EXPLORING THE ILLEGAL MARKET BENEATH GOOGLE REACH- THE UNDERGROUND MARKET ON DARK WEB

Author: **Shubam Sharma* & Dr. Sheetal Arora****

* Independent Researcher, Delhi, India

** Assistant Professor, Sardar Patel University of Police, Security & Criminal Justice, Jodhpur, India

ABSTRACT

Statistics indicate that in cases of credit and debit card fraud in India, from April 2009 till September 2019, fraudsters have siphoned off Rs. 615.39 crores. In the last three months of 2019, Rs 129 crores got stolen, it can be more as India has not kept the record in cases of cybercrime amounting to less than 1 lakh. In the United Kingdom, statistics reveal that such cases registered totaled £671.4 million in 2018, and the fraud in 2019 under the Un-authorized financial crimes is £824.8 million indicating a need for deeper insight into the data collection process followed in India. Such high value of fraud signals that the underground market that primarily deals with such financial fraud products is on the rise. Literature relating to such research area had focused mainly on the organization and structure of the Dark web forums. The majority of studies on the dark web & market are on literature review, expert interviews, or data from forums/markets that eventually close. This paper provides an insight into active marketplaces with active trading of illicit products. The research utilized a mixed-method approach. The findings present data analysis for Dark Web market growth and the presence of working reputation systems based on first-hand data followed by the researcher's conclusion.

***Keywords*:** Carded Product**,** Dark Web**,** Underground Market/ Dark Web market**,** Escrow payment**,** Cyber Crime

INTRODUCTION

Financial frauds

The term "financial fraud" is not explained in the guidelines on fraud by Reserve Bank of India (RBI) but report of RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds defines "Fraud" with respect to digital banking or cyber fraud as -

> *'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.*[i]

Financial Frauds in Cyber Space

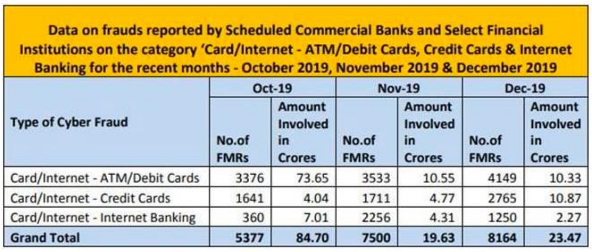
In order to detect, interdict & prevention many institution tried to make a distinction between financial fraud and financial crime although these distinction have got faded with the rise of Cyber space accompanied by Cyber threats. The financial fraud and crime cannot be differentiated based on the law or regulatory view instead it could be viewed as the outcome of organization silos.

The financial crime generally involve practices such as money laundering and criminal transgressions which include tax invasion along with bribery, etc. through the use of financial services to support the criminal enterprises. Whereas the Financial Fraud host crimes such as forgery, credit & card scam, involving deception of financial personnel or services to commit the theft.[ii]

Cyber Frauds in India

The RBI revealed in response to an application under Right to Information (R.T.I), that fraudsters siphoned off Rs 615.39 crore in more than 1.17 lakh registered cases of credit and debit card frauds over a period of 10 years from April 2009 to September 2019. The reply also suggests that, the actual amount would be more, as the bank does not maintain any record of cyber crimes where the amount is less than 1 lakh in the period from April 2009 till April 2017.[iii]

Mr. Anurag Thakur (MoS, Ministry of Finance) while replying to a question in Lok Sabha told that 21,041 cases of debit cards, credit cards, and internet banking amounting Rs 129 crore were registered in last 3 months of 2019. Table 1 presents the amount involved in the frauds reported in the last 3 months of 2019. Out of total Rs 129 crore losses, the loss of Rs 85 crore was just in a single month of October 2019. The table also shows, maximum cases were related to ATM or debit card transactions. The RBI data for frauds that are recorded under the 'Cyber Frauds' are not available, according to Mr. Anurag Thakur due to which all the data concerned with cyber frauds are written under category 'Card/Internet - Debit Cards, Credit Cards & Internet Banking'. So without any proper category with precise information related to cyber frauds, even after the growing network of digital payment and its related interface posses hinder in the smooth functioning of the same.[iv]



Data on frauds reported by Scheduled Commercial Banks and Select Financial Institutions on the category 'Card/Internet - ATM/Debit Cards, Credit Cards & Internet Banking for the recent months - October 2019, November 2019 & December 2019

Type of Cyber Fraud	Oct-19		Nov-19		Dec-19	
	No.of FMRs	Amount Involved in Crores	No.of FMRs	Amount Involved in Crores	No.of FMRs	Amount Involved in Crores
Card/Internet - ATM/Debit Cards	3376	73.65	3533	10.55	4149	10.33
Card/Internet - Credit Cards	1641	4.04	1711	4.77	2765	10.87
Card/Internet - Internet Banking	360	7.01	2256	4.31	1250	2.27
Grand Total	**5377**	**84.70**	**7500**	**19.63**	**8164**	**23.47**

Table 1: Data fraud reported by commercial banks and select financial institute in last 3 months of 2019 (Oct, Nov, Dec)[v]

Financial Fraud in UK

- **UK scenario for the fraud 2018**

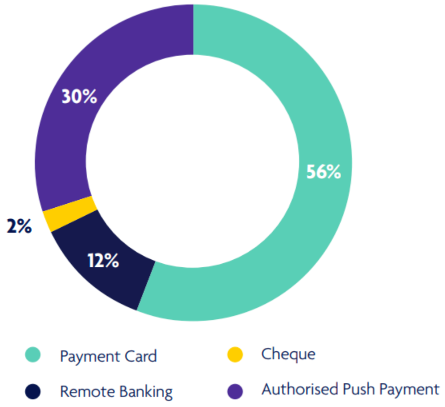
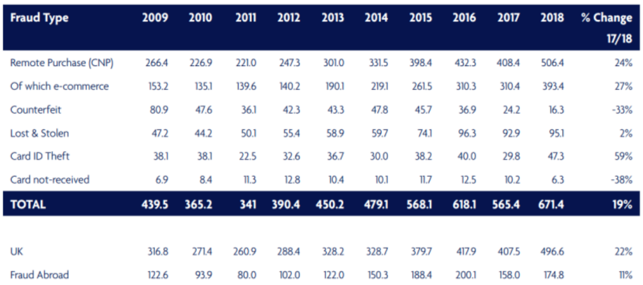


Figure 1: Total financial fraud losses (UK) by type in 2018[vi]

The total registered fraud amount for card been registered in UK totaled £671.4 million in 2018, where 19% increase was recorded from 2017 from £565.4. But in 2018 the spending reached £800 billion including debit and credit cards together with 20.4 billion transaction.



Fraud Type	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	% Change 17/18
Remote Purchase (CNP)	266.4	226.9	221.0	247.3	301.0	331.5	398.4	432.3	408.4	506.4	24%
Of which e-commerce	153.2	135.1	139.6	140.2	190.1	219.1	261.5	310.3	310.4	393.4	27%
Counterfeit	80.9	47.6	36.1	42.3	43.3	47.8	45.7	36.9	24.2	16.3	-33%
Lost & Stolen	47.2	44.2	50.1	55.4	58.9	59.7	74.1	96.3	92.9	95.1	2%
Card ID Theft	38.1	38.1	22.5	32.6	36.7	30.0	38.2	40.0	29.8	47.3	59%
Card not-received	6.9	8.4	11.3	12.8	10.4	10.1	11.7	12.5	10.2	6.3	-38%
TOTAL	**439.5**	**365.2**	**341**	**390.4**	**450.2**	**479.1**	**568.1**	**618.1**	**565.4**	**671.4**	**19%**
UK	316.8	271.4	260.9	288.4	328.2	328.7	379.7	417.9	407.5	496.6	22%
Fraud Abroad	122.6	93.9	80.0	102.0	122.0	150.3	188.4	200.1	158.0	174.8	11%

Table 2: Fraud volume and fraud type data for UK from year 2009 to 2018 [vii]

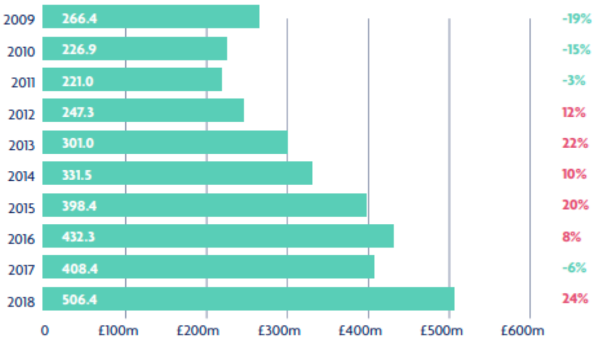


Figure 2: Remote purchase fraud losses on UK issued cards 2009-2018[viii]

The Overall remote purchase fraud see the growth of 24% in 2018 when compared with 2017 with total online remote purchase fraud at £506.4 million in 2018. Out of this the Online fraud against UK retailers itself have a share of £265.1 million in 2018 and it has raised by 29% to 2017. The Mail and telephone order (MOTO) fraud that has been registered against retailers present in the UK also showed increase of 24% with respect to 2017 with reported value of £92.1 million. But substantial number of cases were been registered and showed the increase of 47% in 2018 out of which 24% shows loss rose, suggesting that the card issuer proactively stopped the individual incident after they were being identified by the card issuer.

