The shady economy: Understanding the difference in trading activity from underground forums in different layers of the Web

Abstract—**Underground forums are discussion outlets where criminal communities exchange knowledge about online malicious activities and trade illegal goods and services that promote an underground economy based on malicious software, stolen personal information, tools for financial fraud, drugs and more. Prior work has investigated the interactions between criminals and the type of assets traded in Surface Web forums. At the same time, research evidence suggests cybercriminals are moving their operations to the Dark Web to avoid getting caught and similar research has been carried out in Dark Web forums from different perspectives. However, there is no empirical evidence on how forum criminal activity related to the underground economy takes place in both Web environments. To address this problem, we conduct a quantitative exploratory analysis about the trading activity taking place in four prominent forums in the Surface Web and four in the Dark Web based on the type of posts found in the forums. Then, we compare the data to find differences in the malicious activity observed. Our results show that trading activity is higher in Dark Web forums compared to the Surface Web. We also find that different types of transactions, products and prices vary according to the Web environment.**

Index Terms—**underground forums, underground economy, cybercrime, measurement**

I. Introduction

Underground forums are platforms that facilitate communication among individuals engaging in illegal activities. These forums are used to exchange knowledge and ideas about illicit activities and to trade items and services from an illegitimate origin or purpose. Similar to traditional Web forums, underground users establish relationships to collaborate and to interact with potential trading partners. As a result, underground forums promote innovation in the cybercrime ecosystem and individuals with different levels of expertise are attracted to these communities to obtain resources aimed to perform cyber attacks. According to security firm McAfee, underground cybercrime profits in China have likely already exceeded US$15.1 billion [1]. This deviant behaviour is encouraged by an underground economy where the tools and communication vehicles for miscreants are becoming inexpensive, readily available, and online attacks are monetised.

The underground economy continues to expand through a large number of underground forums dealing with various types of online criminal activities including fraud, abusive monetisation techniques, money laundering, malware distribution, trading illegal physical goods and more [2]. Users advertise products and services in threads across forums, turning them into marketplaces where vendors and buyers trade assets for a price, using different digital currencies and payment providers. Potential buyers either reply to threads in the forum, use a private message service, or use an escrow service to complete the transaction [3]. These forum marketplaces offer plenty of items and services such as stolen personal information, hacking services, malicious software and tools, bullet-proof hosting, currency exchange and even drugs and weapons.

Due to their important role in the cybercrime ecosystem, significant research has been conducted on the Surface Web to better understand the structure and interactions on these forums [3]–[6]. The Surface Web is the portion of the Internet where websites are indexed in the search engines and it is accessible with any browser. Security practitioners and researchers are constantly monitoring forums to detect large data breaches, zero-day exploits and vulnerabilities affecting information systems. Forum marketplaces, for instance, provide valuable information about the state of the underground economy related to emerging threats and attacks that are being traded as goods or services. Analysing these monetisation structures at a large scale is essential to understand the motivations and interests of forum members, which in turn provides insights into the pathways to crime.

However, at the same time, cybercriminals are becoming more sophisticated and continue to improve their methods and techniques to engage in underground communities without getting caught [7]. For this reason, miscreants are migrating to anonymous underground forums within the Dark Web to conduct illegal transactions [8]. The Dark Web refers to websites hosted on networks built on top of the Internet that are not indexed by conventional search engines and only accessible by specialised software such as The Onion Router (Tor) [9]. Tor offers encrypted communications that hamper any attempts by law enforcement entities to uncover illegal activities suggesting that criminals are using hidden outlets in the Dark Web to connect to other individuals and trade illicit items or services [10].

Although a great deal of research has focused on criminal activity in underground forums of the Dark Web from different perspectives [8], [10]–[13], very few studies have compared how the underground economy unfolds in both environments: the Surface Web and the Dark Web [7], [14], [15]. As such, this study seeks to address this gap in the literature by conducting a quantitative exploratory analysis on the trading patterns of several cybercrime-related forums hosted in the Surface Web and the Dark Web and then compare the results to shed light on many elements related to commercial activities in both environments. Our goal is to broadly characterise trading activity in each environment and unveil patterns in products and services offered, prices, payment methods and currencies accepted. We set out to answer the following research question: Does criminal activity in underground forums depends on the Web environment in which they are hosted?

To this end, we crawled eight popular underground forums, all of them dealing with the same type of criminal activities: four in the Surface Web and four in the Dark Web. Our forums deal with topics related to hacking, black-hat activities, financial fraud and stolen data. We extracted all threads (related to trading or not) posted over a period of one year in the same range of dates for each forum. Then, we applied a tool based on natural language processing and machine learning to automatically identify the type of post i.e. whether items are being sold (offered), bought (requested), or currency is exchanged. Additionally, we identity products and prices. Finally, we aggregated our data by environment and performed our analysis to compare forum trading activity in both Web environments.

The results suggest that, in general, trading activity is higher in Dark Web forums than in the Surface Web. At the same time, selling is the most prevalent type of activity on the Dark Web. While this selling activity in the Dark Web is more related to malware, Surface Web forums focus on stolen data. Our analysis indicates that prices are generally higher in the Surface Web; including stolen data and malware. Interestingly, we observed COVID-19 related items for sale at exorbitant prices on the Dark Web. Conversely, buying and currency exchange activities are higher in the Surface Web than in the Dark Web. However, there is a high demand for hacking services on the Dark Web. Moreover, currency exchange activity is mostly based on cryptocurrencies in the Dark Web, whereas on the Surface there is a variety of government-issued currencies and payment systems. In summary, this paper makes the following contributions:

- We studied commercial activity related to trading goods and services in underground forums from the Surface Web and the Dark Web.
- We compared the results of this analysis to understand the underground economy behind forum communities in different portions of the Web.
- We provide a comprehensive overview of underground forums by identifying the type of potential transactions and several product types with different prices.

