

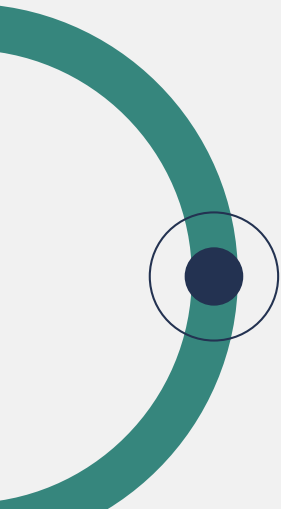
Topic : De-anonymizing of
entities on the onion sites operating on TOR
Network

Domain : Cybersecurity

Team ID :183

Team name : Crimechasers

Team members :SHRYITHA(2303A51637)
VAISHNAVI(2303A51554)
RITHU GOUD(2303A51641)
VARSHITHA(2303A51927)
KAVYASRI(2303A51929)



Objectives

1. Purpose

- Create tools and techniques to assist law enforcement in identifying operators of illegal marketplaces.
- Target de-anonymization of individuals running **onion sites** on the Tor network.
- Address activities such as drug trade, weapons sales, and data leaks.

2. MAIN GOALS:

- Identify Real IP Addresses
- Extract Personally Identifiable Information (PII),
- Disrupt Illegal Activities,

EXPECTED OUTCOMES:

- Real IPs of dark web operators uncovered.
- Names, locations, and identifiers collected.
- Marketplaces dismantled;
- illicit operations halted.



Problem Statement

1. ADDRESSING PROBLEM STATEMENT:

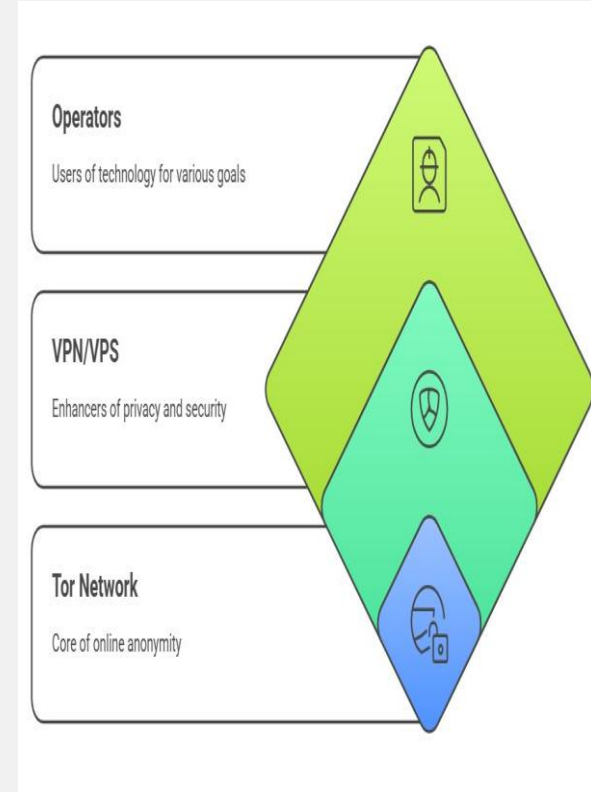
- ❑ Illegal marketplaces on the dark web (hosted as onion sites on the TOR network) are used for selling drugs, weapons, stolen data, fake currencies, and more.
- ❑ These sites are highly anonymous, making it very difficult for law enforcement agencies (LEAs) to trace the people behind them.

2. Challenges in the Current Scenario:

- ❑ **Anonymity Tools:** Tor and VPNs hide operators' real IPs, making tracking difficult.
- ❑ **Encrypted Networks:** Tor's layers of encryption protect operators' identities.
- ❑ **Global Hosting:** Operators use servers worldwide, adding complexity.

3. Key Pain Points:

- ❑ Difficulty identifying operators.
- ❑ Challenges in gathering PII.
- ❑ Unable to stop illegal activities without tracing sources.



Existing system

1.Current System :




- Law enforcement uses manual investigation, OSINT, and network forensics.
- Efforts include tracking leaked credentials, monitoring forums, and analyzing traffic patterns.
- Some tools exist for dark web crawling, but de-anonymization remains a major challenge.

2.Limitations & Inefficiencies:

- **High anonymity** in TOR v3 hides IPs effectively
- **VPN usage** further masks operators' identities.
- Manual methods are **time-consuming and resource-intensive**.
- Lack of automation in extracting PII or network-level leaks.
- Limited visibility into onion service infrastructure.

