Introduction to Digital Forensics Assignment 1

Emma van den Broek | s2804859
Aukje Hekstra | s2294184
Rik Helder | s2864010
Inèz Hemme | s2429837
Ewoud Janus | s2395762
Koen Wilms | s1818872

University of Twente
Introduction to Digital Forensics for Cybercrime

Introduction

The dark web is a hub for internet users who want to remain anonymous whilst browsing the internet. In itself the dark web is not necessarily cause for major concerns, but as the dark web is largely unmonitored and anonymous, illegal activities tend to take place. On the dark web exist marketplaces where users can anonymously purchase different products, services, or other things. These can be legal, but also plenty of illegal items, services, or information are sold on these dark web marketplaces. This is cause for concern, as these marketplaces are not governed by authorities. To reduce crime in general, it can be valuable for authorities to have a closer look at these marketplaces and see what can be done. The goal of this report is to give an overview of what can be found on the dark web, which marketplaces are commonly used, and identify big sellers at whom authorities should take a closer look.

Motivation and goals

In order to know what actions can and should be taken, it is necessary to first have an understanding of what is offered on dark web marketplaces. In this document an analysis of a number of dark web marketplaces can be found with over 100 listings mentioned and analysed. The full methodology and results are described below.

Personal information is one of the more dangerous ‘products’ sold on the dark web. Especially in regard to leaked information, understanding what information is gathered and sold can help with knowing where the weaknesses in security are and what the threats to privacy are, which in turn can help understand what action plans to design to prevent this sensitive data from being leaked in the first place. This abundance of purchasable personal data that is available online leaves people in a more vulnerable position. Personal data could be used for a targeted attack, like for example for spear phishing. The consequences of personal data being available for purchase can be severe and obtaining this information is often relatively achievable. A Dark Web Price Index (Zoltan & ., 2023) made in 2023 found that a full range of documents that would allow for identity theft could be obtained for around 1000 USD. Phenomena like these will likely have a negative impact on the lives of individual people and society as a whole, and therefore taking action to prevent this from happening is something that should be of concern.

International efforts to seize illegal dark web marketplaces have taken and are taking place. An example of such efforts is OPERATION SpecTor (Europol, 2023), which was coordinated by Europol and involved nine countries. As a result, 288 suspects were arrested and EUR 50.8 million was seized, as well as 850 kg of drugs and 117 firearms. This operation was made possible because of the evidence provided by German authorities, who seized the criminal infrastructure of the marketplace “Monopoly Market”, at the end of 2021. In order to be able to repeat operations such as the one mentioned, it is likely to be valuable to identify which illegal dark web marketplaces are currently being used the most and who the top sellers are. This way, action taken can be more efficient and have a larger impact.

Methodology and Results

Each member of the group has investigated a different marketplace on the dark web. This gives the opportunity to compare differences and similarities between the six marketplaces once results are gathered. These different marketplaces were selected individually by the group members, the only thing that was checked was whether the site was an onion site, and it was made sure that no two members checked the same marketplace. Apart from that, the sites were chosen randomly. Since posts were picked randomly, sellers are very different and they may not give a representative sample of sellers on the dark web. Additionally, some of the websites lack a good filtering system, making it impossible to select the top ten sellers from all the websites that were investigated.

Per marketplace 17 different listings have been examined and split into services or products, after which more categories have been introduced to distinguish further between the listings. For example ddos, drugs, gift cards, money, guns etc. These different categories can be seen in the spreadsheet. From these listings the sellers have also been investigated to find, if possible, the rating of the seller, the amount of listings, amount of transactions and the price range.

In order to discern if an offered service or product is legal, it is held against the Dutch law. The laws of the country from which the item originates, were not taken into account. The legality of some products, like prescription drugs, can depend on certain aspects. In those cases, if it is illegal to sell or otherwise distribute the item without the proper authorization, certification and/or documentation, the item is classified as illegal. If an item is only allowed to be distributed in a small quantity, this then also has an influence on whether the item is listed as legal or illegal.

Investigated Marketplaces

The TorDepot website has only been running since August 23rd 2023, therefore it is a smaller site at the moment that is still building its seller and customer base. Currently it deals with money selling and some game console business and has 106 active listings, but the categories listed indicate the website wanting to branch out into drugs and other services. This might make it reasonable for authorities to at least keep an eye on them to see where the marketplace goes and how it grows traffic wise.

