VERACODE

More Than Tor: A Deep Dive

BEN BROWN, *Principal Security Researcher*

1 Executive Summary

The terms darknet or dark web are often presented within a context of misleading framings and sensationalist spin with the main focus being the Tor network. With reports of digital bazaars for guns, drugs, human trafficking, and hitmen for hire, is the image of the dark web portrayed by law enforcement and the media accurate? What about the other extant darknet frameworks? A true understanding of the dark web would be both impossible and misleading if the only focuses were the Tor network and potential criminal activity. This research aims to expand the field of view to encompass other types of dark web content that can be found among the non-Tor frameworks such as Freenet, I2P, and OpenBazaar. The users of these darknets, and their aims, ideologies, and activites don't tend to fit with the mainstream picture that has been painted of them. This paper also looks at the origins and technical underpinnings of these darknets as well as said actors and offerings. There will be discussion of the differentiators that set these networks apart from each other and why they too should be included in modeling knowledge of the dark web. Here the aim is to have readers walk away with a more complete understanding of the internet's hidden corners, the goals of its users, and the technologies that help keep them in the dark.

2 Context Overview

2.1 Definitions

Darknet: A framework with accompanying software and configurations for running and accessing a specific overlay network (e.g. Tor, I2P, Freenet, etc.).

Dark web: Web content that resides on overlay networks, or darknets, and requires specific software, configurations, or authorization to access.

Clearnet: The traditional World Wide Web content, often search engine indexable.

3 Methodology

3.1 Research Environment

A virtual machine instance with a clean install of Windows 10 Pro x64 was used for each darknet install and configuration. All communications with the darknets and their clearnet download sites were performed through a Virtual Network Provider (VPN).

3.2 Candidate Identification

The initial list of darknet frameworks identified for liveness testing and content relevancy checks includes anoNet, Freenet, GNUnet, I2P, Netsukuku, OpenBazaar, Particl, Perfect Dark (パーフェクトダーク), Retroshare, and ZeroNet. Excluded were those frameworks that were easily determined to be defunct and those in development that had not yet reached their public alpha/beta stage.

3.3 Liveness Testing

Of these darknets there were two frameworks that were struck from the list for lack of network liveness. It was found that anoNet's .ano TLD server and Public DNS recursor (required for browsing anoNet network sites) were unresponsive and their Tor web proxy had been disabled. There is no information on the official website (last updated 2014-05-27 13:00 GMT) or Wikipedia entry concerning the current

network status. In their development comments and listserv messages, the Netsukuku developers noted the temporary suspension of the network while the codebase is being overhauled. The latest status update on Netsukuku 2.0 work was provided by the head developer on 2018-08-13[1].

3.4 Content Discovery Methods

Freenet websites were found using the built-in search functionality of the Freenet client, entries in the official wiki, third-party metalists, automated network crawlers, and announcements via the FLIP (Freenet IRC).

GNUnet, Perfect Dark (パーフェクトダーク), and Retroshare content was found using the built-in keyword search functionality. Additionally, Perfect Dark searches were done in both English and Japanese.

I2P websites were discovered using official and unofficial jump services on the network that employ aggregators and liveness testers.

OpenBazaar listings were found using both the official and unofficial listing services to manually comb through offerings in each category.

Particl's marketplace can be keyword searched; however, given the very small number of listings it was preferable to simply show all listings for all categories and manually check them.

ZeroNet content was discovered using the listings of the official ZeroHello site, the 0list service, and the Kaffiene search engine.

3.5 Content Relevance Checks

A further qualifier was applied to the candidate list concerning network content relevance. Research was focused on items related to application security, exploits, attack tools, cybercrime enabling services (e.g. money laundering, hacked accounts or systems, database dumps, hacking services, identity theft artifacts, etc.), other items relevant to corporate threat modeling or business continuity, and content of note that may serve as a differentiator between darknets. As a result, GNUnet, Particl, Perfect Dark (パーフェクトダーク), Retroshare, and ZeroNet failed to provide content of significant interest.

4 Tor

4.1 Mission

Tor's stated goals are to: Protect your privacy and defend yourself against network surveillance and traffic analysis. Another major (and more recent) goal is to bring wider access to anonymous web browsing through increasing user-friendliness, not something you see as a major goal for the darknets other than Tor and OpenBazaar.