3.*Why a New System Is Needed*

- To enable faster, automated identification of illegal onion site operators.
- To assist LEAs with accurate, traceable evidence
- To improve cybercrime response time* and reduce operator anonymity.

 Feature	 Current Method	 Proposed System
Identity Tracing	Manual & partial	Automated & targeted
IP/VPN Detection	Very limited	Improved detection techniques
PII Extraction	Requires extensive effort	Semi/fully automated
Investigation Time	High	Reduced
Accuracy & Efficiency	Low to Medium	High

Proposed system

1. New System Introduction:

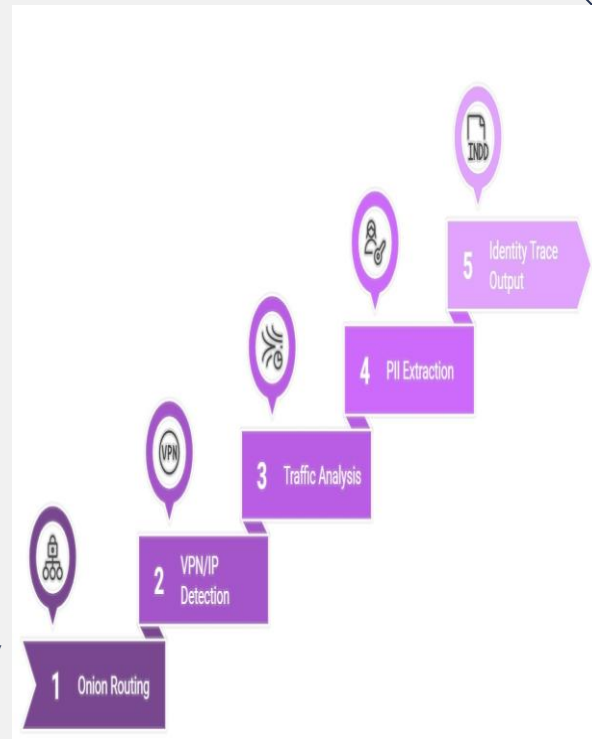
- ❖ A toolkit to identify operators of illegal marketplaces on onion sites using automated analysis, traffic tracing, and data correlation.

Advantages Over Existing Systems :

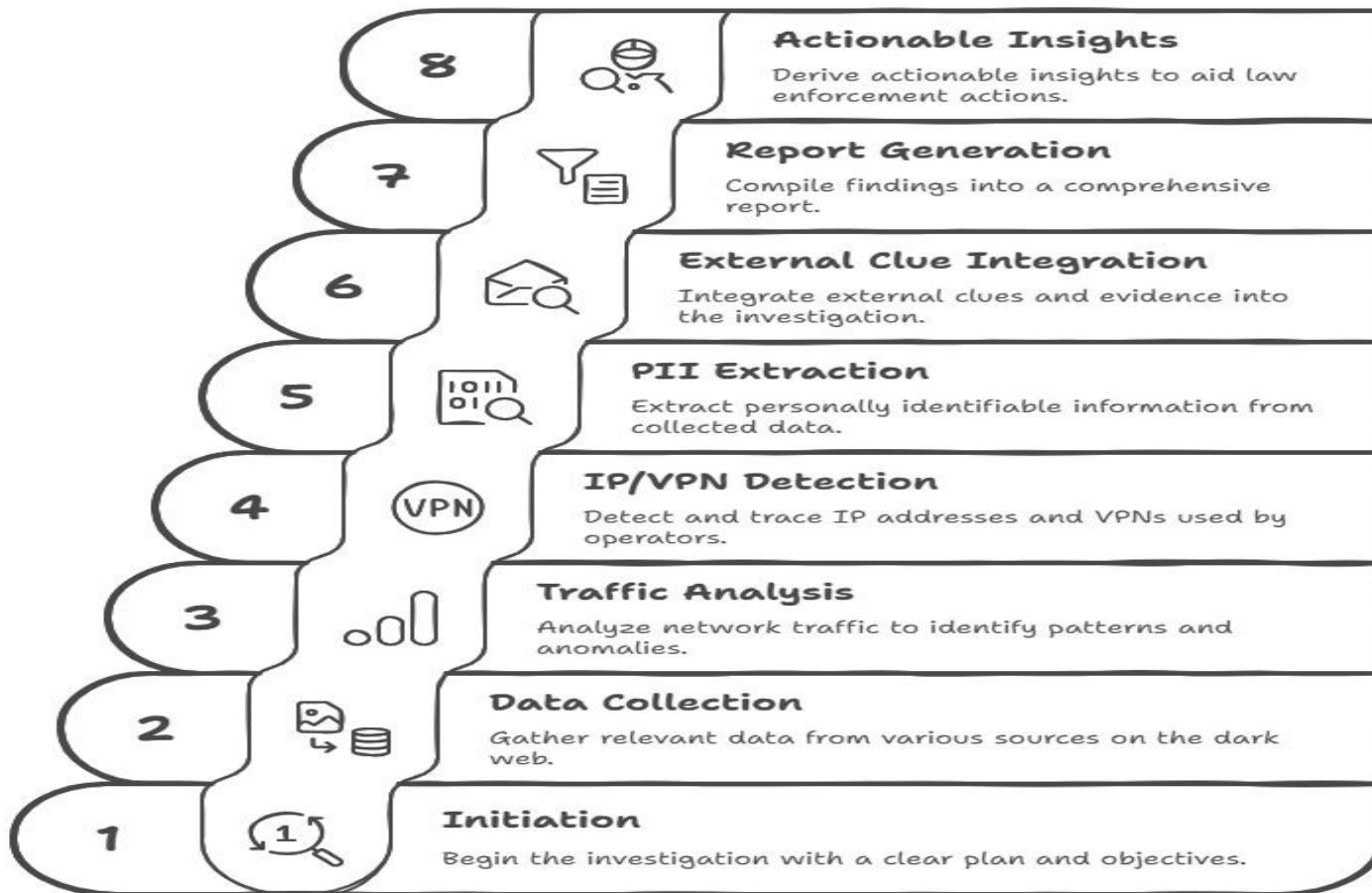
- ❖ Enhanced ability to track real IP addresses hidden by VPNs and anonymity tools.
- ❖ Improved methods to extract PII (names, locations, identifiers) of operators.
- ❖ Supports dismantling illegal marketplaces faster and more efficiently.

