academic publishers

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE (ISSN: 2692-5206)

Volume 04, Issue 10, 2024

Published Date: 27-12-2024

DARKNET BROWSERS: TYPES, CAPABILITIES AND THEIR USE IN CRIMINAL ACTIVITIES

Iminov Abdurasul Abdulatipovich

Head of the Department of Digital technologies and information security,
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan,
candidate of physical and mathematical sciences,associate professor,
e-mail: iminovabdurasul1970@gmail.com

Annotation: This article explores darknet browsers as tools for accessing the anonymous darknet network, their types (Tor, I2P, Freenet), working principles, and technical features. It focuses on the opportunities these browsers offer for both legitimate activities (freedom of speech, privacy protection) and criminal ones (drug trafficking, weapons trade, cybercrime). The use of darknet browsers for illegal purposes and counter-measures against this activity are analyzed.

Key words: darknet, dark web, Darknet browsers, Tor, I2P, or Freenet, onion routing, creation and management of illegal marketplaces, communication between criminal groups, distribution and purchase of illegal content, organization of financial fraud, combating crime on the darknet, international cooperation/

The darknet, or "dark web" is a portion of the internet that is deliberately hidden and requires the use of special tools, primarily darknet browsers, to access. This network, concealed from conventional search engines, has long attracted both those who value anonymity and freedom of expression, and those involved in criminal activities. Darknet browsers, by encrypting traffic and concealing IP addresses, have become both powerful tools for ensuring privacy and a platform for carrying out illegal acts. In this article, we will explore the types of darknet browsers, their capabilities, and the specifics of their use for criminal purposes.

To understand the nature of darknet browsers, it's essential to distinguish between the surface web, deep web, and darknet. The surface web is the part of the internet we commonly use, including search engines, social networks, and websites indexed by search engines. The deep web contains content not indexed by search engines, such as personal data on company servers, online banking, or web pages requiring authentication. The darknet, on the other hand, is part of the deep web but requires special tools, such as Tor, I2P, or Freenet, for access. Darknet browsers ensure anonymity by routing user traffic through multiple intermediate nodes, making it difficult to track their activities.

Several types of darknet browsers exist, each with its own unique characteristics:

Tor Browser: The most popular browser for accessing the darknet. It relies on "onion routing" where data passes through multiple intermediate nodes (relays), each encrypting and decrypting only a portion of the data. This makes it difficult to determine the source and destination of traffic. Tor Browser is free, easy to use, and has a large user community.

I2P (Invisible internet project): I2P creates its own anonymous network over the regular internet. It encrypts traffic and transmits it through a network of I2P routers. I2P offers greater anonymity than Tor but can be more complicated to use.

Freenet: a decentralized peer-to-peer network designed for anonymous access to information. Data is stored in encrypted form on user computers and is accessible through the Freenet network. Freenet also offers a

high degree of resistance to censorship.
Darknet browsers offer a wide array of capabilities that can be used for both legitimate and illicit purposes. Legitimate uses include:
Freedom of speech and circumvention of censorship: In countries with authoritarian regimes or strict censorship, darknet browsers enable communication and dissemination of information without the risk of persecution.
Anonymity and privacy protection: users can protect their personal information and anonymously browse websites.
Circumventing geographical restrictions: access to content restricted by region.
Protection from surveillance: concealing online activities from prying eyes.
Illegal uses by criminals include: drug, weapons, and other illicit goods trafficking: Darknet marketplaces serve as major platforms for illegal trade.
Personal data trafficking: stolen bank details, social media accounts, and other personal information are sold on the darknet black market.
Contract killings: the darknet is used to organize contract killings and other violent crimes.
Cybercrime: the darknet provides a platform for coordinating and carrying out cyberattacks, spreading malware, and organizing DDoS attacks.
Distribution of child pornography: the darknet provides an anonymous platform for the distribution of illicit content.
Money laundering: the darknet is used for the anonymous laundering of illegally obtained proceeds.