4.2 Users and Content Languages

For the Tor network the top countries of origin, in descending order, for mean daily users were The US, Germany, the United Arab Emirates, and Russia[2] with content being overwhelmingly English language oriented.

[1] https://www.netsukuku.network/2018/08/iota.html

[2] https://metrics.torproject.org/userstats-relay-table.html?start=2017-01-01&end=2018-09-30

5 OpenBazaar

5.1 Network Topology

OpenBazaar is a decentralized P2P network built around the InterPlanetary File System (IPFS) protocol. IPFS is a distributed file system using a block storage model leveraging the Bitcoin blockchain protocol. IPFS also uses a BitTorrent-based protocol for block exchanges. The sale of goods through OpenBazaar is governed by Ricardian contracts that oversee the liability of one transaction party to another and create a cryptographically signed record of agreement between the two parties in the exchange which cannot, presently, be forged post-signing and checksum hashing. Payments are carried out with cryptocurrencies in either a direct buyer to seller exchange or in a moderated exchange using an escrow. This is done using a three party multisignature ("multisig") scheme where release of funds requires at least two of the three parties involved, the buyer, the seller, and the moderator. The moderator need only intervene if some dispute arises between the buyer and seller.

5.2 Mission

Intent tends to vary between darknet creators and users as well as over time. Some of them, like OpenBazaar, have pretty clear alignment of intent, in this case a feeless, peer-to-peer marketplace that leverages cryptocurrencies for transactions.

5.3 Users and Content Languages

It was difficult to get user demographic information for OpenBazaar, however it is worth noting that while all of the listings observed were in English, the developers have prioritized support for additional languages including Brazilian Portuguese, French, and, in the near future, Spanish. As for the most used transaction currencies, in descending order, the US Dollar led the pack followed closely by Bitcoin with Euros, the Pound Sterling, Canadian Dollars, and Russian Rubles bringing up the rear[3].

5.4 Interesting Content Findings

While OpenBazaar wants to move away from the stigma of the traditional darknet markets, like those found on Tor and I2P, there were still some similar listings such as those for illicit narcotics, identity theft and fraud artifacts, hijacked accounts, hacking tools, and hackers for hire. However, the vast majority of listings were for mundane items you wouldn't typically find on the Tor darknet markets, things like handmade jewelry, original art pieces, used books, phone cases, clothing, and houseplants.