Incognito Market is a webshop exclusively selling drugs and tobacco. It is a website having 1448 vendors where most have around 100 sales, this scale is smaller compared to the other markets that have been investigated. All payments are either done via Bitcoin (BTC) or Monero (XMR). It has been an established website since January 2021 according to darknetstats.com. However reviews from users on darknetstats have been talking about an exit scam recently developing, casting a shadow on the marketplace’s reliability and trustworthiness

The Dark Market can be found on the darknet and sells different, mostly illegal, products and services. The highest amounts of reviews on products are in the categories of hacking, drugs, and money. The Dark Market seems to be a small to medium market, with only a number of listings per category. There also seems to be little traffic going through the website, as most listings have less than ten reviews and there is no information about total number of sales. For most categories there seems to be only one main seller, sometimes a smaller seller will also have a listing posted under the same category.

Undermarket2.0 is one of the biggest dark web marketplaces found in this report. Having sales numbers of sellers commonly exceed tens of thousands of sales. The website claims to be a totally anonymous and highly secure webshop, where payment is not stored and is done through an escrow. They take pride in being user friendly and easy to use. They list a total of 70 sellers on their website who sell different products and services, ranging from cigarettes and drugs, to money and electronics devices.

Techmarket is a tech webshop on the darkweb. It is a relatively small webshop with around 32 sellers. The products that are selled on this market range from gift cards, money transfers, carding, electronics and hacking services. Many of the reviews on this site seem to be fake, since multiple of the same reviews appear on different products. On top of that, all the reviews are anonymous. This all shows that it might not be a trustworthy site to buy products off.

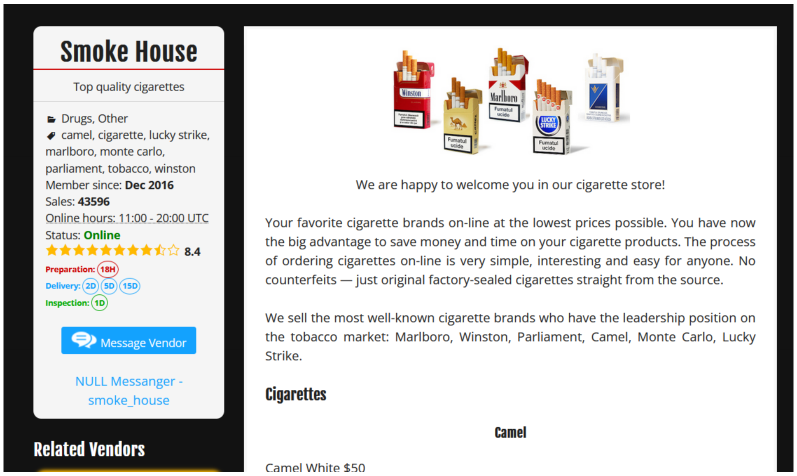
BlackMart is a small marketplace on the darkweb with only 5 sellers. On this marketplace carding, money transfers, gift cards, money money counterfeits, documents and electronics can be bought. Even though it is a small marketplace, the biggest seller has made a total of 30800 sales since 2017.

Bohemia is a marketplace with a focus on drugs, but which also offers items such as exploits and malware, identification documents, banknote forgeries, hacker services and tutorials. The site was launched in May of 2021. The past year, it had 951 active vendors, making it a relatively large site. Bohemia has had a lot of issues with not being reachable online. As of writing this report, no connection has been possible for the past three days. The site has admitted to frequently having to deal with DDoS-attacks, which likely is at least part of the cause of the site being unreachable. Another theory, which is floating around online, is that the website is exit scamming. Reasoning behind these allegations is that some users have reported withdrawal issues or their accounts having been frozen.

Top ten sellers

The Github file (Hekstra, 2023) for this assignment provides the code that was used to automatically find the top ten sellers. There are two criteria on which a top seller can be identified: amount of successful transaction or the rating of the seller. Not all sites mention the amount of successful transactions and this makes it harder to determine the biggest sellers. These sellers seem to have the most (successful) transactions, but they are not necessarily the ones authorities should focus on. These sellers should definitely be kept in mind when selecting sellers to focus on further, but just because they have made a lot of sales does not mean they have the biggest impact on society as a whole. Which, if that is the goal, needs a few more criteria to select which sellers to focus on.

From the sites that provide this data, the biggest seller is from the site Undermarket2.0. The seller calls themselves “Smoke House” and sells cigarettes. This seller “Smoke House” has a total of 36863 successful transactions.



Smoke House

Top quality cigarettes

Drugs, Other
camel, cigarette, lucky strike, marlboro, monte carlo, parliament, tobacco, winston
Member since: **Dec 2016**
Sales: **43596**
Online hours: 11:00 - 20:00 UTC
Status: **Online**
★★★★★★★★☆☆ 8.4
Preparation: 18H
Delivery: 2D 5D 15D
Inspection: 1D

NULL Messanger - smoke_house

Related Vendors

We are happy to welcome you in our cigarette store!