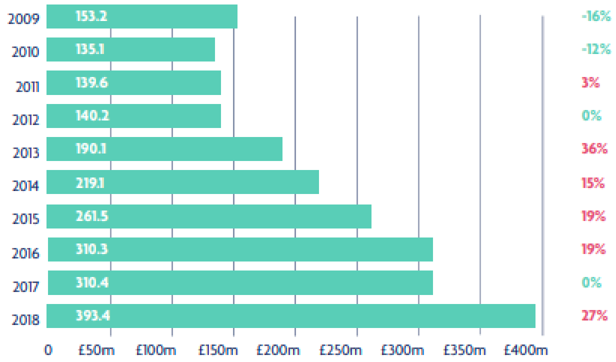


Figure 3: E-commerce/internet fraud losses on UK issued cards 2009-2018[ix]

In the e-commerce category the fraud that took place through cards accounted for 59% of all card fraud and the 78% of all the remote purchase fraud being reported in the UK which have the value of £393.4 million. (Fraud The Facts 2019, 2020)[x]

- **UK scenario for the fraud 2019**

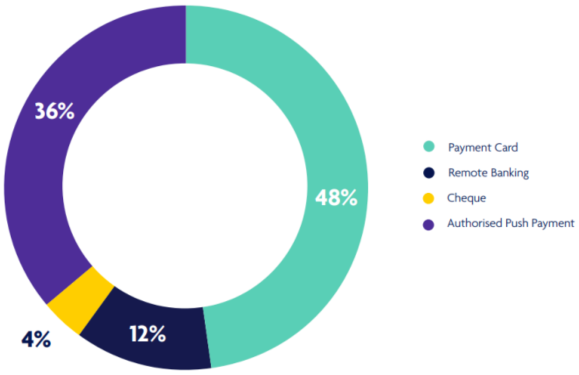


Figure 4: Financial fraud losses (UK) by type in 2019[xi]

The Unauthorized financial fraud recorded in the UK for 2019 is £824.8 million for all the possible categories involving payment cards, cheque and remote banking which shows the 2% decrease when compared to 2018.

The total fraud of £620.6 million is recorded for cards registered in the UK in 2019 with eight percent decrease when compared to 2018 but total the total number of transaction being made in the 2019 was recorded as 22 billion.

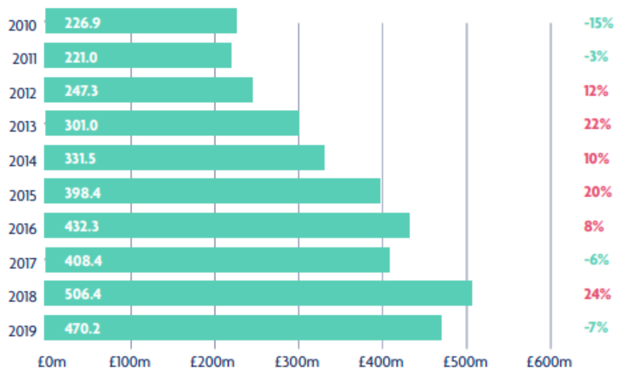


Figure 5: Remote purchase fraud losses on UK issued cards 2010-2019[xii]

- **Remote purchase fraud (involving internet, telephone, mail order but plastic cards were not used):** Overall remote purchase fraud saw the drop of 7% when compared to 2018 and total value dropped to £470.2 million. The Online fraud against UK retailers also saw the decrease of 10% to 2018 and the total of £239.9 million fraud was recorded in this category. The decreasing trend is also seen in the Mail and telephone order (MOTO) fraud against retail present in the UK where it shows the decrease of 5% and the estimated value of trade was £87.3 million.

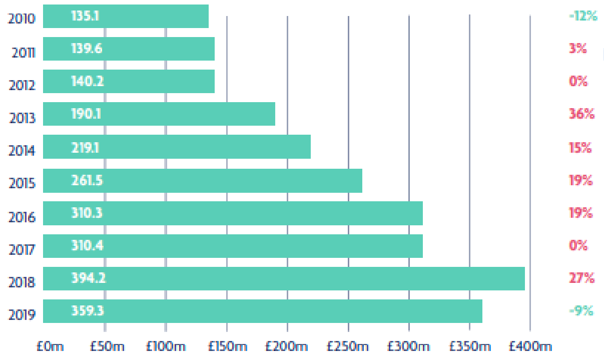


Figure 6: E-commerce/internet fraud losses on UK issued cards 2010-2019[xiii]

- **Internet/e-commerce fraud:** The Internet fraud itself is responsible for 76% of remote purchase fraud and fifty eight percent of card fraud. This category have fraud of £359.3 million e-commerce fraud in 2019. (Fraud-The Fact 2020, 2020)[xiv]

Incidences of Cyber Frauds around the world

According to Cyble research, over 1 million cards are made public for free by AllWorld.Cards store in order to promote their cyber crime Marketplace claiming that the cards are of 2018-

2019 having 20 % active credit cards. The data leak affected almost around 136 countries & 500 banks all over the world including JP Morgan and Toronto-Dominion Bank (TD Bank). The All World Cards Marketplace is active on Dark web from May 2021 and to promote themself they had made the critical information of the user like credit card number, Expiry number, CVV, Name, country, etc. Public for free. [xv]

Security firm Gemini Advisory in August 2019 reported the data leak of more than 1 million U.S. and South Korean credit card information. Stas Alforov Director of reseach at Gemini Advisory told that the return on investment is higher on APAC (Asia Pacific) banks are more vulnerable than western sue to presence of less sophisticated anti-fraud system in place.[xvi]

Incidences of Cyber Frauds in India

Fraud particularly related to our banking sector including the digital payment interface is on rise these days. According to a report surfaced in 2019, nearly 1.3 million Indian bank cards and details related to it, has been put on sale on dark Web. Shockingly cyber security firm Group-IB reveals the 98 per cent cards put on sale were of Indian banks and only 1 per cent were of Colombian banks. Group-IB founder and CEO, Ilya Sachkov mentioned that, this was not promoted anywhere either in any forum or news, etc. on the dark Web. According to report credit and debit cards were made online on “Joker’s Stash” (oldest card shop on Dark Web) where each card was priced at $100. After the Group-IB analysis it was found that more than 18% of the cards database is related to a single Indian bank and the data included the magnetic strip data which implies that it was stolen using skimming method. Total expected earnings from this data Hack is around $130 million.[xvii]

Another data breach of 8.2 terabytes was confirmed by French security researcher Robert Baptiste in 2021. This data breach compromised the detail of 3.5 million user. The breach includes names, email addresses, location data, hashed password, partially masked credit card number, KYC documents photos & list of installed apps.[xviii]

In 2021 only another Independent researcher Rajshekhar Rajaharia reported the potential data theft that had compromised nearly 10 crore credit and debit card holders in the India due to compromised server of digital payment gateway of Justpay based out in Bengaluru. Juspay confirmed that the unauthorized access was attempted in August 2020 but according to Justpay it was not successful as it was terminated when it was in progress and thus no essential detail of customer was compromised as per the spokesperson of Justpay which also claimed the actual number is just fraction of claimed 10 crore.[xix]

Laws relating with Cyber Crimes in India

The term cyber crime is not defined in any legislation in India but the word cyber is used for anything related to IT or computer. Thus the crimes which has cyber as the medium to commit it is known as Cyber crime.

The law related to cyber crime can be found in IT Act 2000 that was made effective from 17 October 2000. The IT Act essentially deal with Legal Recognition of Electronic Documents, Digital Signatures, Offenses and Contraventions along with Justice Dispensation Systems for cyber crimes. Although the IPC Act also have certain parallel section that state the imprisonment and fine for the crimes related to cyber crime. The some of the important section of IT Act that are relevant to cyber crime are:

- The Section 43 and 66 of IT Act deal with Hacking and Data theft that penalize activities ranging from hacking, denying authorized person access to damaging or destroying information residing in digital system, etc. The maximum punishment for the above offenses is term for 3 years or fine of Rs 5,00,000 (Rupees five lac) or both.