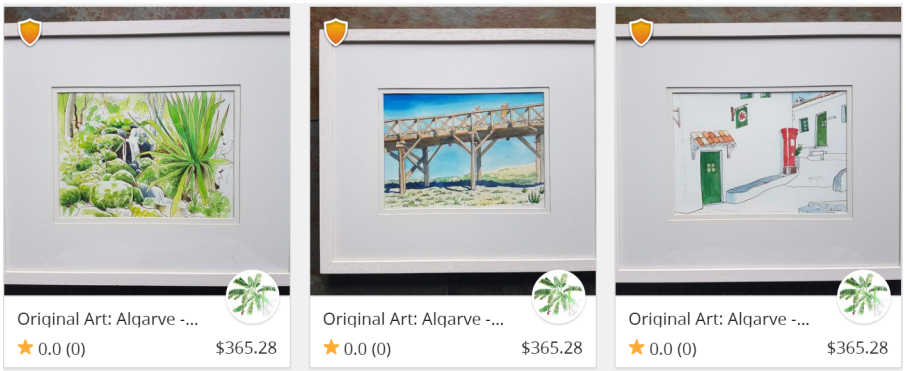

FIGURE 1: Original art for sale on Openbazaar

[3] https://blockbooth.com/stats/

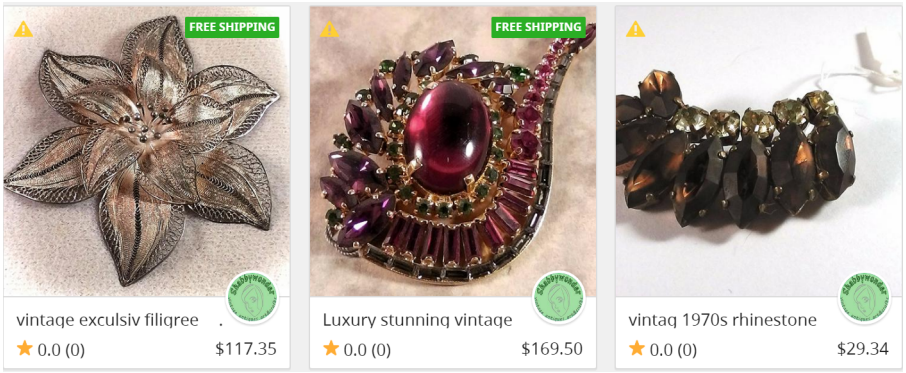

FIGURE 2: Vintage jewelry for sale on OpenBazaar

6 Freenet

6.1 Network Topology

Freenet is a peer-to-peer (P2P) platform that both retrieves and stores information using a decentralized distributed data store spread among peer nodes. There are no central servers; instead, the network relies on its users to contribute bandwidth and storage space to keep it running. Both the relaying of requests and the data itself are encrypted. Content is introduced to the network using ephemeral publishing nodes and then distributed to the hosting nodes via encrypted blocks that are independently handled and stored. Unlike many other P2P systems Freenet administrators cannot, currently, enforce any type of ratio system rating nodes based on their upload to download differences. There is no designed hierarchical topology, so individual nodes moving information do not know if the previous or subsequent node is an originator, destination, or relay node. The network employs a key-based routing protocol that can be run in either a darknet mode where only known, manually added nodes are used or in opennet mode where faster, topologically closer, nodes are used and then forgotten in FIFO order. Document originators can choose to use Content Hash Keys (CHK) that employ SHA-256 to obtain a hash of a document, which is built on a post-encryption hash of the original data, to transport the information requested for reassembly and decryption by the requesting node. Alternatively, document originators can elect to use Digital Signature Algorithm (DSA)-backed Signed Subspace Keys (SSK) for public-key cryptography to be verified by each node along its path.

6.2 Mission

The Freenet project states that Freenet "is a peer-to-peer platform for censorship-resistant communication and publishing" and focuses heavily on the promotion of freedom of speech over censorship, copyright, and takedown.

6.3 Users and Content Languages

Freenet's distribution of user nodes are largely concentrated in the US, Germany, the UK, and France with smaller, yet significant collections in Japan, Russia, and Brazil[4]. This matches well with the content languages observed: English, Japanese, French, German, and Russian.

[4] "Measuring Freenet in the Wild: Censorship-resilience under Observation" Stefanie Roos, Benjamin Schiller, Stefan Hacker, Thorsten Strufe

6.4 Interesting Content Findings

Freenet did indeed have content that could also be found on Tor, things like database dumps, pilfered politician emails, internal law enforcement documents, poison and bomb guides, as well as malware how-tos. The difference? While these types of offerings are for sale on Tor's darknet markets, Freenet users offer them to anyone free of charge. Freenet also has a few things not currently found on Tor or the other darknet frameworks tested, including darknet-only sites for terrorist groups such as the Order of White Knights and the Animal Liberation Front. There was even a Chinese language freesite with a detailed plan for assassinating China's president Xi Jinping. All this being said, the lion's share of freesites were personal blogs, political movement sites, codesharing initiatives, a surprising amount of amateur novelists, and social hubs.

