**INSE6610: Cybercrime Investigations**

**Concordia Institute for Information Systems Engineering (CIISE)**

**Concordia University**

  
**“Study of Underground Hacker Forums”**

* Pranshu Mainrai (40206628)
* Collins Chukwu (40184336)
* Aayush Mehrotra (40191642)
* Ishan Chaudhari (40192935)
* Hussein Al-Masaabi  (40182554)
* Sahaj Vinayak  (40196687)
* Shyamanuj Yadav (40218973)

**Introduction**

The Internet's depths extend well beyond the surface information that many people may quickly access in their routine searches. The additional content is from the Deep Web, which has not yet been included in standard search engines like Google. Content that has been purposefully hidden can be found in the Dark Web's most remote regions or the Deep Web. The Dark Web can be utilized for noble causes as well as to hide illegal or otherwise immoral behavior. Officials and legislators are interested in how the Dark Web is being used for unlawful activities. Individuals can access the Dark Web using special software such as Tor (short for The Onion Router). By routing users' web traffic through several other users' computers, Tor uses a network of volunteer computers to ensure that the originating user cannot be identified from the traffic. Although accessing the Dark Web via these methods does not anonymize activities, some developers have devised solutions, such as Tor2web, that may allow users to access tor material without downloading and installing the Tor program. Once on the Dark Web, people frequently search for content using directories like the "Hidden Wiki," which lists websites according to a category, much like Wikipedia. People can use search engines to look for illegal goods like drugs, weapons, or counterfeit money. These engines might be general or more focused, looking over the Deep Web. People can communicate using the Dark Web via secure email, online chats, or Tor-hosted personal messaging. Although solutions like Tor strive to anonymize content and activity, researchers and security experts continuously create ways to identify or "deanonymize" certain concealed services or people. Tor and other anonymizing systems have been used for both legitimate and unlawful purposes, from safeguarding privacy to selling illicit items that were paid for with Bitcoin or other virtual currencies. They can be used to get around censorship, access content that has been restricted or protect the confidentiality of private discussions or business ideas. However, various nefarious actors, including terrorists, criminals, and state-sponsored spies, can also use cyberspace. The Dark Web can be a discussion, planning, and active place. It is unclear how much of the Dark Web is currently utilized to support a specific black market. It is much more difficult to determine how much traffic is going to any site because of the anonymity provided by services like Tor. Just as criminals can rely upon the anonymity of the Dark Web, so can the law enforcement, military, and intelligence communities. For instance, they might employ it for anonymous tip lines, online sting operations, and monitoring. On the Dark Web, anonymity can protect authorities from being tracked down and hacked. Additionally, it can be used to carry out a covert or clandestine computer network operation, such as the denial-of-service assault, bringing down a website, or intercepting communications. Officials are constantly developing new methods to deanonymize Dark Web activity and cybercriminals.

**Background and related work**

Forums. Web forums are among the first and most fundamental forms of Internet communication, and the idea of a forum dates back even longer. Web forums first appeared in the early 1970s. The emergence of the carding forum Carder Planet in the early years of the new century solidified a paradigm that was imitated by all subsequent forums run by cybercriminals. Cybercriminals still utilize forums now to get guidance and talk about the newest methods and advances, much like they did in the past.

Communication and trade systems have emerged, offering better efficiency, simplicity, and security compared to the cumbersome thread-and-post approach employed by forums. There are centralized systems like blockchain DNS (Domain Name System), i2P, and BitTorrent, as well as messaging services and encrypted applications like Telegram, Wickr, and Discord. Marketplaces and AVCs are two examples of automatic trading platforms that have established themselves in the industry.

Supply and demand are the driving forces behind underground market businesses, just like in standard ones. An instrument or piece of knowledge is worth more the more esoteric it is. In contrast, when a market is oversaturated with products (such as credit cards), the price per unit drops.

In contrast to traditional enterprises, these businesses run more like a market-driven fair economy of buyers and sellers, each of whom serves as an independent contractor and adds value to the community. These independent contractors are free to choose their own hours and frequently have a second job to support their activities.