II. Background and related work

The evolution of technology and the Internet has enabled a wide spectrum of criminal offences that generate revenue for actors conducting these activities. Therefore, over the last decade, criminological research into cybercrime has expanded, with a particular focus on offences related to economic motivation [16]. For instance, underground forums open up cybercrime opportunities for potential offenders motivated to obtain easy money. According to the criminological theory of social learning, individuals gain insights about criminal activities while interacting with others as a natural behaviour in closed communities [17]. Consequently, they acquire the required skills and knowledge to engage in deviant behaviour. A great deal of information and techniques used by miscreants has led to the transformation of traditional forums into underground communities where cybercrime grows exponentially. This criminality is considerably promoted by a thriving underground economy where information about the availability of goods and services is shared by individuals seeking to monetise their illegal activities [18].

Underground forums make available countless products and services that are posted in threads by sellers advertising what they have to offer including price, payment method, contact information and any rules regarding the transaction process. In turn, potential buyers contact the seller to ask questions and discuss the terms of the sale. After an agreement is reached, buyers make the payment and the goods are delivered [19]. Correspondingly, potential buyers make posts to advertise any product or service they are requesting. The myriad of products and services offered includes stolen accounts credentials, credit card data, malicious software, botnets, hacking and cashout services, currency exchange, etc. In terms of payments, several payment methods, currencies, cryptocurrencies and money transfer systems are accepted, or an escrow system is used. The success of these transactions relies on trust and informal social control through forum moderators and reputation indicators [20].

Since forums are a form of an online social network, prior research has analysed underground forums to understand interactions between criminals, the type of assets being traded and reputational factors [4], [21]. Pastrana et al. [18] focused on understanding criminal pathways and characterise key actors related to illegal activities using a social network approach. McAlaney et al. [22] studied discussions within online forums to better understand how individuals may be influenced in hacking behaviours and beliefs. As for analysing the purpose of posts, Caines et al. [23] examined the function and intend of posts from a corpus of several underground forums. Other authors studied private interactions between forum members by identifying whether a thread is likely to generate private messages aimed to complete transactions [6], [24]. Our work also considers intrinsic characteristics of underground forums; however, we specifically focus on the aspects related to the underground economy, such as type of potential transactions, products and prices.

Other researchers have investigated specific types of content on underground forums. For instance, Samtani et al. [5] identified characteristics and functions of hacker assets (tools) that are used in cyberattacks and are obtained within underground forums. Similarly, Fang et al. [25] studied threads related to data breaches. Haslebacher et al. [3] focus on carding forums trading stolen financial data and analyses products, prices, seller prolificacy, seller specialisation, and seller reputation. We differ from these studies as we focus on measuring posts related to the type of potential transactions, a variety of products and prices but not only from forums related to a specific topic (such as carding) but with a broader spectrum in terms of the topics and activities performed on them.

Analysing data from underground forums is a demanding task that involves the review of a large number of posts related to different domains and specific jargon. To overcome this challenge, Portnoff et al. [26] developed a series of tools to extract high-level information from forum unstructured data using natural language processing and machine learning. We leverage these tools to extract data from underground forums at a large scale to answer our research question.

The above studies focused mostly on underground forums positioned in the Surface Web which refers to the indexed and publicly accessible part of the Internet that is searchable using a web search engine such as Google, Bing, Yahoo. Users on this Web environment are subject to being tracked because their browsing histories and IP addresses are not hidden and can be identified [8]. Therefore, criminals are seeking safer alternatives and migrating to the Dark Web to conduct illegal activities. The Dark Web refers to websites on a darknet. A darknet is an encrypted network built on top of the Internet which has been designed specifically for anonymity and is accessible through specific software and tools such as Tor [27]. The Dark Web contain websites (known as hidden services) whose content has been intentionally concealed [28].

A growing body of research has examined underground forums on the Dark Web. Similar to the Surface Web, several studies focused on social network interactions. Nunes et al. [13] analysed forum discussions in the Dark Web to identify vulnerable platforms, vendors and products (e.g. hardware or software) that are at risk to be exploited by hackers. Likewise, Pete et al. [12] explored post discussions from six Dark Web forums to understand networks structures and structural patterns within these communities. Other papers studied the characteristics of hidden services acting as specialised marketplaces more focused on trading items than in engaging in thread discussions [27]. Dolliver et. al [8] conducted a quantitative analysis of drug vendor characteristics on two marketplaces to determine differences among them. Hardy et al. [29] investigated the effect of seller reputation on prices of goods and services in the Silk Road marketplace. It is important to note that our work focuses on underground forums that might include a marketplace section, not in pure marketplaces.

The Dark Web poses a major challenge to law enforcement agencies because the identities and activities of actors involved in criminal activities remain largely unknown. This is a strong incentive to some underground communities in the Surface Web to shift their activities to hidden services in the Dark Web. Although there is a vast amount of forums located in both Web environments, their dynamics, interactions and the goods or services they trade might change depending on the Web environment. Since underground forums drive a large underground economy, it is important to understand the differences between individuals trading in these outlets. As there is no sound information available about it so far, this study shall provide some insight by measuring trading activity on underground forums in the Surface Web and the Dark web and compare the results to understand criminal activity in different layers of the Web.