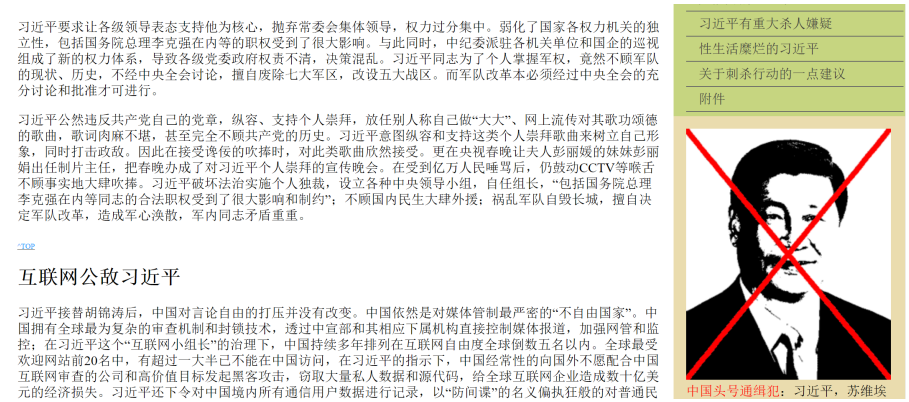

FIGURE 3: Assasination plan for Xi Jinping found on Freenet

FIGURE 4: French language philisophy blog on Freenet

FIGURE 5: Libertarian Marxist blog on Freenet

7 I2P

7.1 Network Topology

I2P is a decentralized P2P network that uses a distributed hash table (DHT) to build its network database and a modified Kademlia algorithm to determine node ("router") closeness. Clients on the network query this network database to interact with other clients. Messages on the network are addressed to a receiving client's cryptographic identifier ("destination") and transported through unidirectional inbound and outbound "tunnels" that support pooling, mixing, and explicitly delaying messages for increased anonymity. These tunnels are built using end-to-end (E2E) encryption, specifically ElGamal/AES+SessionTag[5].

7.2 Mission

The I2P project states that I2P "is intended to protect communication from dragnet surveillance and monitoring by third parties such as ISPs" and is "used by many people who care about their privacy: activists, oppressed people, journalists and whistleblowers, as well as the average person."

7.3 Users and Content Languages

The geographic locations for I2P peers saw the US, Russia, and the UK holding the lion's share with fewer, but still greater than 4,000, in France, Canada, Australia, Germany, and the Netherlands[6].

7.4 Interesting Content Findings

I2P also provided offerings that can be found on Tor, though with important differences. A ready-to-go SPECTRE exploit with instructions was available, free of charge. Money laundering services were also on the table, though most of them involved a very little known cryptocurrency out of Russia called GOSTcoin. In one of the forums discovered there was a hacking sub-section with hacking tutorials, Distributed Denial of Service (DDoS) for hire, and partnership requests offering to pay botnet admins for use of their farms. This research also uncovered an eepsite for "SecOps, sysAdmins, & Activists" that offered free use of their website vulnerability scanner, web-based DDoS tool, and live classes for various hacking topics and techniques. The most interesting part of this was that it looks like one of the advanced courses was taught to these "activists" by a Director level security professional working at an industry leading company.

[5] https://geti2p.net/en/docs/how/elgamal-aes

[6] "An Empirical Study of the I2P Anonymity Network and its Censorship Resistance" Nguyen Phong Hoang, Panagiotis Kintis, Manos Antonakakis, Michalis Polychronakis

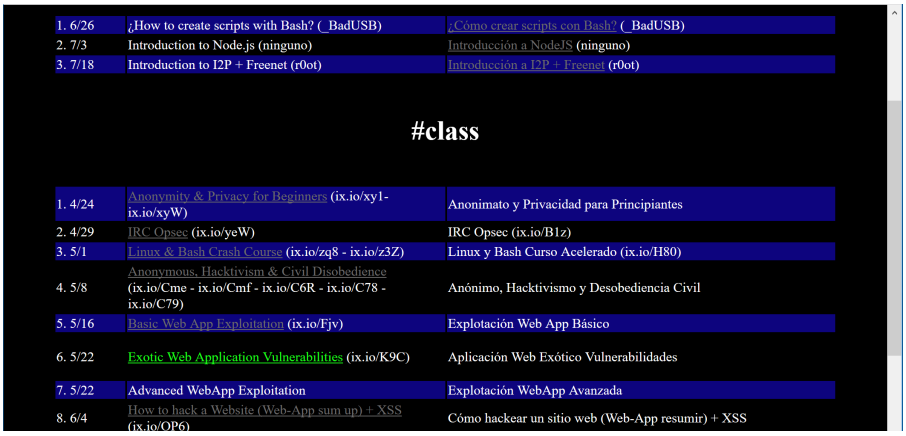

FIGURE 6: Live hacking classes taught on I2P

Like Freenet and OpenBazaar, these types of offerings were in the minority. Most of the content on I2P is comprised of things like personal blogs, (mostly European) political party eepsites, gateways to other darknets, ASCII and other digital art pieces, social media platforms, chat services, hobby forums, Git repos, filehosting services, pastebin clones, PGP keyservers, and a few individual gems like a service for playing live, anonymous chess matches, and an interactive ESP test.