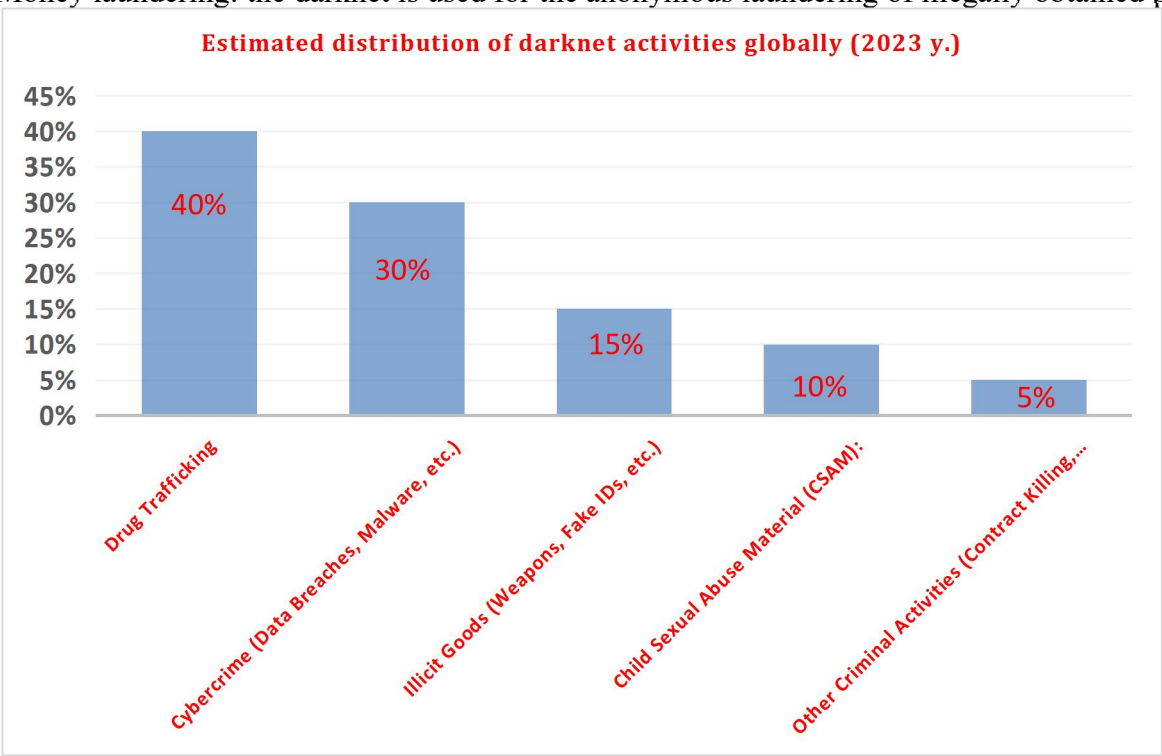

Diagram 1. Estimated Distribution of Darknet Activities

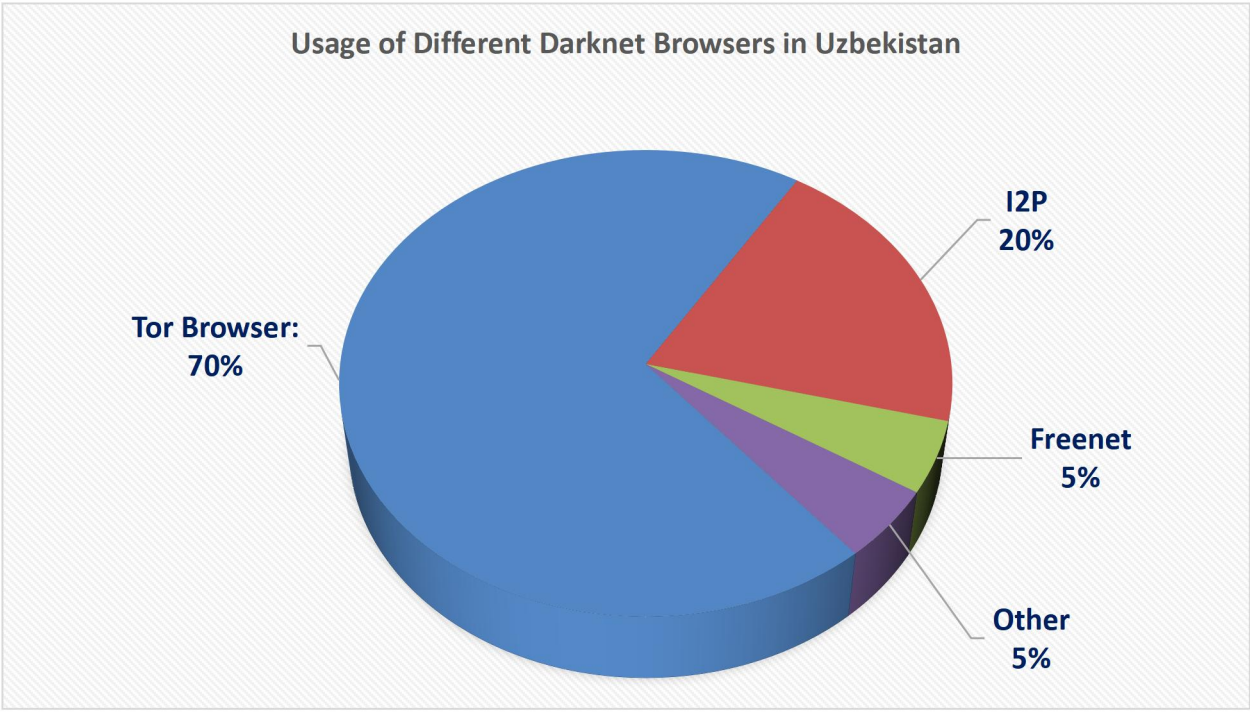

Diagram 2. Usage of Different Darknet Browsers in Uzbekistan

Darknet browsers provide the anonymity that is a key attraction for criminals. This anonymity allows for:
Creation and management of illegal marketplaces: These platforms are hubs for the trafficking of drugs, weapons, and other illegal goods and services.
Communication between criminal groups: the darknet is used to coordinate activities and plan crimes while remaining undetected by law enforcement.
Cybercrime execution: the darknet provides a platform for spreading malware, coordinating cyberattacks, and selling stolen data.
Distribution and purchase of illegal content: the darknet is an environment for distributing child pornography, extremist propaganda, and other prohibited content.
Organization of financial fraud: money laundering, tax evasion, and other financial crimes are carried out on the darknet using cryptocurrencies.
Combating crime on the darknet is a complex challenge for law enforcement. Anonymity, technical complexities, and the international nature of criminal activities make it difficult to track and prosecute offenders.
However, law enforcement agencies are taking the following steps:
International cooperation: law enforcement agencies from different countries are collaborating to fight darknet crime.
Development of specialized technologies: specialized programs and tools are being created to track criminals on anonymous networks.
Conducting raids: regular operations are conducted to shut down illegal darknet marketplaces.