III. Methodology

In this section, we present the methodology we used for our data collection. First, we developed a web crawler to extract posts spanning a one-year period from a selected group of underground forums from the Surface Web and the Dark Web. Then, we instrumented our crawler with a modified version of the automated analysis tools proposed by Portnoff et al. [26] to retrieve the information we used for our comparison.

A. Forum selection criteria

To add consistency to our comparison, we considered selection criteria based on two conditions. Our forums should deal with similar topics and activities, and the time coverage should be comparable i.e. data should be available for the same range of dates. Therefore, we selected 2 sets of forums (one for the Surface Web and another for the Dark Web) matching our criteria. In the following subsections, we apply our criteria for the selection of our forums.

B. Forum search

To build our forum dataset, we searched for prominent underground forums in the Surface Web and the Dark Web. For a comprehensive list of forums, we used the CrimeBB dataset provided by the Cambridge Cybercrime Centre (CCC). CrimeBB is a collection of posts from Surface and Dark Web forums scraped using the CrimeBot tool developed for researchers from CCC [30]. At the time of writing, CrimeBB hosted data from 18 Surface Web forums and 5 Dark Web forums. However, not all of them met the selection criteria because the time coverage was not comparable. Thus, we searched for additional forums on Google, onion directories and Tor search engines based on our criteria.

Our search resulted in an extensive number of forums for both Web environments. Most of them had been shut down, especially hidden services. From those still active, we first considered forums of the same nature to match our first selection criteria. Then, we chose forums where the same range of dates was available for extraction. Our selection included forums found in the CrimeBB dataset. However, we extracted a more recent version of the data based on our criteria.

As a result, we selected 8 forums (Table I): 4 from the Surface Web and 4 from the Dark Web covering activity over a period of 12 months, specifically from January 2020 to January 2021. Our forums focus on hacking, black-hat activities, malware distribution, financial fraud, stolen data and illegal monetisation techniques.

Hack Forums. According to the Alexa traffic ranking, Hack Forums is the number one website in the ”Hacking” category. It covers a wide variety of topics relating to hacking (tools and training), exploits, malware, stolen data and blackhat activities in general.

RaidForums. RaidForums focuses on "raiding", which is the practice of engaging in online collective activities such as DDoSiNg, doxxing, spamming or trolling. It is an exclusive database sharing and marketplace forum where members trade stolen information. RaidForums is a very popular forum hosting discussions on topics including raiding, hacking, leaks and tutorials.

Cracked.to. Cracked.to focuses on cracking tools and techniques aimed to gain unauthorised access into information systems. It includes database and stolen data trading, illegal monetisation techniques, hacking, etc.

Nulled. Nulled is another cracking community focusing on a wide variety of topics including stolen personal information, databases, social engineering, malware, etc.

CryptBB. CryptBB is a cybercriminal forum in the Dark Web that focuses on hacking, carding and fraud. Initially, it was exclusive for experienced hackers who needed to pass an application process. However, in 2019 a public section was open resulting in a user increase on the site to roughly 10,000 as of August 2020.

DarkWeb Forums (DWF). DWF focuses on several black-hat activities such as hacking, cracking, carding, illegal monetisation techniques, databases and accounts.

Deutschland im Deep Web (DiDW). DiDW is a German-speaking forum covering topics related to hacking, financial fraud, weapons and drugs. This is the only forum in our dataset dealing with drug trafficking but we filtered that data out. DiDW was seized and shut down in 2017 but went online again with different onion addresses.

HM Forum. HM Forum is hosted in the Dark Web and specialises in fraud, carding, stolen financial data and illicit monetisation techniques. It also covers topics about hacking, stolen accounts and leaks.

TABLE I: Number of threads extracted from each forum for a one-year period. *Trading* represents the proportion of posts identified as trading posts. Users account for the total number of members since the forum was created.

	Forum	Threads (Commerce)	Users
Surface	Hack Forums	29,634 (18.69%)	4,971,816
	RaidRorums	8,251 (15.39%)	558,729
	Cracked.to	10,234 (11.13%)	2,128,049
	Nulled	6,805 (12.78%)	4,039,030
Dark	CryptBB	1,617 (23.87%)	≈10,000
	DarkWeb Forums	1,308 (27.68%)	8,892
	Deutschland im Deep Web	5,024 (28.26%)	10,468
	HM Forum	2,740 (24.29%)	11,578

C. Post extraction

Online forums consist of tree structures composed of boards, threads and posts. Boards divide forums into categories for relevant discussions. Under the boards, members create threads by writing an initial post in which other users contribute by posting replies. Our approach is to extract the initial post within a thread. We excluded information about the author because we are not interested in community members. Similarly, we did not include replies to the initial post. According to Portnoff et al. [26], relevant information about trading is found in the initial post of a thread and further replies do not improve the performance of the analysis tools. Some forums have dedicated marketplaces to trade goods and services; however, we observed that commerce threads are posted in different sections across the boards. Therefore, we extracted all the threads for the given range of dates.

To this end, we developed a Web crawler based on Selenium (a browser automation framework used to test Web applications). The main feature of Selenium is the use of a WebDriver which has the ability to drive a real Web browser natively as a user would. We designed our crawler following the strategies proposed by CrimeBoT [30] to collect publicly available data efficiently. We visited the list of forums matching our selection criteria and scraped the posts required for our analysis.

