

# A Darknet Market Rises

## An Exploratory Single Case Study of the Empire Market

Fredrik Hellström

*Department of Computer  
Systems & Sciences, DSV  
Stockholm University  
Stockholm, Sweden  
frhe0558@student.su.se*

Tomas Olsson

*Department of Computer  
Systems & Sciences, DSV  
Stockholm University  
Stockholm, Sweden  
tool1575@student.su.se*

Richard Wennerstrand

*Department of Computer  
Systems & Sciences, DSV  
Stockholm University  
Stockholm, Sweden  
riwe7471@student.su.se*

**Abstract**—The darknet markets continue to operate without any major disruption. When one market gets seized by law enforcement, another takes its place. Today, the Empire Market is one of the major actors on the darknet facilitating sales of illegal goods and services. Through an exploratory case study of the Empire Market, using both qualitative and quantitative research methods, this study shows that drugs and controlled substances account for most of the available products for purchase on the website. Trust is a valuable commodity and an escrow service is used to gain trust from both sellers and buyers. Bitcoin is the most accepted cryptocurrency by sellers, and the layout of the website is like most other legal websites. Products and service can be searched for and sorted by popularity or origin, for example. Europe is overrepresented in terms of the origin of the product advertisements. The information gathered is discussed and could serve as a useful foundation for future research on the subject.

**Keywords**—Darknet, Dark Web, Markets, Marketplaces, the Empire Market, The Onion Router, TOR, Cryptocurrency, Bitcoin, Litecoin, Monero, Escrow, Crime, Drugs

### I. INTRODUCTION

#### A. Background

Infamous for its anonymity, the darknet with its forums and markets remains much of a mystery to the general public. Generally, anonymity is the key characteristic when accessing this subpart of what is known as the deep web. The deep web is essentially the portion of the Internet which cannot be accessed using conventional web browsers since the darknet has not been indexed by major search engine providers such as Google or Bing. Unlike the common perception, most of the deep web consists of databases, records, and other non-illicit documents [1]. The darknet is only a fraction of the vast deep web and can only be accessed by using

specialized browsers and protocols. One of the most commonly used web browsers for this purpose is The Onion Router, known by most as the TOR Browser [2].

Despite being a small part of the deep web, the darknet is large enough to have harbored some of the largest illegal websites known, the most famous one being Silk Road. The Silk Road website was an online criminal marketplace offering numerous different products, most of them controlled substances which are strictly illegal to sell and purchase. A potential buyer or seller only had to download the proper anonymizing software and acquire the exact URL of the site in order to use its services.

With cryptocurrencies such as Bitcoin, users could remain anonymous while selling and purchasing these illicit commodities. The owner of Silk Road eventually got caught by the FBI and later prosecuted in the United States, but another version of the website was up and running in less than a month's time [3]. Simply put, if you know where to look, you can basically find anything for purchase on these darknet marketplaces: drugs, payment card information, different types of software, weapons, malware kits, and so on.

Law enforcement is working to seize these websites, but despite their efforts, new marketplaces continue to appear rapidly without any meaningful disruption. In 2013, the infamous Silk Road market was shut down [4]. In 2017, two of the largest darknet markets, AlphaBay and Hansa, were shut in a law enforcement crackdown [5]. In 2019, the two largest darknet markets, Dream Market and Wall Street Market, went offline, essentially leaving the throne for a new market to emerge as the new number one the fast-growing Empire Market [5] [6] [7].

## *B. Research Problem*

Today there are numerous markets fully operational on the darknet. The illicit items are purchased online and delivered directly to an address of the buyers' choosing, sometimes with regular postal services. To combat this type of websites and services, we need to continuously learn about them. Understand how these darknet marketplaces operate, why and how their users gain access to these services, and what information that can be found on these illicit sites.

Furthermore, there is currently no scientific, academic research focusing on the Empire Market specifically. With this study, we aim to contribute to this area of research by exploring a darknet market that appears to be on the rise [7].

## *C. Research question*

- What are the main characteristics and traits of the Empire Market?

### *Sub questions*

- What products does the Empire Market focus on, if any?
- What payment methods and currencies does the Empire Market utilize?
- What geographical region does the Empire Market focus on, if any?
- What vendor information is made available to the Empire Market users?
- What user information of potential buyers is made available to the Empire Market users?
- What activities occur on the forum associated with the Empire Market, if any?
- What information is available on the Empire Market forum, if any?

## **II. RELATED WORKS**

### *A. Darknet*

Today it is easy to explore openly searchable websites on the World Wide Web, using conventional web browsers and search engines. However, some content that resides on the Internet is not indexed and thus not generally accessible through popular web browsers such as Google Chrome, Internet Explorer, Microsoft Edge or Safari. Unindexed web content that is also intentionally hidden – sometimes due to its illicit characteristics – resides on what is commonly referred to as the darknet [8].

The darknet is a global computer network that enables users to utilize certain Internet services anonymously without revealing any trace of their location. Not unexpectedly, some darknet users abuse this level of privacy and conduct illicit activities, including both technology-driven crimes, such as computer hacking, but also activities to facilitate nontechnology driven crimes, such as human trafficking [10].

Due to the growing threat of illicit activities on the web, facilitated by the darknet infrastructure, governments invest heavily, both in security services as well as research, for hampering this development [9]. Consequently, also the scientific community's interest in researching the darknet increases [8].

However, researching darknet activities, like policing associated illicit activities, are problematic endeavors due to increasingly more sophisticated encryption and anonymization techniques. Moreover, also considering the increase of illicit activities on the darknet, there is a continuous need to develop methods and tools for investigating these crimes [8] [9].

Accessing the darknet requires specialized web browser software and protocols, for example, the Tor Browser and the Onion Service Protocol. Although such specialized darknet browsers and protocols are readily available and free to use, traversing the darknet is not a straightforward undertaking and can entail difficulties in discovering, tracking and authenticating websites [8] [9] [11]. These features of the darknet impede both policing and researching Dark Web activities.

### *B. TOR – The Onion Router*

Onion routing is the foundation of what became to be known as TOR and was first developed by the U.S Naval Research Lab. The intention of the project was to enable secure communication over the Internet. The main principle was to route traffic through different proxy servers and applying protection through encryption with every different node used for routing [12]. Despite used for legal activities in the beginning, and serving as an enabler for civic resistance to violations of humans rights e.g., the TOR router is also used by various people for illicit activities, such as using it to access darknet marketplaces to buy drugs [13]. The use of encryption through the TOR browser has been problematic. Several entities have been voicing their concern about what this anonymity is being used for. Governments, intelligence agencies and