- Section 66B of IT Act have punishment for dishonestly receiving any stolen computer resource or communication device. According to this section the term for 3 year or fine of upto Rs 1,00,000 (Rupees One Lac) or both.

- The Section 66C of IT Act deals with the punishment for identity theft and cheating by personating that is imprisonment up to 3 year and shall be liable for fine of up to Rs 1,00,000 (Rupees One Lac).

- The Section 66D of IT Act deal with the punishment for cheating by personating using computer resource that is imprisonment that may extent for the term of 3 years and fine that may extent upto Rs 1,00,000 (Rupees one lac).[xx]

Background and Context

In this study, data collection is done directly from the Dark Web Market, with focus on the market itself. Since Dark Web market facilitates, the fraud chain which start with the seller. So understanding the market itself plays crucial role in order to regulate and cease these Dark Web market by choking the essential element that would be required by these market in order to survive.

Existing literature focuses mainly forums/market that has already been shutdown. Furthermore, studies are usually based on literature review, expert interview, or data from forums/market that have already been shut down. For the purpose of this study, the researcher proposes two hypotheses. These are dealt using findings based on data collected through observations on active market places with an active trading of product. The researcher applied non-participator observation method to observe/ four Market places, and collects data information in the form of posts from the market over a period of March- May. The data collected is analyzed both qualitatively and quantitatively to prove/support the Hypothesis. In the latter part of this paper, findings and discussions are presented based on first-hand data collected empirically.

Research Hypothesis

H1: On the Dark Web market, a particular seller/ vendor in limited to particular market only.

H2: All Vendor for carded product show specialization, that is all the vendor sell only one product type.

H3: The Dark Web market have working reputation systems that are as sophisticated as those of legal marketplaces.

H4: The Dark Web markets are growing even after the strict policies of government internationally.

Rationale

This study helps in providing clarity whether the Dark Web market have working reputation systems or not and whether it is growing with time or not even after international agencies continuous watch.

Gaps in Existing Knowledge

As the global Dark Web market is more dynamic and relatively unstable in nature when compared to legal market. The international agencies have continuous watch on these illicit market and shutdown them regularly due to which all the studies done earlier for market are no longer functional or it has been taken down by agencies by FBI, NIA etc.

REVIEW OF LITERATURE

All Your Cards Are Belong To Us: Understanding Online Carding Forums:

This research paper focuses on underground online forums for which the researcher selected the forums. The researcher selected five out of 25 discovered forums, collected posts and analyzed the thread present on the forum for the lead for the seller profile in the forums over a three-month period, and analyzed them quantitatively and qualitatively. The paper concluded that the prices for the plastic cards, dumps and fullz were still in the price category as suggested by the previous literature. Dumps & Fullz were 3 times more expensive than CVV's but PayPal credentials were listed on some forums but the market of cards seem to more stable and concrete than PayPal. Western Union money transfer services play holds some share in some of the forums.

Specialization of the seller was one of the parameter that was tested in the research and the key characteristic for most of the seller was not limited for providing some specialized services only instead seller has wide number of product listing.[xxi]

Market for Cybercrime Tools and Stolen data: Hacker's Bazar

In 2014, Rand corporation published this research in which they analysed the hacking community and cyber black markets to see whether they are proliferating or not. Findings pointed out the markets as the ad hoc network of organised groups from all across the world and the common thing that unites them is traditional crimes like mafias, drug, smuggling, etc.

The cyber dark markets do not deviate much from a traditional market where the buyers commute to reach the criminal enterprises and finalize the order to get the order. If we see the evolution process for normal market like groceries, clothing, etc the ones established online. Then, we will observe that innovation and growth both played vital role in it. Similar evolutionary path is observed for the dark market in which dark mark can be more profitable than the illegal regular market trade.

The Cyber Black Markets is the large pool consisting of people from worldwide which are continuously resisting the Outside Forces who try to reset the growth of such market with moving the transaction to dark nets; more encryption techniques; providing anonymity to the people on the virtual world and restricted access to the dark net eliminate the possible and effective crackdown by the international agencies on such markets.

But as the player become highly customized with the listing and specialized and they tend to move behind the bigger target to have more profit they also attract the law enforcement agencies to counter them in the cyber space as more technological savvy person are being attracted to these market place to earn the luck. Hence pressure of these agencies has also increased many fold.

The cyber black market is still resisting the outside pressure and remains resilient showing the accelerated growth using the high end digital defense strategies making the enforcement agencies to keep up the pace with the growing dark market trend.[xxii]

Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web:

In another, report published in 2019 by Rand Corporation “Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web” which emphasizes that the information sharing and improvised training will play a critical role in these kind of investigation and apprehension of such cases.

The report suggest the need to have the investment in the training irrespective of the level which mean the training from initial rank officer to higher most rank officer should be well versed with the relevant artifact knowledge and the same should be incorporated during the training module.

The international agencies across all the international border should share the information irrespective of the border separating them because the criminals take the leverage of such communication gap between countries.

Investigating officer sometimes overlook the evidences that hold important value like the simple random number or words found in the notes may be identified as crypto wallet addresses, website link for dark web addresses, etc that may be used to correlate the different evidences or different cases all together. The anonymity and various encryption method employed in the dark web make in more difficult for the investigators to detect and investigate the crime. The research "Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web" also emphasized upon the following point in order to resolve the existing issues:

- New standard operating procedure adoption for the purpose of developing new standard for testing tools that can be employed to collect the electronic evidences that may have sophisticated software running in them to access the dark web.
- For inspecting the packages through the mail services via U.S. mail, etc. The researches should be employed to modernize the existing laws related to it.

Conducting research for the nature of crime that are linked together in order to make sure that the investigating agencies are able to focus on the iceberg tip (i.e., traditional crime) along with the less visible portion of the iceberg (i.e., digital/electronic nature of the crime).[xxiii]

RESEARCH METHODOLOGY

During the process of data collection, various approaches were undertaken in order to collect the names of Dark Web websites from various sources and after the discovery of various websites, only 4 websites that matched our selection criteria were selected for further examination. The data was collected and analyzed for the period of two months starting from March 2020.

Forum search

For this research, various steps were followed to find the names of the Dark Web website dealing with illicit products. Initially, the names from the existing literature were collected that claimed to have done research on Dark Web markets or forums. Second, we tried to carry out searches through a number of search engines like Google, Bing, etc but since all these search engines are capable to search only in the clear-net we were directed to more literature. So in the third step, we started the search, namely via the Tor network, and "The Hidden Wiki." But the majority of the market mentioned in the Hidden Wiki majorly belongs to a single vendor store, and since our study had the focus to study the market, not vendor alone so those market and the forums information was not included in the research. Finally, we searched forums threads that we already found for references for markets that could probably be dealing with the marketplaces on the darknet. In the last, the researcher adopted the method of snowball sampling. The selection criterion at that time was driven by a language barrier, due to which the researcher had to only choose the market or forums that were at least partly in English with .onion domain.

We have not included the market dealing with only one particular category of product or the website owned by any individual vendor in our analysis because chances of manipulation are extremely high, chances of fraudulent vendors increase manyfold as compared to a market with a pool of vendors.

To narrow down the field of vision of the research the researcher had only chosen to have the analysis of only four Dark Web markets: Dark bay, Dark Market, Torrez Market, and Versus Market.

The initial two markets chosen had a high number of the vendor along with the high listing of product and the other two have a small share of vendor and product listing because these are the new website on the dark-net in the initial proliferation stages.

The researcher had tried to choose the mix of markets on the basis of the approximate age of the dark web website.

Temporal sampling

In order to have a comparable result at the last during the analysis of the market the researcher had chosen the time frame of 2 months for all the 4 markets of interest, the researcher monitored the market on various parameters over the period of two months, starting from March to May 2020. This specifically means that the snapshot of the data that was both quantitative and qualitative in nature was collected at the beginning of march and the same process was repeated with the marketplace after the duration of 2 months in May. This two months limitation meant that the full activity of the market could not be recorded for a longer duration. However, this 2 months limitation for this research is still comparatively beneficial that the shorter duration that would not be able to have the data that could present the real scenario of the dark web.