Raising awareness: information campaigns are underway to educate the public about the risks associated with using the darknet.
Monitoring and analysis: new trends in darknet criminal activity are constantly being monitored and analyzed to develop effective countermeasures.
The integration of statistical data, while inherently difficult to ascertain in definitive terms, helps illustrate the scope and severity of criminal activities on the darknet. Both the global view and conceptual data for Uzbekistan provide a vital context for understanding the scale and nature of darknet-facilitated crime. This underscores the necessity for continued research, enhanced security measures, and international cooperation to combat these threats effectively.

List of References and Internet Sources:

1. Goldsmith, J., & Wu, T. (2006). Who controls the internet? illusions of a borderless world. Oxford University Press.
2. Greenberg, A. (2019). This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information. Penguin Press.
3. Olson, P. (2012). We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Back Bay Books.
4. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
5. Tor Project official website: https://www.torproject.org/
6. I2P official website: https://geti2p.net/en/
7. Freenet official website: https://freenetproject.org/
8. Europol (European Union Agency for Law Enforcement Cooperation): https://www.europol.europa.eu/
9. FBI (Federal Bureau of Investigation): https://www.fbi.gov/
10. Academic research papers on darknets and cybercrime (Search through scientific databases such as IEEE Xplore, ACM Digital Library, Scopus).