D. Trading information extraction

Based on the tools for automated forum analysis described in Portnoff et al. [26], we developed a modified version that integrates our crawler with the modules that extract the data required for our analysis. We extracted 3 elements from each post appearing in a forum. **Type of transaction** refers to the type of post i.e. the nature of the trading; a user may initiate a post to *buy* or *sell* a product or service, *exchange currency* or a topic related to anything other than trading. It is important to note that we observe the type of posts, not actual transactions. It is not known if the transaction is successfully executed or not. We also extracted the **product** and **price** involved in the post. If a post is tagged as currency exchange, we extracted the currencies exchanged.

IV. RESULTS

In this section, we describe our analysis of the trading activity in underground forums in the Surface Web and the Dark Web. We collected and aggregated data from 4 forums on each Web environment (8 in total) for a period of one year. We extracted 54,924 posts from forums in the Surface Web and 10,689 posts from forums in the Dark Web (see Table II). We used a chi-square test (χ^2) [31] to determine differences in trading activity between both Web environments. Trading threads are more likely to take place in the Dark Web (26.67%) than in the Surface Web (16.05%) ($\chi^2 = 689.83$, p<.001). Moreover, our values are consistent with previous research [26] stating that less than 40% of forums posts are related to commerce.

TABLE II: Number of trading and non-trading threads. Trading threads are more likely to take place in the Dark Web than in the Surface Web.

	Trading	%	Non-trading	%	Total
Surface	8,818	16.05%	46,106	83.95%	54,924
Dark	2,851	26.67%	7,838	73.33%	10,689

A. Type of transaction

Table III shows the type of transaction posted in forums in the Surface Web and the Dark Web. A chi-square test revealed that the type of transaction significantly differs between both environments ($\chi^2 = 1050.01$, p<.001). Overall, selling posts (19.24%) are most likely to take place in the Dark Web while posts related to buying or requesting products (6.85%), and exchanging currency (2.17%) are more likely to occur in the Surface Web. Even though, in general, all kinds of activity (trading and non-trading) is higher in the Surface Web, selling posts are more prevalent in the Dark Web which indicates that hidden underground forums are suitable venues for miscreants to monetise their illicit activities.

TABLE III: Type of transactions. Selling posts are most likely to be found in Dark Web forums while buying and exchanging currency posts are more likely to occur on the Surface Web.

	Sell	**Buy**	**Curr**	**Other**	**Total**
Surface	7.04%	6.85%	2.17%	83.94%	54,926
Dark	19.24%	5.84%	1.60%	73.32%	10,690

B. Products

We identified 3,865 products offered to sell and 3,762 requested to buy in Surface Web forums. For the Dark Web, 2,057 selling posts and 624 buying posts. As stated by Portnoff et al. [26], the product extraction tool only captures one product per post even if there are more. Similar to their work, we sampled 100 posts from the Surface Web and 100 from the Dark Web to confirm that multi-product posts rarely occur. In our samples, only one post offered more than one product for each environment. Also, where possible, we grouped posts selling/buying the same product with a different name. For example, we grouped posts about ”RAT” (Remote Access Trojans) and ”backdoor” because they are the same.

1) Selling Activity: Table IV shows the top 10 selling products for each Web environment. In the Surface Web, most of the goods offered are associated with stolen personal information. This is in agreement with the findings of a previous work [7], showing that exposure of stolen data is higher in Surface Web forums than in the Dark Web. More specifically, online accounts (22.02%) and databases (17.71%) are the products that are for sale the most on the Surface Web. There is a wide selection of account types offered such as email accounts, media streaming services, social media, online stores, payment systems and more. Databases or dumps offered can be email addresses used for spamming, email credentials from free providers or private companies, personal information and credentials from different websites (shops, dating sites, government systems, financial institutions), etc. Also, a high percentage (%12.01) of ”make money fast” schemes are offered. These are paid packages including software, tutorials and resources aimed to conduct affiliate marketing activities. Even though the activity itself is not illegal as claimed by vendors, the packages offered might not work as reported by some users. There is also activity related to malware (botnets: 9.12%) and DDoS services (7.24%).

Regarding the Dark Web, most of the selling activity revolves around malware. Approximately 50% of the posts offer malicious software including RAT (23.52%), botnets (14.01%) and crypters (10.25%). RATs are popular because they give complete access to a victim’s device, allowing an attacker to manipulate files, turn on or off the camera and even the device. A crypter is a tool used to encrypt and obfuscate malware, making it undetectable to antivirus programs. Another prominent activity is money laundering, advertised as ”transfers” (18.11%) where criminals sell money they obtained illegally by transferring it to the buyer’s bank account or any payment system account such as PayPal. There is also selling activity related to financial stolen data such as credit cards credentials (6.17%) and fullz. Fullz are packets of information about individuals. They contain Personal Identifiable Information (PII) such as full name, phone number, address, social security number, date of birth, driver’s license which is used by criminals to commit fraud and identity theft.

In essence, the Surface Web has a higher amount of activity surrounding stolen data, whereas the Dark Web has a larger amount of activity related to malware and financial fraud. Interestingly, we observed several posts offering products related to COVID-19 disease at high prices. We grouped these products under the same tag and we found that 1.76% of all selling posts on the Dark Web are related to COVID-19 goods. These products include antibody tests, N95 masks and drugs that allegedly could be used to treat the disease such as, Chloroquine, Lopinavir and Ritonavir.