Data collection

The process of data collection was performed for all the 4 Dark Web markets of interest. The collected information about markets includes the language, number of product listings, the total number of registered users, working reputation of the markets if any, and all other relevant information regarding the market was collected. All the analysis done under this research is based on the perspective of the user of such a website. So our data collection was also influenced by user perspective analysis only.

During the data collection process, the researcher included all potential products that would be placed in the carded product: watches, masks and other medical equipment (corona supplies), mobile, laptop, other electronics, shoes, gift cards. The researcher also tried to have a clear distinction between the carded product and other categories of goods like smuggled products (gold, platinum diamond, other metal like mercury, etc.) which were not included.

At first, the vendor name was written and the product that they offer was written in front of the vendor name. This process was repeated for all the vendors that provided any of the carded products. This was repeated for all 4 markets of interest to known the carded product listed on all 4 websites along with vendor name. So that we could see whether the vendor is limited to one market or not along with whether the vendor is specialized in providing any particular product or not. And with this data collection only we could easily interpret two Hypotheses that are H1 and H2.

For the Hypothesis, H3 various aspects of the market were considered and recorded for ascertaining whether they had the working reputation as sophisticated as a normal online market like Amazon, etc or not. So, for this, each market was analyzed for the various parameters like rating option for the vendor by the buyer, feedback for purchase of the particular product by the buyer, dispute resolution system, privacy protection, money protection, protected payment option, etc. All the four websites were analyzed by reviewing the market vendor policy, escrow payment and the mode of payment, FAQ of all 4 markets to arrive at the conclusion whether the market has the reputation system in place to protect the buyer or not.

The number of users that had profiles with the carding market, the total number of products listed along the total number of vendors were recorded on March and May 2020 with the time duration of 2 months for verifying the Hypothesis H4.

Analytical strategy

To keep the track of all the data of the Dark Web market combined approach was applied to make the data ready for the analytical approach. The data acquired from the 4 Dark Web markets is analyzed with a combined approach, both quantitatively and qualitatively.

The data was categorized using the qualitative method but for the purpose of comparison, the data for a market like the number of users, vendors, etc. followed a quantitative approach for the analysis purpose.

The next step was the data representation in the form of a table, bar graph, pie chart, and categorization of product. The categorization process undertaken did not have too much bifurcation in the product listing for the ease of research and understanding the category.

In order to test the H1, all the vendor list was prepared with the product they have on offer in the form of tabular data representation through which it could be determined whether the same vendor is present on a different website or not. For H2, the same tabular data could be used to know whether the vendor is specialized in only one product or not by looking at the product listing for a particular vendor for a particular market.

For Hypothesis H3, the analysis of the qualitative data was required which involves the characteristics of the Dark Web market like feedback mechanism of the vendor absence or presence, order dispute features, etc. for arriving at the conclusion of H3. Hypothesis H4 required the comparative analysis of the stats that had to present in the form of a bar graph for the number of users, the number of products, and a pie chart for the number of vendors on different websites to have data representation.

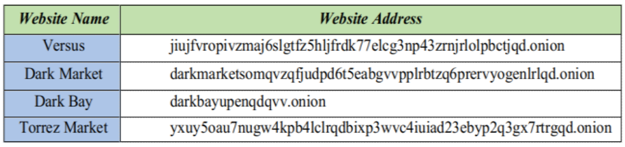
All the process mentioned above for H4 was carried for the 3 market only because for the fourth market data was not available and it was not feasible for the researcher to do the same due to the number of limitation.

ANALYSIS

Overview

For the purpose of this study, only 4 websites are being considered for analysis. The various attributes of the websites are name, language, founding date, total members, total posts, and accessibility of the website.

Name: The website discovered after the detailed study using the sophisticated software to dive into the dark web is listed in Table 3. The website analyzed has the onion domain only followed by content in English. The country of origin from where these websites operate cannot be determined and it is beyond the scope of the research.



Website Name	*Website Address*
Versus	jiujfvropivzmaj6slgtfz5hljfrdk77elcg3np43zrnjrlolpbctjqd.onion
Dark Market	darkmarketsomqvzqfjudpd6t5eabgvvpplrbtzq6prervyogenlrlqd.onion
Dark Bay	darkbayupenqdqvv.onion
Torrez Market	yxuy5oau7nugw4kpb4lclrqdbixp3wvc4iuiad23ebyp2q3gx7rtrgqd.onion

Table 3: Dark web website name and the URL of the website

Total Product Listed: The total number of the product listing on the market are depicted through the bar graph in Figures 7 & 8 showing the comparison recorded before and after the 2 months duration but the stats for Versus market could not be retrieved for the study purpose of this research.

Total User: The total number of users that had the account with the above mentioned Dark Web market is depicted through bar graph in Figure 7 & 8 showing the comparison of the total user before and after the duration of 2 months duration but the stats for Versus market could not be retrieved for the study purpose of this research.

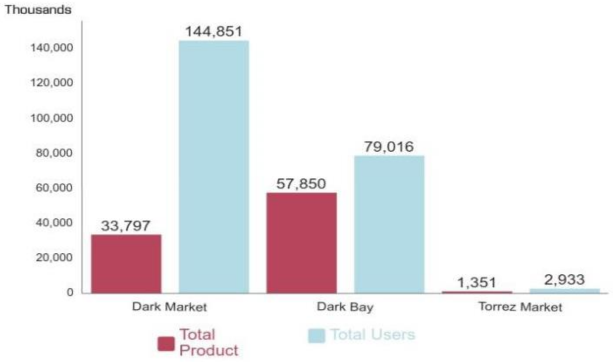


Figure 7: Total number of product and user as recorded on 9-10 March 2020

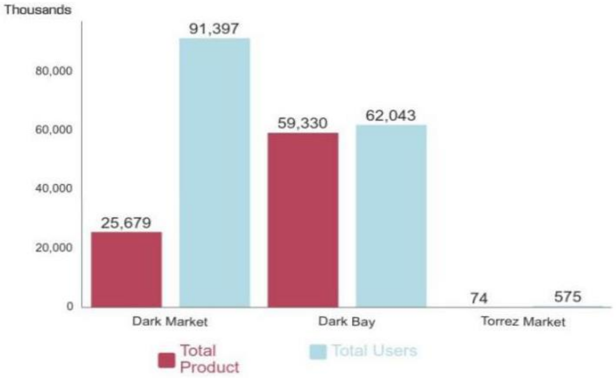


Figure 8: Total number of product and user as recorded on 10-11 May 2020

Total Vendors: The total number of Vendors that had their products on Dark Web market are depicted through a pie chart in Figures 9 & 10 showing the comparison of the total vendor on the 3 websites before and after the duration of 2 months duration. The stats for the versus market could not be retrieved for the study purpose of the research.

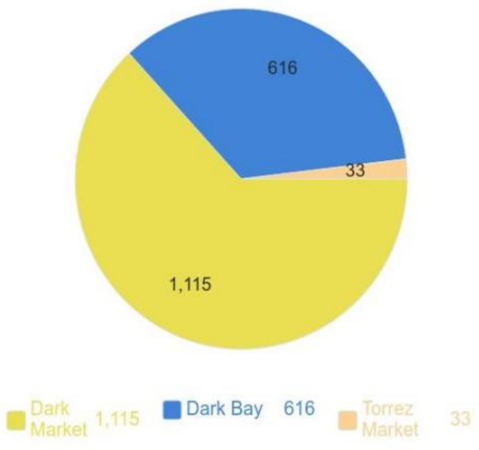


Figure 9: Vendor number recorded on 9 and 10 March 2020

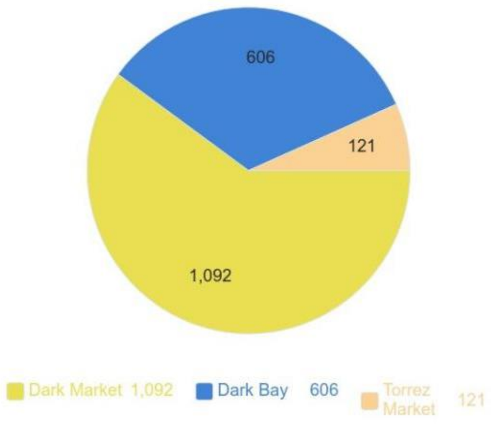


Figure 10: Total vendor number recorded on 10 and 11 May 2020

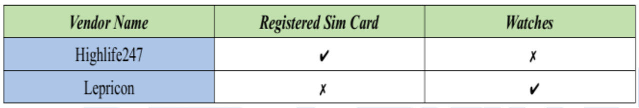
Founding date: The founding date of the market could not be determined with accuracy as the websites do not mention the founding date but according to the various sources and the information collected through the individual website/forums it can be said that the 3 websites that are Dark Bay, Dark Market, Versus are present on the dark web for more than the year but the Torrez Market has been launched in 2020 only. Nothing in the above can be confirmed with exact accuracy but the evidence gathered from forums discussion points toward the tentative founding date.