Your favorite cigarette brands on-line at the lowest prices possible. You have now the big advantage to save money and time on your cigarette products. The process of ordering cigarettes on-line is very simple, interesting and easy for anyone. No counterfeits — just original factory-sealed cigarettes straight from the source.

We sell the most well-known cigarette brands who have the leadership position on the tobacco market: Marlboro, Winston, Parliament, Camel, Monte Carlo, Lucky Strike.

Cigarettes

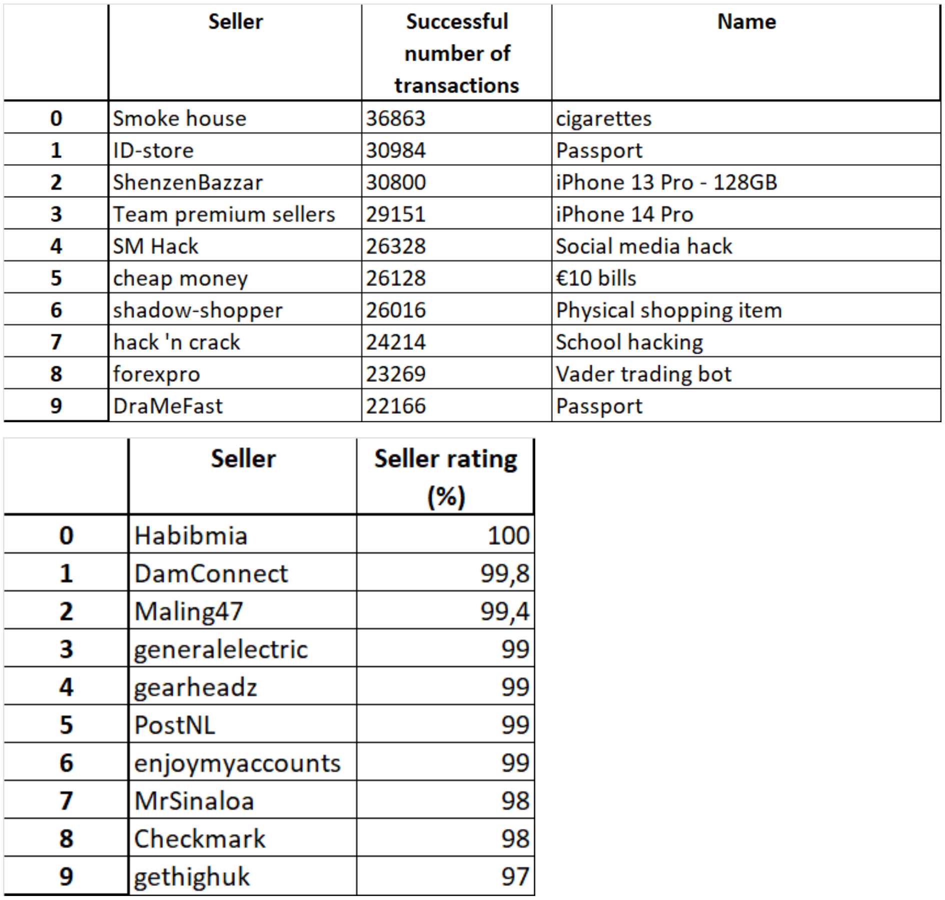
Camel

Camel White $50

Figure 1. Product page of cigarettes from seller "Smoke House" on Undermarket 2.0.

Aside from "Smoke House" the remaining top sellers sell a range of products and services, including passports, Iphones, social media hack, Euro bills, physical shopping item, school hacking and a vader trading bot. Most of these top sellers make use of Undermarket2.0, except for one seller called "ShenzenBazzar", who sells on a different website called BlackMart.

The code will automatically output a xlsx file that shows the top ten sellers for both the rating and the transactions. As can be seen, the seller with a 100 procent star rating is Habibmia. This seller sells uncut cocaine on the Bohemia marketplace.



	Seller	Successful number of transactions	Name
0	Smoke house	36863	cigarettes
1	ID-store	30984	Passport
2	ShenzenBazzar	30800	iPhone 13 Pro - 128GB
3	Team premium sellers	29151	iPhone 14 Pro
4	SM Hack	26328	Social media hack
5	cheap money	26128	€10 bills
6	shadow-shopper	26016	Physical shopping item
7	hack 'n crack	24214	School hacking
8	forexpro	23269	Vader trading bot
9	DraMeFast	22166	Passport

	Seller	Seller rating (%)
0	Habibmia	100
1	DamConnect	99,8
2	Maling47	99,4
3	generalelectric	99
4	gearheadz	99
5	PostNL	99
6	enjoymyaccounts	99
7	MrSinaloa	98
8	Checkmark	98
9	gethighuk	97

Figure 2: Tables of the top 10 sellers. Top figure: top 10 sellers with the most transactions and the corresponding product.