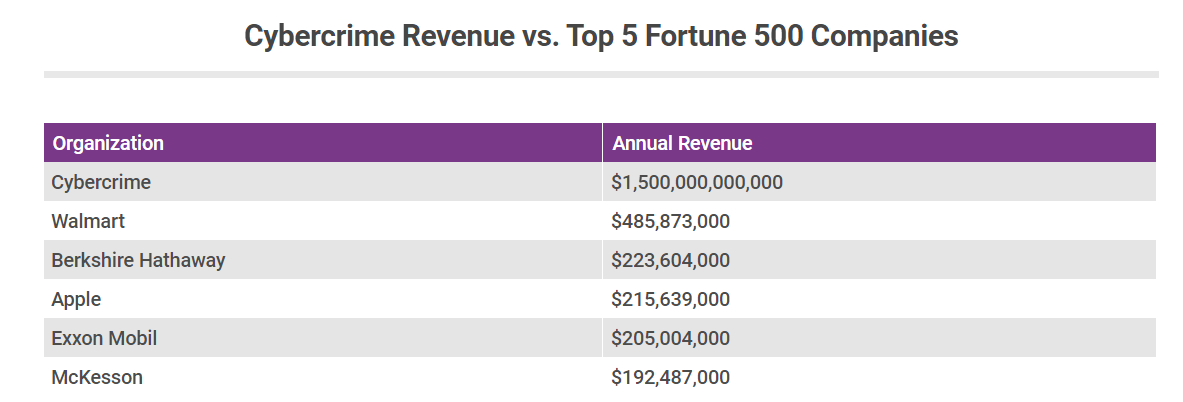
Operating principles and forum regulations are present on hacking marketplaces. A hackers' code of ethics is followed by white hats. The criminal, however, has always behaved unethically.

**Dark-web marketplace transactions**

Since Silk Road, the first successful dark web marketplace, emerged in February 2011, online illicit marketplaces known as crypto markets have drawn significant attention from the media, government authorities, law enforcement organizations, and researchers. Although they share many characteristics with genuine online marketplaces like eBay, these new online marketplaces put a strong emphasis on anonymity and security to reduce the risk of identification. The development of crypto markets was facilitated by two online anonymizing technologies. Bitcoin is the first (Bitcoin).

Blockchain-based digital money called Bitcoin is completely decentralised . Bitcoin payments are anonymous until the Bitcoin addresses and transactions can be linked to specific people, even though all transaction data are accessible to the public. The second technology is the Tor network, which builds a barrier between users and the websites they access by routing messages through several relays. This makes it challenging to pinpoint the location of a website user. Administrators of dark websites can escape law enforcement by hiding the location of their website servers. Numerous crypto markets have been established since Silk Road was shut down and its operators were detained in October 2013 because of increased scrutiny from the relevant authorities.

Several illegal online marketplaces have been taken down by law enforcement agencies in a few success stories. However, there are still hundreds of thousands of active dark markets.



Sources: [Into the Web of Profit Report](https://www.scribd.com/document/377159562/Into-the-Web-of-Profit-Bromium-Final-Report) and [Fortune 500](http://fortune.com/fortune500/)

Cybercrime is a very massive business that is rapidly expanding and involves more than simply "hackers in hoodies." As more of our regular activities move online, so too does crime, where the rewards for fraudsters are frequently bigger and the chances of being detected are typically smaller.

**Conclusion**

One of the main foundations supporting the development of the underground economy is underground forums. These forums are appealing sites for young, unskilled people to learn about hacking because of the sense of anonymity they offer and the simplicity of access to attack tools and services. It is possible to think about early intervention strategies to steer these low-level hackers away from illegal activity by analyzing their development. To quickly react to new attack types, it also helps to know who the important players are and what new tools they offer. For instance, antivirus firms should keep an eye on companies who offer tools for evading detection and tracking down new malware types.

To learn more about how people's hacking actions and ideas may be influenced, conversations within these online forums might be researched. Furthermore, it demonstrates the considerable amount of hacking knowledge that can be used to address the key issues society is currently facing with cybersecurity and the shortage of trained personnel. By interacting with these groups, it would be able to direct young people away from criminal activity and toward the increasing number of genuine cybersecurity job openings that are vacant.