Language: During the Dark Web website search many non-English origin websites have been discovered on the Dark Web having languages like Russian, German, etc. but for the simplicity and ease of research only the website in English has been taken into consideration.

Detailed analysis

In this part of the research, we discuss the research hypotheses that are provided at the starting of the research for the 4 markets that are selected for this research.

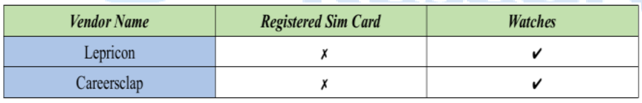
The list of vendors that is listed on the 4 markets is provided in the table from Table 4 to Table 10. Tables 4 and 5 are for Versus market and table 6 is for Torrez Market showing data collected on 10/March/2020. Table 7 and 8 are for the Dark market whereas the Table 9 and 10 are for Darkbay market.



Vendor Name	Registered Sim Card	Watches
Highlife247	✓	✗
Lepricon	✗	✓

Table 4: Vendor name along with their list of product listed on Versus market

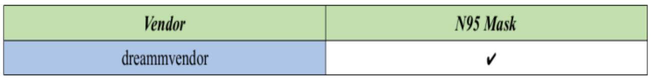
(Data collection date- 9/March/2020)



Vendor Name	Registered Sim Card	Watches
Lepricon	✗	✓
Careersclap	✗	✓

Table 5: Vendor name along with their list of product listed on Versus market

(Data collection date after 2 months -10/May/2020)

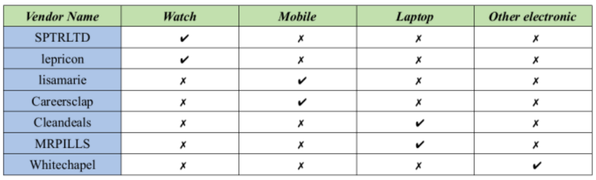


Vendor	N95 Mask
dreammvendor	✓

Table 6: Vendor name along with their list of product listed on Torrez Market

(Data collection date – 10/March/2020)

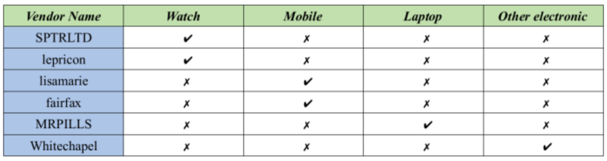
- After the 2 months period (Data collection date -11/May/2020) the researcher collected and analyzed the data for the Torrez Market but no product was listed under the carded product or after going through the Torrez Market researcher could not found any carded product. Hence after 2 month period on 11/May/2020, no carded product was available at the Torrez Market.



Vendor Name	Watch	Mobile	Laptop	Other electronic
SPTRLTD	✔	✗	✗	✗
lepricon	✔	✗	✗	✗
lisamarie	✗	✔	✗	✗
Careersclap	✗	✔	✗	✗
Cleandeals	✗	✗	✔	✗
MRPILLS	✗	✗	✔	✗
Whitechapel	✗	✗	✗	✔

Table 7: Vendor name along with their list of product listed on Dark market

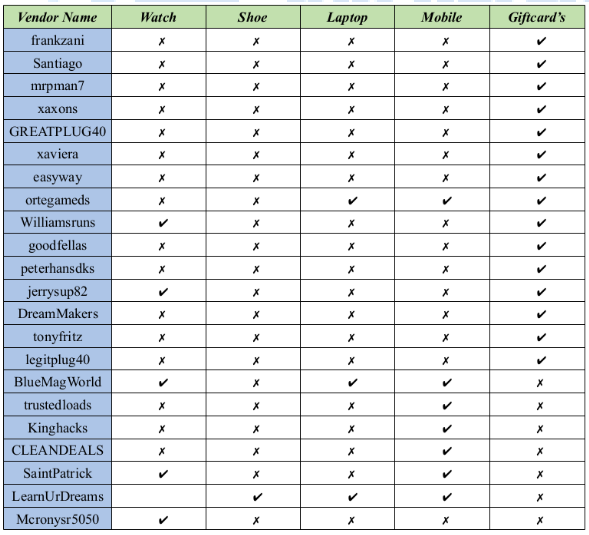
(Data collection date – 10/March/2020)



Vendor Name	Watch	Mobile	Laptop	Other electronic
SPTRLTD	✔	✗	✗	✗
lepricon	✔	✗	✗	✗
lisamarie	✗	✔	✗	✗
fairfax	✗	✔	✗	✗
MRPILLS	✗	✗	✔	✗
Whitechapel	✗	✗	✗	✔

Table 8: Vendor name along with their list of product listed on Dark market

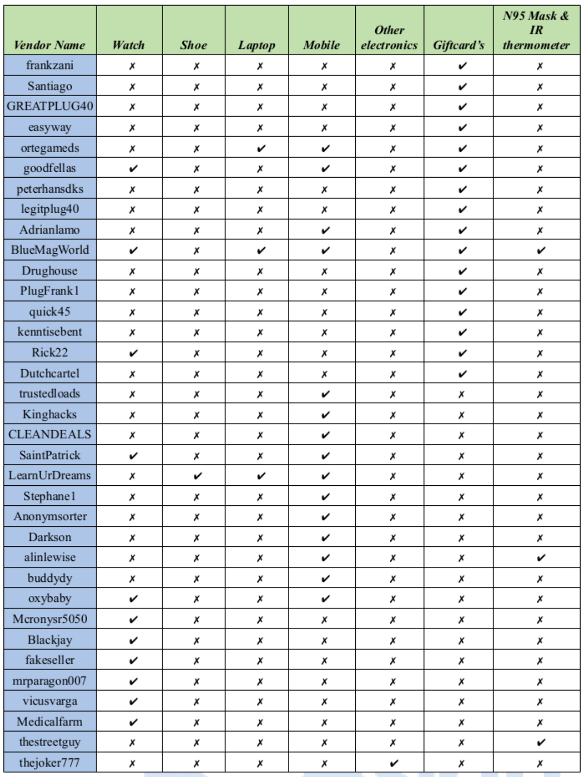
(Data collection date after 2 months - 10/May/2020)



Vendor Name	Watch	Shoe	Laptop	Mobile	Giftcard's
frankzani	✗	✗	✗	✗	✔
Santiago	✗	✗	✗	✗	✔
mrpman7	✗	✗	✗	✗	✔
xaxons	✗	✗	✗	✗	✔
GREATPLUG40	✗	✗	✗	✗	✔
xaviera	✗	✗	✗	✗	✔
easyway	✗	✗	✗	✗	✔
ortegameds	✗	✗	✔	✔	✔
Williamsruns	✔	✗	✗	✗	✔
goodfellas	✗	✗	✗	✗	✔
peterhansdks	✗	✗	✗	✗	✔
jerrysup82	✔	✗	✗	✗	✔
DreamMakers	✗	✗	✗	✗	✔
tonyfritz	✗	✗	✗	✗	✔
legitplug40	✗	✗	✗	✗	✔
BlueMagWorld	✔	✗	✔	✔	✗
trustedloads	✗	✗	✗	✔	✗
Kinghacks	✗	✗	✗	✔	✗
CLEANDEALS	✗	✗	✗	✔	✗
SaintPatrick	✔	✗	✗	✔	✗
LearnUrDreams		✔	✔	✔	✗
Mcronysr5050	✔	✗	✗	✗	✗

Table 9: Vendor name along with their list of product listed on Dark Bay

(Data collection date - 10/March/2020)