TABLE IV: Top 10 most products for sale in forums for each Web environment. Surface Web forums have a higher amount of activity surrounding stolen data, whereas the Dark Web has a larger amount of activity related to malware and financial fraud.

Sell			
Surface		**Dark**	
accounts	22.02%	rat	23.52%
database	17.71%	transfers	18.11%
money	12.01%	botnet	14.01%
botnet	9.12%	crypter	10.25%
ddos	7.24%	credit cards	6.17%
verification	5.31%	ddos	4.47%
traffic	3.09%	fullz	2.33%
proxy	1.97%	accounts	2.02%
rdp	1.28%	COVID-19	1.76%
stock	1.08%	wallets	1.21%

2) Buying Activity: Table V reports on the top 10 products required for buying for each Web environment. Similar to selling posts, buying activity in the Surface Web mostly pertains to stolen data, especially user accounts, which represent around a third of all buying posts (31.61%). Correspondingly, combinations of users and passwords known as ”combos” (7.01%) and databases (3.72%) are popular data-related items requested in Surface Web forums. Furthermore, there is a high demand for DDoS services (8.83%) that are requested to damage specific companies. Posts purchasing hacking services (”hack”) are prevalent in the Surface Web (4.24%). These are requests to gain unauthorised access to accounts, devices, websites or servers. Usually, a specific individual or company is the target but no context is provided in the request.

Hacking services are the most requested services in Dark Web forums. Unauthorised access (18.13%) is requested to download files or execute commands on a website or server. Code for shells (14.03%) and RATs (12.09%) are popular buying items. These requests vary depending on the goal of the adversaries and target system. Likewise, attacks (6.61%), where a hacking method or technique is requested, are among the most popular products to purchase. A high level of buying activity has to do with malware installs (7.15%) that are services aimed to deploy malicious software on devices or network infrastructures as well as set up web hosts that are used to host malware, botnets, phishing sites, spam tools, etc.

While in Dark Web forums buying activity is mostly based on hacking services, in the Surface Web items related to stolen data are the most requested. There is also some level of hacking services requests in the Surface Web; however, these requests do not provide any information about the target. They usually focus on requesting access to a single personal account. Conversely, requests for hacking services in the Dark Web are more sophisticated and provide context about the system such as platforms, vendors, potential exploits, IP addresses, etc.

TABLE V: Top 10 most products required for buying in forums for each Web environment. While in the Surface Web forums buying activity is mostly based on stolen data, in the Dark Web hacking services are the most bought items.

Buy			
Surface		**Dark**	
accounts	31.61%	access	18.13%
ddos	8.83%	shells	14.03%
combos	7.01%	rat	12.09%
hack	4.24%	cryptominer	9.54%
databases	3.72%	install	7.15%
e-whoring	1.96%	attack	6.61%
keylogger	1.64%	id	2.11%
review	1.39%	giftcard	1.47%
keys	1.12%	ddos	1.32%
giftcard	1.07%	server	1.24%

C. Price

In our dataset, 48.72% of the selling posts in the Surface Web forums and 52.44% of the posts in the Dark Web mention pricing information. The rest of the posts require the interesting parties to contact the vendor by private message. In some cases, there is an escrow or contract system available by the forum administrator to manage transactions. Posts with pricing information show the value of the product usually in USD dollars and payment method. Less than 1% of the posts do not include the payment method. On the contrary, buying posts never includes pricing information.

Overall, prices are higher in Surface Web forums than in the Dark Web (see Table VI). Since our prices distributions are not normal, we performed a non-parametric Mann-Whitney-U test [32] to determine statistically significant differences between price products. For instance, PayPal accounts costs more in the Surface Web compared to the Dark Web ($Mann-Whitney-U = 5314$, $z = 11.86$, p<.001). On average, a PayPal account with a $4,500 balance cost approximately $220 in the Dark Web, whereas the Surface Web costs $260. Similarly, the average price for a single email account ($0.70 vs .$0.50) is higher in the Surface Web than in the Dark Web ($Mann-Whitney-U = 6804$, $z = 5.86$, p ¡ 0.01). User databases price is also higher ($15 vs. $12) in the Surface Web compared to the Dark Web ($Mann-Whitney-U = 4276$, $z = 8.15$, p<.001).

Malware is generally cheaper in Dark Web forums compared to the Surface Web. For example, crypters and RATs are among the cheapest items that can be found on the Dark Web costing $1 each at the lowest. The average price for crypters is higher ($27 vs. $3) in the Surface Web compared to the Dark Web (Mann-Whitney-U=2042, z=10.53, p<.001). The same happens for RATs ($Mann-Whitney-U = 1974$, $z = 6.34$, p<.001), costing $39 and $5 in the Surface Web and the Dark Web respectively. As we observed in several posts, malware tools offered in the Surface Web are proprietary software developed by, according to the authors, companies providing support and updates. On the other hand, malware in the Dark Web is sold by individuals that sometimes includes also the source code in the deal. Then, the average price for DDoS services is higher in the Surface Web compared to the Dark Web. These services can be hired daily, weekly or monthly with an average price of $202 in the Surface Web and $175 in the Dark Web per day.

