Dark Web Investigation Assignment

Date : 29 – 09 - 2025

Raj Shekhar - 240545002004

Objective: To understand the methodology and challenges of a dark web investigation by passively analyzing an illicit marketplace, focusing on evidence collection without direct interaction.

---

1. Setup

The first step involved creating a secure and isolated digital environment to ensure both safety and ethical compliance. A virtual machine (VM) was configured with all persistence and file-sharing features disabled, acting as a disposable computer. If the VM were compromised, it could be deleted without affecting the host operating system.

The Tor Browser was installed within this VM to access .onion websites. Using a dark web search engine, often referred to colloquially as an "Onionland" search, the marketplace known as "SilverLine Shop" was located. The investigation was strictly passive: no accounts were created, no items were purchased, and no communication was initiated with any vendors or administrators. Snapshots of the VM were taken before and after the session to preserve the state of the environment for reproducibility.

---

2. Analysis

The analysis focuses on how the Tor network facilitates the anonymity that marketplaces like SilverLine Shop rely on. A standard connection through Tor is routed through three relays: an Entry Node (which knows the user's IP but not the destination), a Middle Node (which only passes encrypted data), and an Exit Node (which connects to the public internet and only sees the traffic, not the user).

However, for .onion services like SilverLine Shop, the model is even more secure. There is no exit node. Instead, the connection is established through a Rendezvous Point, a third node chosen by the Tor network that allows the user and the hidden service to connect without either knowing the other's real IP address. This architecture makes it exceptionally difficult for law enforcement to locate the server hosting the marketplace through traditional network surveillance.

This means that investigations cannot rely on intercepting traffic to find a server's location. Instead, they must pivot to other avenues of evidence, primarily the metadata and operational details that users inadvertently leave behind.

---

3. Findings

Through passive browsing of SilverLine Shop, several key pieces of evidence were identified without any login or interaction:

- Illicit Goods: The marketplace openly advertised and sold various controlled substances and banned medicines, with listings for drugs like MDMA being clearly visible.

- Payment Method: All transactions were conducted using cryptocurrency, which provides a pseudo-anonymous but publicly recorded ledger of transactions.
- Vendor Clues: Several vendors made critical operational security mistakes by leaving identifiable information in their public profiles. This included:
    - Cryptocurrency Wallet Addresses for receiving payments.
    - Contact Emails, such as *johnmilles@tutanota.com*.
    - PGP Public Keys, used for securing communications but which can also serve as a unique identifier for a vendor across different platforms.

These findings are typical of the "digital traces" that form the backbone of many dark web investigations and SilverLine Shop was found openly promoting illegal drugs and medicines in exchange for cryptocurrency. Without engaging with the site, metadata such as wallet addresses and possible contact emails were visible. Some vendors also shared PGP public keys, indicating efforts to secure communication with buyers

---

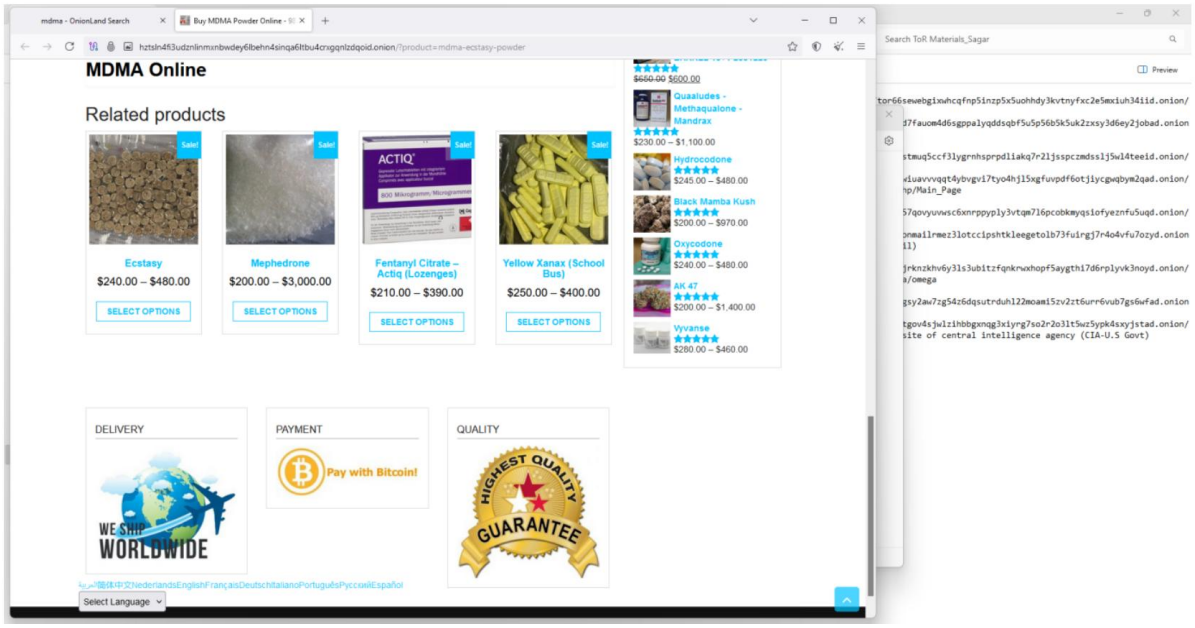

Fig1: SilverLine shop Page

4. Conclusion

This investigation demonstrates that valuable intelligence can be gathered from dark web marketplaces through safe, passive observation. The core evidence—crypto wallets, contact emails, and PGP keys—is often available without needing to engage directly with the illicit service, maintaining ethical and legal boundaries.

The fundamental challenge remains the powerful anonymity provided by the Tor network, which renders direct technical de-anonymization of users or services nearly impossible. Therefore, a successful investigation cannot rely on a single method. Progress depends on combining the gathered metadata with other techniques, such as blockchain analysis to trace cryptocurrency flows, OSINT (Open-Source Intelligence) to link online identities, and formal legal cooperation to compel information from service providers. In this landscape, these small pieces of information become the most critical leads for advancing an investigation.