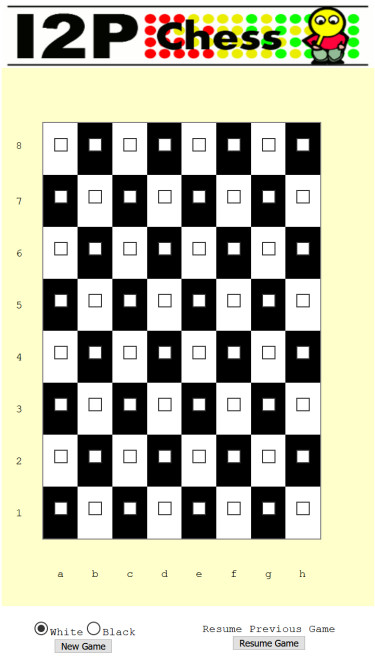

FIGURE 7: Anonymous chess on I2P

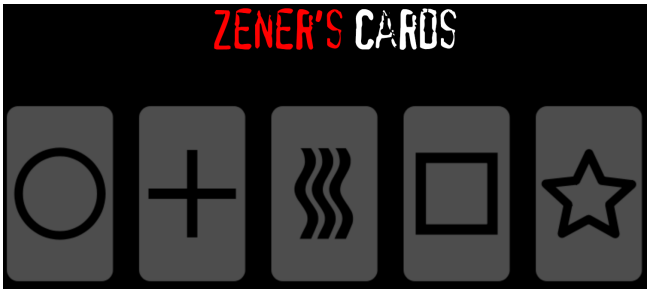

FIGURE 8: Interactive ESP test on I2P

8 Conclusions

When the dark web is discussed by the media or public sector they often evoke an image of some hidden and shielded den of crime populated by anonymous ne'er-do-wells engaged in illicit affairs. While this narrative is useful for getting views and justifying enforcement budgets, it can also lend itself to skewed threat modeling and unfocused alarm. The majority of the content found was in most cases rather benign. The criminals offering or seeking illicit goods or services were present on each of the darknets, but made up a small minority of the network activity and content.

Despite major darknet market takedown operations like Onymous and Bayonet there has been neither an explosion of new marketplaces, as seen after the Silk Road takedown, nor has there been large migrations to other darknets. In looking at the differing topologies, user bases, and content focuses, the case against mass migrations becomes clearer. For I2P and Freenet the pre-existing pools of potential buyers are orders of magnitude smaller than that of the Tor network (think tens of thousands vs approximately 2 million). On top of this those pre-existing user bases aren't really focused on the types of commercialized offerings and interactions that the Tor markets deal in, users there are more likely to give away crime oriented tools, exploits, guides, and training. As seen in the OpenBazaar content sweep the commercialization is there, but the focus isn't criminal enterprise so much as mundane goods and services. Porting extant buyers and vendors from Tor runs into issues of lower name recognition and higher technical barriers to entry. With their unfimiliarity, more complicated installs and configurations, and very different topologies, the concept of moving to another darknet can be daunting for Tor buyers, sellers, and developers.

Much more of this type of commerce is found on the clearnet (typically in forums, many with vetting systems). These forums, typically in English, Russian, or Chinese, are where most of the online cybercrime economies thrive. In the case of vulnerabilities and exploits, they are sold out in the open by legitimized firms such as HackingTeam, Gamma International, and Zerodium.

While the dark web should have a place in many entity's risk analysis and threat modeling, it is important to understand both the sort of content that is contained or trafficked on the dark web and the scale of this activity when compared to other theaters such as meatspace, over telecom systems, or on the clearnet. With this in mind remember that buying weapons is often much easier and less expensive through legitimate venues or off the street, human trafficking is by and large the domain of word of mouth and Craigslist-like clearnet sites, and there are no legitimate hitmen for hire on the dark web, no matter what the media may say.