Some exceptions are prices for fullz and Web hosting. Fullz are significantly higher in the Dark Web than in the Surface Web ($Mann-Whitney-U = 3211$, $z = 13.02$, p<.001) with an average cost of $23 in the Dark Web and $17 in the Surface Web. According to the sellers, these are high-quality fresh fullz; therefore more expensive. Similarly, Web hosting is on average more expensive in the Dark Web compare to the Surface Web ($5 vs. $12 per month), although the difference is not significant. Probably the reason for a higher price in the Dark Web is that this is a specialised bulletproof Web hosting aimed to host botnets, malware, spam and phishing sites, etc.

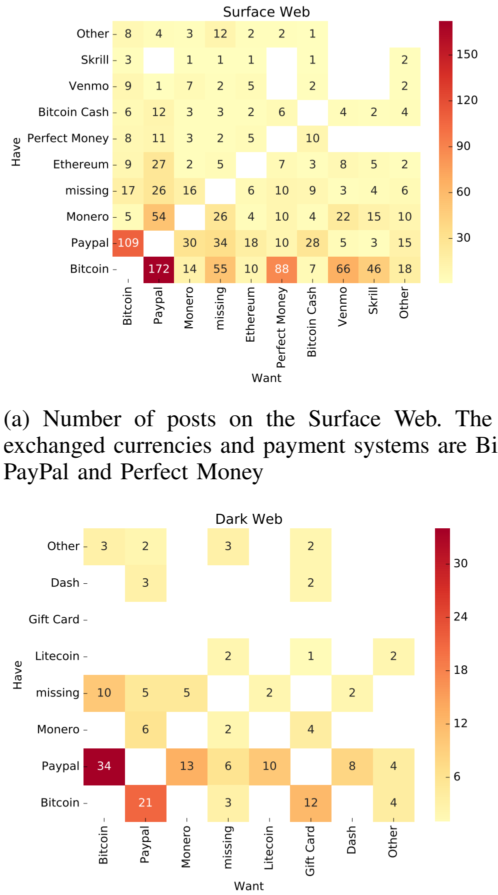
In terms of payment methods, in Surface Web forums, the most used payment methods are Bitcoin, PayPal, Monero, Ehtereum and Perfect Money. As regards the Dark Web, Bitcoin, Monero, Litecoin, Bitcoin Cash and Dash. This suggests that the underground economy in the Dark Web is based on cryptocurrency more than in the Surface Web.

D. Currency Exchange

Figure 1 shows the number of posts related to currency exchange in both Web environments. Rows represent the currency or payment system offered and the columns the one sought. Each cell reports on the number of posts for each offered/desired combination. We identified 23 payment mechanisms in the Surface Web and 14 in the Dark Web.

TABLE VI: Prices for products. Overall, prices are higher in Surface Web forums than in the Dark Web.

Product	**Surface**	**Dark**
PayPal accounts ($45,000 balance)	$260	$220
Bank accounts	$48	$22
Email accounts	$0.70	$0.50
Social media accounts	$90	$62
Social media followers	$7	$9
Netflix accounts	$3	$1
User databases	$15	$12
Fullz	$17	$23
DDoS (per day)	$202	$175
RDP Servers	$23	$17
Crypter	$27	$3
Remote Access Trojan (RAT)	$39	$5
Web hosting (per month)	$5	$12
Fake passport	$1850	$2100
ATM skimmers	$800	$800



(a) Number of posts on the Surface Web. The most exchanged currencies and payment systems are Bitcoin, PayPal and Perfect Money

(b) Number of posts in the Dark Web. PayPal, Bitcoin and Monero are the most popular currencies on exchange.

Fig. 1: Number of currency exchange posts for each pair of currency or payment system (offered and desired) in each web environment. *missing* stands for transactions where that side of the transaction was not mentioned or not extracted. ”Other” is the sum of other currencies or payment methods with less than 2 transactions combined to save space.

We extracted 1,193 exchange posts from the Surface Web (see Table 1a). In this environment, the most exchanged currencies and payment systems are Bitcoin, PayPal and Perfect Money. The most common operation is offering cryptocurrency in exchange for money in a payment system where exchangers profit by charging a fee for the transaction. Moreover, we believe that some criminals seek to cashout illegally obtained cryptocurrency for money in a payment system. In general, the most popular exchange is Bitcoin for PayPal. Our experiments confirm previous findings from Portnoff et al. [26] about this pattern.

Regarding Dark Web forums, we extracted 171 posts related to currency exchange as shown in Table 1b. PayPal, Bitcoin and Monero are the most popular currencies on exchange. Contrary to the Surface Web, the most common operation is offering money in a payment system in exchange for cryptocurrency. We presume the reason for the demand is that miscreants seek to obtain cryptocurrencies anonymously, which otherwise must be obtained from official exchanges who request personal data; therefore, they can perform their illegal activities unidentified. Another reason might be cybercriminals selling money from stolen payment systems in exchange for cryptocurrency as a kind of money laundering mechanism. Generally, the most popular exchange is PayPal for Bitcoin.

V. Discussion

Our results show that there is a higher level of trading activity in underground forums within the Dark Web compared to the Surface Web. While posts related to selling goods and services are higher in the Dark Web, requesting products to buy, and currency exchange posts are higher in the Surface Web. Most of the products for sale in the Surface Web are related to stolen data, whereas the Dark Web is focused on malware assets. Similarly, items related to stolen data are the most requested for buying on the Surface Web. On the other hand, the most requested products on the Dark Web are hacking services. In terms of prices, these are higher in Surface Web forums than in the Dark Web. Moreover, currency exchange posts in the Surface Web deal with a great variety of currencies including government-issued currency and cryptocurrency. Conversely, cryptocurrency is the main mean of exchange in the Dark Web.