Vendor Name	*Watch*	*Shoe*	*Laptop*	*Mobile*	*Other electronics*	*Giftcard's*	*N95 Mask & IR thermometer*
frankzani	✗	✗	✗	✗	✗	✔	✗
Santiago	✗	✗	✗	✗	✗	✔	✗
GREATPLUG40	✗	✗	✗	✗	✗	✔	✗
easyway	✗	✗	✗	✗	✗	✔	✗
ortegameds	✗	✗	✔	✔	✗	✔	✗
goodfellas	✔	✗	✗	✔	✗	✔	✗
peterhansdks	✗	✗	✗	✗	✗	✔	✗
legitplug40	✗	✗	✗	✗	✗	✔	✗
Adrianlamo	✗	✗	✗	✔	✗	✔	✗
BlueMagWorld	✔	✗	✔	✔	✗	✔	✔
Drughouse	✗	✗	✗	✗	✗	✔	✗
PlugFrank1	✗	✗	✗	✗	✗	✔	✗
quick45	✗	✗	✗	✗	✗	✔	✗
kenntisebent	✗	✗	✗	✗	✗	✔	✗
Rick22	✔	✗	✗	✗	✗	✔	✗
Dutchcartel	✗	✗	✗	✗	✗	✔	✗
trustedloads	✗	✗	✗	✔	✗	✗	✗
Kinghacks	✗	✗	✗	✔	✗	✗	✗
CLEANDEALS	✗	✗	✗	✔	✗	✗	✗
SaintPatrick	✔	✗	✗	✔	✗	✗	✗
LearnUrDreams	✗	✔	✔	✔	✗	✗	✗
Stephane1	✗	✗	✗	✔	✗	✗	✗
Anonymsorter	✗	✗	✗	✔	✗	✗	✗
Darkson	✗	✗	✗	✔	✗	✗	✗
alinlewise	✗	✗	✗	✔	✗	✗	✔
buddydy	✗	✗	✗	✔	✗	✗	✗
oxybaby	✔	✗	✗	✔	✗	✗	✗
Mcronysr5050	✔	✗	✗	✗	✗	✗	✗
Blackjay	✔	✗	✗	✗	✗	✗	✗
fakeseller	✔	✗	✗	✗	✗	✗	✗
mrparagon007	✔	✗	✗	✗	✗	✗	✗
vicusvarga	✔	✗	✗	✗	✗	✗	✗
Medicalfarm	✔	✗	✗	✗	✗	✗	✗
thestreetguy	✗	✗	✗	✗	✗	✗	✔
thejoker777	✗	✗	✗	✗	✔	✗	✗

Table 10: Vendor name along with their list of product listed on Dark Bay

(Data collection date after 2 months - 11/May/2020)

After having the list of all the vendors that are listed on dark web websites along with the product they offer from Table 4 to 10 we can arrive at the conclusion of the Hypothesis that we made at the starting of the research.

- **Presence of vendor on multiple website.**

The vendor keeps their profile name in such a way that the name does not disclose the identity of the vendor or the origin of the vendor in order to stay anonymous.

The reason the vendors have the same name on the different websites is to make trust in the buyer community and make the buyer base and even the market praises the vendor to carry the same name by giving rebate in the subscription fee to the vendor when he forms the vendor account with the dark web market places if they are the trusted seller on another market already.

The vendors in the category of carded products are not limited to just one market instead they may be listed on multiple markets at the same time. The vendor name that is listed on multiple websites are “Lepricon” and “Careersclap” which is listed on Dark Market and Versus. The vendor “cleandeals” is listed on the two markets that are Dark Market and Dark Bay. So with this, we can say that Hypothesis 1 made in the starting is not true. Hence the Hypothesis 1 “On active carding product marketplace, a particular seller/ vendor is limited to particular market only.” does not hold true. It is important to remember that the dark web has a number of websites but for this study, only 4 are considered and for this research, only one category (carded product) is being considered.

- **Seller specialization.**

Table 4 to 10 lists the vendor product along with the vendor name. The specialization of the vendor could be determined if the vendor sells only a particular product or sells in a particular category only. The carded product is itself a very small category of the dark web market place but for our second Hypothesis, we would consider the bifurcation of the product that is listed under the carded product on the market for sale.

The 2 markets out of 4 markets considered in this had a very small share in terms of the product listing and the vendor number too is low. These two markets are Versus and Torrez Market and the product listed under the carded product is also limited in number but the vendor shows specialization. But as we move to a bigger market like Dark Bay then we can see in table 9 and table 10 that the vendors have multiple listings. Hence the vendors do not show specialization in the product category. Unlike the Dark market where the vendors show specialization if we consider carded product market but as we view a bigger picture then the different vendors in the category of the carded products also have listing for a wide variety of products ranging from drugs to online e-book, in fact, all the vendor on all the market have multiple listing under the different category which violates the criteria of seller specialization. Hence the Hypothesis 2 that is “All Vendors for carded products show specialization, that is all the vendors sell only one product type.” is false.

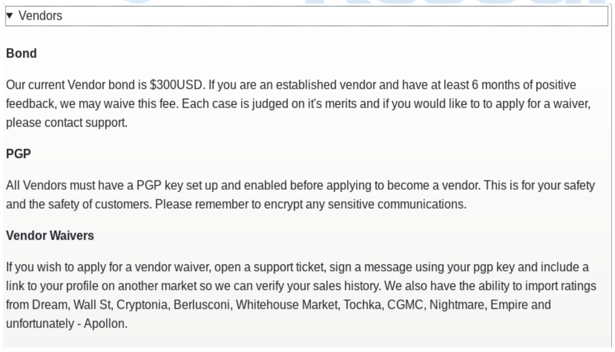
- **Market reputation system.**

In the beginning of the research the Hypothesis 3 (H3) was made that the market under analysis have working reputation systems that are as sophisticated as those of legal marketplaces like Amazon, Ebay, Flipkart which have feedback mechanisms for the seller & the buyer along with the rating for the seller product. The legal markets like Amazon also have buyer protection in the cases of the fraud by the seller. These markets also include the protection for your money and if you face any problem related to your product then you can always raise a dispute against the seller on the market via email or in the website itself for the resolution. The reputation system that exists for the Dark Web website is as follow:

1. Vendor bond: This is the fee charged by the markets on the dark web to let the vendor list their product on their platform which also acts as a surety in case the seller has done some fraud with the buyer. This vendor bond is taken by all 4 websites if any fraud takes place then the vendor bond's money is being used to settle out the matter related to a particular vendor.

The Vendor bond is taken by the darkweb website in order to make sure that the seller do cheat the buyer but if the vendor is already a renowned vendor on the other market then the vendor can apply for the waiver of vendor bond for the particular Market and can list the product and start trading. It acts as a sign of a surety for the market as well as the buyer and acts as buyer protection.

The vendor fee is not universal for all markets but these are fixed by the market itself and the minimum vendor fee was observed at Torrez market at $ 250 and the vendor fee for dark market and darkbay market is $ 300. The Versus market does not display the vendor fees online so it could not be ascertained.



▾ Vendors

Bond

Our current Vendor bond is $300USD. If you are an established vendor and have at least 6 months of positive feedback, we may waive this fee. Each case is judged on it's merits and if you would like to to apply for a waiver, please contact support.

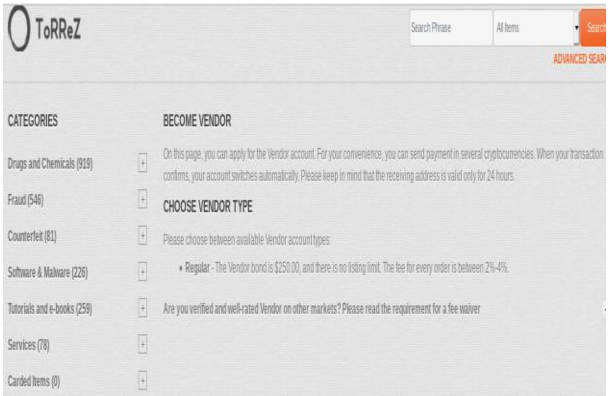
PGP

All Vendors must have a PGP key set up and enabled before applying to become a vendor. This is for your safety and the safety of customers. Please remember to encrypt any sensitive communications.

Vendor Waivers

If you wish to apply for a vendor waiver, open a support ticket, sign a message using your pgp key and include a link to your profile on another market so we can verify your sales history. We also have the ability to import ratings from Dream, Wall St, Cryptonia, Berlusconi, Whitehouse Market, Tochka, CGMC, Nightmare, Empire and unfortunately - Apollon.

Figure 11: Screenshot taken from Dark Market showing the Vendor bond information



BECOME VENDOR

On this page, you can apply for the Vendor account. For your convenience, you can send payment in several cryptocurrencies. When your transaction confirms, your account switches automatically. Please keep in mind that the receiving address is valid only for 24 hours.