Top three sellers to be investigated

Three sellers were selected which were deemed most important to be investigated by authorities further. These sellers were chosen based on some criteria, the most important criteria was what the impact of their product is on the general population. Other criteria include how many transactions have been made and how highly the seller is rated on their respective marketplace.

The first seller who should be investigated is “gearheadz” on the Bohemia website. This seller was picked out for several reasons. First of all the seller deals in opioids, which are responsible for a significant amount of yearly drug deaths (National Institute of Health, 2023). Here it shows that opioids are on the rise in the amount of drug related deaths each year. Next to the impact the seller's product has on society, the large amount of transactions is another reason that this seller should be investigated. So far there are 3500 transactions for this seller. So the combination of a large amount of transactions combined with the impact the drugs being sold have makes investigating the seller important.

“EU-Asylum" from Undermarket2.0 is another big seller who should be investigated. This seller has a total of 12054 successful transactions. “EU-Asylum” has 5 active listings and has a price range between $1.000 and $1.500. This seller not only sells identity documents, but also refugee status papers. The seller claims to have contacts in the governments of different countries and can get the buyers information into their systems. This is misuse of the poorest and most desperate people in the world. The consequences of being found with falsified documents is often being sent back to the country of origin. This targets those people specifically. It is morally wrong to target these people. The different papers could also be used for human trafficking, or be used by terrorist organisations to get their people into different countries to perform terrorist attacks. Therefore it is important for authorities to know about this seller and make an attempt to stop their business.

The final seller advised for investigation is called “Smoke House”. They operate on Undermarket2.0 and sell cigarettes by the carton. “Smoke House” has 35 listings of different types of cigarettes and sells them between $49 and $54 per carton. This in itself may not be a reason to specifically investigate them, but between October 9th 15:15 2023 and October 11th 13:30 2023 they have made nearly seven thousand transactions according to the Undermarket2.0 site. When every order costs a minimum of $49, the total amount of money transferred in these three days will likely be well over $350,000. This should be of concern for authorities, as likely no taxes have been paid over any of these profits. Also how the seller gains their cigarettes is not certain, they claim to get the cartons straight from the factory source. All of this combined makes them a valuable target for authorities to investigate further.

Most surprising posts

When looking at the gun laws in the Netherlands it was shocking to find that it is extremely easy to buy a gun on the darkweb. For just 430 USD it is possible to buy a SIG Sauer P320, a semi-automatic handgun that can easily kill a person. The opportunity that guns give a person to commit terror attacks was recently displayed in the hospital of Rotterdam where an armed person killed multiple people. Assuming the sellers legitimately have these guns, and are able to get them to the customer, it is extremely easy for someone to commit a murder, robbery or terror attack whatever their reasoning is. The only requirements are a tor browser and some crypto currency to pay the seller.

Also, a lot of fake passports/ID cards and certificates can be found on the darkweb. For just 39 dollars a fake passport can be bought. It was surprising to find out how easy it is to obtain fake documents. The availability of fake documents offer people tools to easily commit identity theft and fraud.

That different currencies were sold was in itself not a big shock, but just how cheap it was to purchase thousands of euros or dollars in counterfeit money was shocking. One could easily get ten times as much money as what they paid in a bitcoin wallet, or on a credit card. Some sellers even gave up to and over 100 times the value in return. The legitimacy of some of these listings should be taken into consideration. The most surprising listing that was found was a purchasable bitcoin wallet with 100 bitcoin in it, only costing $27,487.00. Also, indirect money could be found in gift cards, credit cards and the like.

General price per category

To see what the general prices of the products are, a boxplot was made in the code (Hekstra, 2023). This is per category, so no specific products that can be compared. Also, the fliers of the data are removed to make the figure readable. For example, the 100 BTC purchase of more than 27 thousand dollars is not included. These fliers are outside of the bounds of 1,5 times the inter-quartile range (IQR) (The Matplotlib development team, n.d.). The code for the boxplot can be found in the github file for this assignment.