Key Features & Functionalities :

- ❖ IP/VPN Detection Module: Tracks potential real IP or VPN IP used behind the onion site.
- ❖ PII Extraction Engine: Scrapes hidden metadata, credentials, and identifiers.
- ❖ Traffic Pattern Analyzer: Detects abnormal or suspicious activity behavior.
- ❖ OSINT Integration: Gathers external clues (forums, leaked DBs, crypto wallets, etc.).
- ❖ Real-time Alerts & Reports: Provides live dashboard insights for LEAs.



Workflow



System Architecture

Tech Stack



Java for backend development, Html ,Css, Javascript for frontend



SQL or MongoDB for database management.



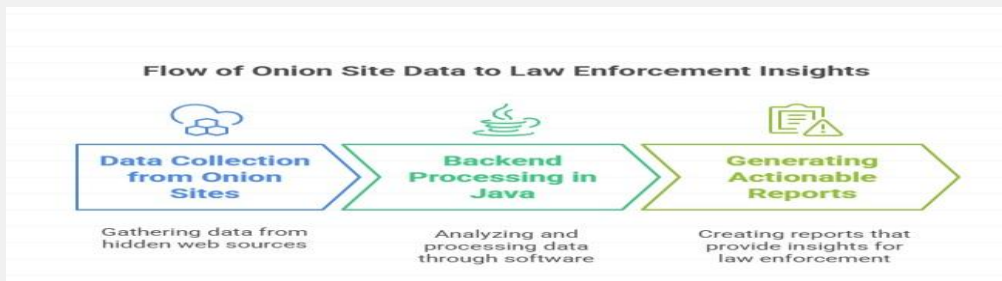
A secure, encrypted database like PostgreSQL or MongoDB to handle sensitive data.



Cloud services like AWS or Azure for reliability and scalability.



Integration with OSINT tools and network analysis APIs to gather external clues and process data



Conclusion & Future Scope



1. **Key Takeaways:** The system helps law enforcement identify operators on onion sites and shut down illegal marketplaces using tools like IP detection and data analysis.*Impact and Benefits:* - Supports faster action against illegal activities. - Enhances public safety by reducing crime on the dark web.
2. **Future Improvements:** - Add predictive analytics to anticipate operator behavior. - Expand to analyze other hidden networks. - Strengthen data security measures.
3. **Conclusion:** This system is a powerful step toward combating dark web crimes and creating a safer digital environment.