CHOOSE VENDOR TYPE

Please choose between available Vendor account types:

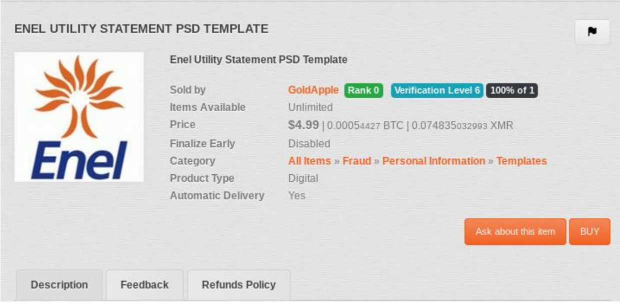
- **Regular** - The Vendor bond is $250.00, and there is no listing limit. The fee for every order is between 2%-4%.

Are you verified and well-rated Vendor on other markets? Please read the requirement for a fee waiver

Figure 12: Screenshot taken from Torrez Market showing the Vendor bond information

2. Feedback and rating mechanism: All the 4 analyzed markets had the feedback mechanism along with the rating mechanism same as a normal legalized markets like Amazon, Flipkart, etc. in which the buyer can provide its valuable feedback along with the rating like a star for the services/ product they have purchased from the vendor. This feedback and rating help to build the reputation of the vendor which in turn attract the more customer and build the customer base for the particular website.

During this research, the 4 markets were analyzed and all 4 markets had the fully functional feedback and rating mechanism and for the convenience of the customer. The market also has the ranking or the level mechanism for the vendor. Higher the level or rank more is the trust and these level could be increased by fulfilling the order.



ENEL UTILITY STATEMENT PSD TEMPLATE

Enel Utility Statement PSD Template

Sold by	GoldApple Rank 0 Verification Level 6 100% of 1
Items Available	Unlimited
Price	$4.99 | 0.00054427 BTC | 0.074835032993 XMR
Finalize Early	Disabled
Category	All Items » Fraud » Personal Information » Templates
Product Type	Digital
Automatic Delivery	Yes

Figure 13: Random listing from the Torrez Market showing the feedback option along with the rank/level of the vendor

3. Dispute resolution: In the case of any dispute regarding any product, all 4 market websites offer the dispute resolution facility with end-to-end encryption for the safety of both parties. The 4 websites also have the feature to talk with the vendor directly so the buyer can clarify all its doubts and still if the dispute occurs then it could be resolved at the dispute center of the website. This dispute resolution works the same as that of a normal market like Amazon or Flipkart etc. where the buyer raises the dispute and the website checks and resolves.

4. Payment security: All the payment on the dark web is accepted in the form of cryptocurrency which helps both sender and receiver to stay anonymous while using the services provided by the dark web market. All Dark Web market has the Escrow payment (multi-signature payment) option in which the payment sent by the buyer is not completed without the multiple approvals. For example, the person buys a product from the dark web market and the buyer sends money to the market for the particular product. Then the vendor processes the order and as soon as the buyer receives it. He confirm that with the website and then the payment is been released to the vendor. So this is a very effective payment method to dodge the fraud on Dark Web

Hence, after accessing all 4 markets for the various mechanisms employed to safeguard the customer we can say that the Dark Web market is as sophisticated as that of the market present on the clear-net. So our Hypothesis 3 that the carding product market under analysis has working reputation systems that are as sophisticated as those of legal marketplaces like Amazon, Flipkart stands true.

- **Dark Web Market growth.**

At the starting of the research, we made a Hypothesis 4 (H4) that the active carding market is growing. In order to arrive at the conclusion for this, we have to consider the factors like the user base, vendor number, the product listed on each of the markets selected for this study except the versus for which data could not be retrieved.

1. Total Product Listed: The number of product listed as on 9/March/2020 on the Dark Market were 25679 (total listing in all category). After the 2 months, the total product listing showed an increase of 31.6134 % as on 10/May/2020 the product listed number stood at 33797.

The number of products listed on the Dark Bay on 9/March/2020 is 59330 and after 2 months the product listing showed a decrease of 2.49452 % and the number of product listings was recorded as of 10/May/2020 was 57701.

The number of products listed on the Torrez Market on 10/March/2020 was 74 and the total number of product listing after two months showed a tremendous increase of 1725.68% as on 11/May/2020 the total product listed were 1351.

2. Total User: The number of users on the Dark Market on 10/March/2020 was 91397 and after the 2 month period on 10/May/2020 it increased by 58.4855% and the total user stood at 144851 on the Dark market.

The number of user on Dark Bay on 10/March/2020 were 62043 and after 2 months on 11/May/2020 it increased by 27.2537% and the total user listed on the website were 78952.

The number of user on Torrez Market on 10/March/2020 were 575 and after 2 month period on 11/May/2020 it increased by 410.087% and the total user listed on the website were 2933 on 11/May/2020.

3. Total Vendor: The number of vendors on the Dark Market on 9/March/2020 was 1115 and after the 2 month period on 10/May/2020 it decreased by 2.06278% and the total vendor was 1092 on the Dark market.

The number of the vendor on Dark Bay on 9/March/2020 was 616 and after the 2 month period on 10/May/2020 it decreased by 1.62338% and the total vendor registered was 606 on Dark Bay.

The number of vendors on Torrez Market on 10/March/2020 was 33 and after the 2 month period on 11/May/2020 it increased by 266.667% and the total vendor were 121 on Dark Bay.

If we come to a conclusion after analyzing the stats that are presented above for the number of products, users, vendors then we can come to the conclusion that the Dark Web markets are on the rise irrespective of the various international agencies behind them.

The total number of product listed, the total number of user, and vendor shows the rapid growth if we neglect the slight dip of 1.5~2.5% in certain cases that could be due to various other factors but they do not point towards the activity decline in any market as the user base of all the market have rapid growth.

Hence we can say that Hypothesis 4 that the active carding markets are growing even after the strict policies of government internationally stands true.

- **Shortcoming of present practices in law and enforcement agencies**

The term Financial fraud and Cyber Fraud are not been explained by any guideline on fraud by RBI or any legislation in India respectively which opens the window for misinterpretation by the law enforcement agencies and other relevant agencies leading to a slow justice process in long run.

The data collection in India also has many shortcomings which the Government itself accepted when RBI is replying to RTI saying that they have not kept a record of cyber crime that amounts to less than 1 lakh in the period from April 2009 till April 2017.

The finance minister also accepted that RBI data for frauds that are recorded under the 'Cyber Frauds' are not available, due to which all the data concerned with cyber frauds are written under the category 'Card/Internet - Debit Cards, Credit Cards & Internet Banking while replying to question in Lok Sabha.

The fine that are been imposed by IT Act 2000 through sections 43, 66, 66B, 66C and 66D may not fit the gravity of crime in certain cases where the person may have lead to losses amounting to more than the fined amount mentioned among the section of IT Act.

CONCLUSION

Conclusion

The carded product market which is a small part of the dark web underground marketplace is very complex in nature due to the diversity it has and the use of sophisticated tools used to keep the user and the person on the other end anonymous on priority. The carded market does not have a large category of product bifurcation but on the active carded marketplace, the particular vendor is not restricted to a particular market. The vendor may be listed on the other markets also in order to increase the incoming order from multiple illegal websites. Thus, it helps the vendor to have more income by processing multiple orders from multiple sites. Following the same pattern in order to have multiple income sources, it is observed that sellers are not restricted by providing a particular product or have any specialization in the carded product market, that is most of the vendors do not sell only one product type.

The Vendor alone cannot have a large number of product listings without the dark web market places where all the buyers and vendors interact with each other and process their orders virtually by providing the interface to the buyer to pays the amount for the order. These markets also have encrypted chat services through which the buyer can directly contact the vendor in case of doubt (similar to the eBay platform but it is encrypted), the buyer can raise the dispute or ticket if the buyer faces any issue with an order, have a refund and return policy, and payment protection for the safety of the buyer. These features help the buyer to have trust in these websites and Hence attract the customer due to which we can observe that the dark web market is seeing the constant boom even after the strict policies of the government internationally. The Dark Web market is very complex in nature due to the diversity and prerequisite knowledge required in order to dive into it.

The Dark Web markets: Versus, Dark Market, Dark Bay, and Torrez Market all have a working reputation system that is very much comparable to the online market like Amazon, Flipkart, etc. Because they have a presence of Feedback and rating mechanism, Vendor bond, Dispute resolution, Payment security.

The total number of product listed, the total number of user, and vendor shows the rapid growth if we neglect the slight dip of 1.5~2.5% in certain cases that could be due to various other factors but they do not point towards the activity decline in any market as the user base of all the market have rapid growth. Hence, we can say that the dark web market is growing even after the strict policies of government internationally, and if we talk about India then India should first have proper data collection tags and categories to evaluate the value of the fraud Indian cyber space is tackling along with more rigid laws, definition & policy. So, that accordingly India and other countries can exchange the Data in a fast-paced manner to tackle the growth of the underground market by adopting the universal legislation and laws pertaining to cyber.