Overall, there is more activity in terms of threads and users in the Surface Web (commercial and non-commercial). Normally, Surface Web forums have a longer lifespan; therefore, there are more users creating threads over time. In contrast, forums in the Dark Web are online for shorter periods of time because they are continually shut down by law enforcement agencies or taking over by competitors [33]. Furthermore, Surface Web forums are more accessible for any user regardless of their technical skills, whereas visiting forums in the Dark Web requires some knowledge and specialised software to access anonymity networks and a level of skill to search these hidden services. Thus, we believe there is a higher concentration of skilled users in Dark Web forums. Selling posts are more prevalent in the Dark Web, this suggests that Dark Web forums are specialised marketplaces where skilled users are offering products to a knowledgeable audience that already knows that the products they need are available and do not need to request them. Although posts related to buying products are higher on the Surface Web, we found a demand for hacking services in both environments. The main difference is that requests in the Dark Web are more sophisticated with users dealing with specific types of tools, methods and techniques used to perform cyberattacks. In terms of currency exchange, since financial activity on the Dark web is conducted via the tools of cryptocurrencies (especially Bitcoin) to maintain anonymity, there is more activity in the Surface Web as users deal with a variety of currencies and payment systems.

Our comparison shows that there is a higher level of sophistication among Dark Web users and the activities they perform in these underground forums. While users in Surface Web forums are more likely to search, request and buy readily available products such as stolen accounts or databases for monetisation purposes, Dark Web users seek to monetise their skills offering products or services for specific goals or targets. Therefore, the underground economy is increasingly growing facilitated by underground forums which are key drivers in the adoption of technologies with great potential such as encrypted messaging and cryptocurrency that challenge our notions of privacy and money. Moreover, although the COVID-19 has negatively affected economies worldwide, it seems to have opened up new opportunities for online black markets.

We believe the results of our work are key to improve threat intelligence strategies regarding underground forums; therefore law enforcement agencies, security practitioners and the research community can make better decisions about how to develop procedures and policies to prevent, stop or deter illegal activities conducted in underground forums depending on the layer of the Web where shady commercial activity is conducted. Threat intelligence analysis is important because it provides information about the techniques, tools and assets of adversaries. By improving this analysis, researchers will be able to detect threats more efficiently. For instance, trading activities related to malware, large data leaks, or zero-day exploits may be detected promptly; thus minimising the damage caused to the individuals or companies involved.

Our work clearly has some limitations. First, some forums, especially on the Dark Web, require to pay a membership or an invitation to access premium areas; therefore our data may not represent all the content posted in those forums. One forum in the Surface Web and two in the Dark Web had areas with restricted access. Second, since our crawling was performed from a user's perspective, we did not include private messages that might provide information about finished or closed transactions in the forums. Third, the data collection period is not enough to analyse trends and changes in trading activity, for example, those related to the COVID-19 pandemic that may have change patterns in the underground economy. Lastly, some trading posts could be aimed to scam users. As a result, because of all these limitations, our analysis might not present a complete picture of the trading activity in the forums. However, since we collected a great deal of data, we were able to perform a thoughtful analysis.

As part of future work, we plan to include more forums in each Web environment and collect data for a longer period of time to obtain more representative results. Our work focuses on trading posts such as types, products and prices. Similarly, other studies have examined only social networks interactions including user behaviour and private interactions. Therefore, future research should consider the analysis of all the variables of the forum ecosystem to understand the role of underground forums in the evolution of cybercrime. Researchers should also analyse scam threads to identify patterns and proportions of real trading in underground forums. These findings would be useful to improve threat intelligence activities aimed to counter illegal activities in these underground communities.

VI. Conclusion

As underground forums become increasingly central to exchange information about malicious activities on the Internet, including perform illegal commercial activities, and since more cybercriminals are migrating to the Dark Web to hide their operations, it is important to understand how illicit goods and services are exchanged in different layers of the Web. In this paper, we collected data related to trading activities from forums in the Surface Web and the Dark Web covering a period of 12 months. Our findings suggest that the Dark Web has a higher degree of trading activity compared to the Surface Web. Most of this activity is related to products offered for sale and shows a higher level of sophistication. This work is an initial step in a larger research agenda to understand the modus operandi of cybercriminals in different portions of the Web.

References

[1] McAfee, "Chinese cybercriminals develop lucrative hacking services." https://www.mcafee.com/blogs/other-blogs/mcafee-labs/chinese-cybercriminals-develop-lucrative-hacking-services/, Dec 2017.

[2] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna, "The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns," in *4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 11)*, (Boston, MA), USENIX Association, Mar. 2011.

[3] A. Haslebacher, J. Onaolapo, and G. Stringhini, "All your cards are belong to us: Understanding online carding forums," in *2017 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 41–51, 2017.

[4] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker, "An analysis of underground forums," in *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, IMC '11, (New York, NY, USA), p. 71–80, Association for Computing Machinery, 2011.

[5] S. Samtani, R. Chinn, and H. Chen, "Exploring hacker assets in underground forums," in *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 31–36, 2015.

[6] R. Overdorf, C. Troncoso, R. Greenstadt, and D. McCoy, "Under the underground: Predicting private interactions in underground forums," 2018.