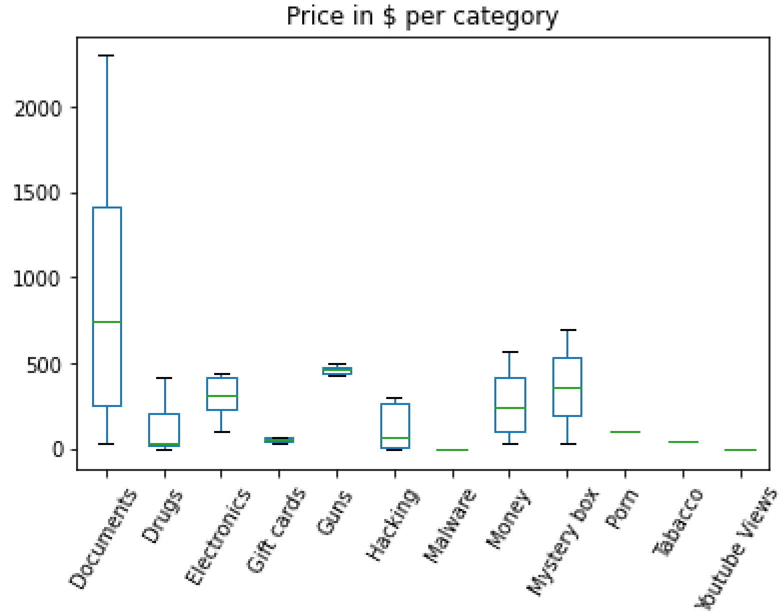


Figure 3: Boxplot without the fliers (outside 1,5 IQR) of prices of products per category.

For some categories, the prices are in a small window. This could be due to the fact that some smaller categories are made with very few data points.

Conclusion and Reflection

The dark web is used for a lot of different things. Purchasing different goods, either legal or illegal, is common on the dark web and is usually done through dark web marketplaces. Seven different dark web marketplaces were analysed, some bigger sites, and some smaller sites. From these marketplaces, between 4 and 17 listings were selected for further analysis. Most of the listings found in this report are, in some way, illegal according to Dutch law, either because no taxes are paid, or because ownership/selling of the products is simply illegal. The top ten sellers from these marketplaces were identified for authorities to monitor. Three sellers were identified which were deemed to be the most important for authorities to actually investigate.

There are many different things that can be found on the dark web market. The different products and services are classified in twelve different categories. Some legal things can be found, but most are illegal or at least questionable. This includes guns, drugs, falsified money or documents and hacking services. These categories were made to include as many listings as possible, though not all categories have a lot of listings in them. For example the Youtube Views category only has one item. For future research, more broad and better defined categories would be advised.

It should be acknowledged that some cells in the Excel file are left empty for some websites, this was because these websites did not give the necessary information. This is not necessarily an issue, but it needs to be mentioned that it has an impact on some of the selections made. The top ten sellers were identified based on the number of successful transactions and their rating, not all websites gave this information about their sellers or their transactions. The sellers on these websites could not be included in this calculation. During the exploration phase this could have been prevented and a different website could have been selected or different criteria for the top ten sellers could be identified.

All in all, the search done in this report can be a valuable starting point for authorities if they want to identify some sellers or marketplaces for further investigation. Though it should be kept in mind that the search done in this report was limited to only a few marketplaces and a number of randomly selected listings per website. Few listings of the same seller were included in this search, which broadens the scope and allows for a broader overview of available items on each marketplace. This also causes the information in this report to not be as detailed or focused on specific sellers.

References

Europol. “288 dark web vendors arrested in major marketplace seizure | Europol.” *Europol*, 2 May 2023, https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure. Accessed 11 October 2023.

Hekstra, Aukje. “Github: project group 2.” *Github project*, 11 October 2023, https://github.com/Aukiee/CSCC_minor.git. Accessed 11 October 2023.

National Institute of Health. “Drug Overdose Death Rates.” *NIDA.NIH.GOV | National Institute on Drug Abuse (NIDA)*, National Institutes of Health, 30 June 2023, https://nida.nih.gov/research-topics/trends-statistics/overdose-death-rates. Accessed 11 October 2023.

The Matplotlib development team. “matplotlib.pyplot.boxplot — Matplotlib 3.8.0 documentation.” *Matplotlib*, https://matplotlib.org/stable/api/_as_gen/matplotlib.pyplot.boxplot.html#matplotlib.pyplot.boxplot. Accessed 11 October 2023.

Zoltan, Miklos, and Shanika W. . “Dark Web Price Index 2023 - Exclusive Research.” *Privacy Affairs*, 23 April 2023, https://www.privacyaffairs.com/dark-web-price-index-2023/. Accessed 11 October 2023.