REFERENCES

1. *Reserve Bank of India - Speeches*. (2013, July 29). Reserve Bank of India. Available at: <https://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826>

2. McKinsey & Company. 2019. *Financial Crime and fraud in the age of cyber security*. [online] Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf

3. S Naidu, J., 2020. *'₹615.39Cr Lost To Debit, Credit Card Frauds'*. [online] Hindustan Times. Available at: <https://www.hindustantimes.com/mumbai-news/615-39cr-lost-to-debit-credit-card-frauds/story-E335UM0fj1dVKJYZcJ2zRN.html>.

4. Sharma, S., 2020. *Hundreds Of Crores Of Rupees Lost In Card Payment, Internet Banking Frauds In Just 3 Months*. [online] The Financial Express. Available at: <https://www.financialexpress.com/industry/banking-finance/hundreds-of-crores-of-rupees-lost-in-card-payment-internet-banking-frauds-in-just-3-months/1886386/>.

5. Ukfinance.org.uk. 2020. *Fraud The Facts 2019*. [online] Available at: <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf>.

6. Ukfinance.org.uk. 2020. *Fraud-The Fact 2020*. [online] Available at: <https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf>.

7. Blog.cyble.com. 2021. *One Million Credit Cards Leaked In A Cybercrime Forum For Free.* [Online] Available at: <https://blog.cyble.com/2021/08/08/one-million-credit-cards-leaked-in-a-cybercrime-forum-for-free/>

8. Su, J. (05/August/2019). '*Data Breach Alert: Over 1 Million Credit Card Data From The U.S., South Korea Have Been Leaked*'. Forbes. Retrived from: <https://www.forbes.com/sites/jeanbaptiste/2019/08/05/data-leak-alert-over-1-million-credit-card-from-the-u-s-south-korea-have-been-stolen/?sh=1a84e620928e>

9. Ganjoo, S., 2020. *Details Of 1.3 Million Indian Credit And Debit Cards Selling Online: Everything You Need To Know In 10 Points*. [online] India Today. Available at: <https://www.indiatoday.in/technology/features/story/details-of-1-3m-indian-cards-selling-online-everything-you-need-to-know-in-10-points-1614411-2019-10-31>.

10. Hariharan, S. (31/March/2021). '*Security breach: 8.2TB data up for sale on dark web*'. The Times of India. Retrieved from: <https://timesofindia.indiatimes.com/business/india-business/security-breach-8-2tb-data-up-for-sale-on-Dark Web/articleshow/81769741.cms>

11. IANS (04/January/2021).'*10 crore Indians' card data selling on Dark Web: Researcher'*. The Economic Times. Retrieved from: <https://economictimes.indiatimes.com/tech/technology/10-crore-indians-card-data-selling-on-Dark Web-researcher/articleshow/80093994.cms?from=mdr>

12. Joseph, V., & Ray, D. (10/February/2020). *Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence*. Mondaq. Retrieved from: <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>

13. Haslebacher, A., Onaolapo, J. and Stringhini, G., 2017. *All Your Cards Are Belong To Us: Understanding Online Carding Forums | Request PDF*. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/317555385_All_Your_Cards_Are_Belong_To_Us_Understanding_Online_Carding_Forums>.

14. Ablon, L., C. Libicki, M. and M. Abler, A., 2020. *Markets For Cybercrime Tools And Stolen Data*. [online] Rand.org. Available at: <https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf>.

15. E. Goodison, S., Woods, D., D. Barnum, J., R. Kemerer, A. and A. Jackson, B., 2019. *What Could Help Law Enforcement Deal With Crime On The Dark Web*. [online] Rand.org. Available at: <https://www.rand.org/pubs/research_reports/RR2704.html>.

ENDNOTES

[i] RBI Speeches & Interviews -Inaugural address by Dr. K.C. Chakrabarty, Deputy Governar, Reserve Bank of India (29/July/2013) https://www.rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826

[ii] McKinsey & Company. 2019. *Financial Crime and fraud in the age of cyber security*. [online] Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf

[iii] S Naidu, J. (11/February/2020). *'₹615.39Cr Lost To Debit, Credit Card Frauds'*. Hindustan Times. Retrieved from: <https://www.hindustantimes.com/mumbai-news/615-39cr-lost-to-debit-credit-card-frauds/story-E335UM0fj1dVKJYZcJ2zRN.html>.

[iv] Sharma, S. (02/March/2020). '*Hundreds Of Crores Of Rupees Lost In Card Payment, Internet Banking Frauds In Just 3 Months*. The Financial Express. Retrieved from: <https://www.financialexpress.com/industry/banking-finance/hundreds-of-crores-of-rupees-lost-in-card-payment-internet-banking-frauds-in-just-3-months/1886386/>

[v] Retrieved from Hundreds Of Crores Of Rupees Lost In Card Payment, Internet Banking Frauds In Just 3 Months. Copyright 2020 by Financial express

[vi] Retrieved from Fraud The Facts 2019. Copyright 2019 by Rand Corporation.

[vii] Retrieved from Fraud The Facts 2019. Copyright 2019 by Rand Corporation.

[viii] Retrieved from Fraud The Facts 2019. Copyright 2019 by Rand Corporation.

[ix] Retrieved from Fraud The Facts 2019. Copyright 2019 by Rand Corporation.

[x] Ukfinance.org.uk. 2020. *Fraud The Facts 2019*. [online] Available at: <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20%20FINAL%20ONLINE.pdf>.

[xi] Retrieved from Fraud-The Fact 2020. Copyright 2020 by Rand Corporation.

[xii] Retrieved from Fraud-The Fact 2020. Copyright 2020 by Rand Corporation.

[xiii] Retrieved from Fraud-The Fact 2020. Copyright 2020 by Rand Corporation.

[xiv] Ukfinance.org.uk. 2020. *Fraud-The Fact 2020*. [online] Available at: <https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf>.

[xv] Blog.cyble.com. 2021. *One Million Credit Cards Leaked In A Cybercrime Forum For Free*. [Online] Available at: <https://blog.cyble.com/2021/08/08/one-million-credit-cards-leaked-in-a-cybercrime-forum-for-free/>

[xvi] Su, J. (05/August/2019). '*Data Breach Alert: Over 1 Million Credit Card Data From The U.S., South Korea Have Been Leaked*'. Forbes. Retrived from: <https://www.forbes.com/sites/jeanbaptiste/2019/08/05/data-leak-alert-over-1-million-credit-card-from-the-u-s-south-korea-have-been-stolen/?sh=1a84e620928e>

[xvii] Ganjoo, S. (31/October/2020). '*Details Of 1.3 Million Indian Credit And Debit Cards Selling Online: Everything You Need To Know In 10 Points*. India Today. Retrieved from: <https://www.indiatoday.in/technology/features/story/details-of-1-3m-indian-cards-selling-online-everything-you-need-to-know-in-10-points-1614411-2019-10-31>

[xviii] Hariharan, S. (31/March/2021). '*Security breach: 8.2TB data up for sale on dark web'*. The Times of India. Retrieved from: <https://timesofindia.indiatimes.com/business/india-business/security-breach-8-2tb-data-up-for-sale-on-Dark Web/articleshow/81769741.cms>

[xix] IANS (04/January/2021).'*10 crore Indians' card data selling on Dark Web: Researcher'*. The Economic Times. Retrieved from: <https://economictimes.indiatimes.com/tech/technology/10-crore-indians-card-data-selling-on-Dark Web-researcher/articleshow/80093994.cms?from=mdr>

[xx] Joseph, V., & Ray, D. (10/February/2020). *Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence*. Mondaq. Retrieved from: <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>

[xxi] Haslebacher, A., Onaolapo, J. and Stringhini, G., 2017. *All Your Cards Are Belong To Us: Understanding Online Carding Forums | Request PDF*. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/317555385_All_Your_Cards_Are_Belong_To_Us_Understanding_Online_Carding_Forums>.

[xxii] Ablon, L., C. Libicki, M. and M. Abler, A., 2020. *Markets For Cybercrime Tools And Stolen Data*. [online] Rand.org. Available at: <https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf>.

[xxiii] E. Goodison, S., Woods, D., D. Barnum, J., R. Kemerer, A. and A. Jackson, B., 2019. *What Could Help Law Enforcement Deal With Crime On The Dark Web*. [online] Rand.org. Available at: <https://www.rand.org/pubs/research_reports/RR2704.html>.