5. 
6. 
7. 