[7] D. A. Bermudez Villalva, J. Onaolapo, G. Stringhini, and M. Musolesi, "Under and over the surface: a comparison of the use of leaked account credentials in the dark and surface web," *Crime Science*, vol. 7, p. 17, Nov 2018.

[8] D. S. Dolliver and J. L. Kenney, "Characteristics of drug vendors on the tor network: A cryptomarket comparison," *Victims & Offenders*, vol. 11, no. 4, pp. 600–620, 2016.

[9] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected Areas in Communications*, vol. 16, pp. 482–494, May 1998.

[10] D. Lacey and P. M. Salmon, "It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums," in *Proceedings of the 12th International Conference on Engineering Psychology and Cognitive Ergonomics - Volume 9174*, (Berlin, Heidelberg), p. 117–128, Springer-Verlag, 2015.

[11] D. S. Dolliver, "Evaluating drug trafficking on the tor network: Silk road 2, the sequel," *International Journal of Drug Policy*, vol. 26, pp. 1113–1123, Nov 2015.

[12] I. Pete, J. Hughes, Y. T. Chua, and M. Bada, "A social network analysis and comparison of six dark web forums," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 484–493, 2020.

[13] E. Nunes, P. Shakarian, and G. I. Simari, "At-risk system identification via analysis of discussions on the darkweb," in *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12, 2018.

[14] A. Bermudez-Villalva, M. Musolesi, and G. Stringhini, "A measurement study on the advertisements displayed to web users coming from the regular web and from tor," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 494–499, 2020.

[15] M. Zamani, F. Rabbani, A. Horicsányi, A. Zafeiris, and T. Vicsek, "Differences in structure and dynamics of networks retrieved from dark and public web forums," *Physica A: Statistical Mechanics and its Applications*, vol. 525, pp. 326–336, 2019.

[16] T. Holt and A. Bossler, *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge, 2015.

[17] R. L. Akers, *Social learning and social structure : a general theory of crime and deviance*. Northeastern University Press Boston, 1998.

[18] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *International symposium on research in attacks, intrusions, and defenses*, pp. 207–227, Springer, 2018.

[19] A. Hutchings and T. J. Holt, "The online stolen data market: disruption and intervention approaches," *Global Crime*, vol. 18, no. 1, pp. 11–30, 2017.

[20] S. Afroz, V. Garg, D. McCoy, and R. Greenstadt, "Honor among thieves: A common's analysis of cybercrime economies," in *2013 APWG eCrime Researchers Summit*, pp. 1–11, 2013.

[21] M. Yip, N. Shadbolt, T. Tiropanis, and C. Webber, "The digital underground economy: a social network approach to understanding cybercrime," in *Digital Futures 2012: The Third Annual Digital Economy All Hands Conference (22/10/12 - 24/10/12)*, October 2012.

[22] J. McAlaney, S. Hambidge, E. Kimpton, and H. Thackray, "Knowledge is power: An analysis of discussions on hacking forums," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pp. 477–483, 2020.

[23] A. Caines, S. Pastrana, A. Hutchings, and P. J. Buttery, "Automatically identifying the function and intent of posts in underground forums," *Crime Science*, vol. 7, p. 19, Nov 2018.

[24] Z. Sun, C. E. Rubio-Medrano, Z. Zhao, T. Bao, A. Doupé, and G.-J. Ahn, "Understanding and predicting private interactions in underground forums," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, CODASPY '19, (New York, NY, USA), p. 303–314, Association for Computing Machinery, 2019.

[25] Y. Fang, Y. Guo, C. Huang, and L. Liu, "Analyzing and identifying data breaches in underground forums," *IEEE Access*, vol. 7, pp. 48770–48777, 2019.

[26] R. S. Portnoff, S. Afroz, G. Durrett, J. K. Kummerfeld, T. Berg-Kirkpatrick, D. McCoy, K. Levchenko, and V. Paxson, "Tools for automated analysis of cybercriminal markets," in *Proceedings of the 26th International Conference on World Wide Web*, WWW '17, (Republic and Canton of Geneva, CHE), p. 657–666, International World Wide Web Conferences Steering Committee, 2017.

[27] E. Marin, A. Diab, and P. Shakarian, "Product offerings in malicious hacker markets," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, pp. 187–189, Sept 2016.

[28] G. Weimann, "Terrorist migration to the dark web," *Perspectives on Terrorism*, vol. 10, no. 3, pp. 40–44, 2016.

[29] R. A. HARDY and J. R. NORGAARD, "Reputation in the internet black market: an empirical and theoretical analysis of the deep web," *Journal of Institutional Economics*, vol. 12, no. 3, p. 515–539, 2016.

[30] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "Crimebb: Enabling cybercrime research on underground forums at scale," in *Proceedings of the 2018 World Wide Web Conference*, WWW '18, (Republic and Canton of Geneva, CHE), p. 1845–1854, International World Wide Web Conferences Steering Committee, 2018.

[31] P. L. MacDonald and R. C. Gardner, "Type i error rate comparisons of post hoc procedures for i j chi-square tables," *Educational and Psychological Measurement*, vol. 60, no. 5, pp. 735–754, 2000.

[32] H. B. Mann and D. R. Whitney, "On a test of whether one of two random variables is stochastically larger than the other," *The Annals of Mathematical Statistics*, vol. 18, no. 1, pp. 50–60, 1947.

[33] V. Bhaskar, R. Linacre, and S. Machin, "Dark web: The economics of online drugs markets," *LSE Business Review Blog*, 2017.