

Cyber Threats-as-a-Service Economy: A Dark Business

Vivek Tejas Rao
Department of Computer &
System Sciences, Stockholm
University
Stockholm, Sweden
vira3085@student.su.se

Abstract—The internet has provided plethora of opportunities for the modern society. Various avenues exist for the purpose of making a living and gaining benefits such as monetary, competitive advantage and intelligence. However, the surface web accessible via the ubiquitous infrastructure is only the tip of the iceberg. The underlying cyberspace constitutes an exceptionally large portion of the internet. The so called “deep web” offers opportunities to mostly engage in illegal activities along with certain other actions which require privacy and anonymity. Additionally, the chat forums which exist on the deep web encourage nefarious communications which otherwise might not be carried out in the public domain. Therefore, this paper focuses on conducting a qualitative research by utilizing netnography as a method on few of the prominent darknet marketplaces in order to investigate the threat landscape that exists for cybersecurity. Chat forums where the criminals engage in communications corresponding to their activities on the marketplace shall also be investigated with the same objective. The insights to be gained upon conducting this study shall enable individuals, corporates or any entity concerned with the security of its ICT infrastructure and law enforcement agencies to understand the catalogue of services being offered which could define the current threat landscape within cyberspace.

Keywords—Darknet, threats, marketplace, forums, cybersecurity

I. INTRODUCTION

A. Background

The world wide web was introduced as a powerful tool for the purpose of solving problems faced by the modern society. With its proliferation, almost every

operation was moved online. The internet soon proved to be a boon for mankind. As time progressed, the complexity of the infrastructure kept on enhancing and evolving which resulted into a revolution. The information age as we all know provided a platform to enable digital transformation. However, the desire for absolute privacy and anonymity led to the emergence of The Onion Router or commonly referred to as the TOR [1]. As users across internet equipped themselves with the anonymising technology, a dark avenue came into existence. [2]. The darknet is unregulated and serves as a breeding ground for mostly unethical and illegal activities. [2] [3].

As reliance on information technology and corresponding infrastructure has peaked, so have the threats to the cybersecurity. As a result, the author suspects that various threats to the security objectives such as confidentiality, integrity and availability might be on sale on the darknet. These threats might be offered in various forms as services. Threats which are typical to cybersecurity include social engineering, malware, unauthorised access, password cracking, exploits for zero-day as well as well-known vulnerabilities, Denial-of-Service or Distributed Denial-of-Service attacks and much more. In order to deploy controls to enable cybersecurity at various tiers, it is vital to be aware of the threats that have the potential to be realized.

It is highly imperative to understand and explore the various threats being sold as services that could compromise the objectives of information and cyber security. As cyber threats are digital in nature, almost everyone is faced with the risks and threats. This study presents an overview of the current threat landscape that originates from the darknet.

B. Research Problem

The darknet comprises of various marketplaces and forums in order to facilitate the business. An updated list of currently active marketplaces and forums can be found in the portal of Dnstats [3]. Currently, very few studies

have been conducted which address the threats to cybersecurity emerging from the darknet. Upon being aware about the catalogue of services offered on the darknet, the corresponding vulnerabilities can be worked upon as well as necessary controls can be deployed.

Therefore, this research shall intend to answer the following research question:

- How mature is the economy on the darknet which facilitates the offering of cybersecurity threats as services?

C. Delimitations

Due to limited resources such as manpower, time and opportunity, this research shall consider the sample from only a few marketplaces and forums. By considering the legal boundaries, items and services offered on the darknet will not be purchased. Interactional data shall neither be produced or analysed since there is high likelihood of being cheated and deceived.

II. LITERATURE REVIEW

A. DARKNET

The realm of internet is composed of layers such as surface web, deep web and the darkweb [2]. These terms although mean similar but have distinct attributes. The legitimate websites which a typical user visits are unencrypted and hosted on the surface web. However, the darkweb or darknet is located within the deepweb and offers much more than a user could imagine. Dedicated protocols and browsers are required to browse through the darknet. One such prominent example is of the Onion Router or TOR browser [1]. The user's request passes through three intermediary nodes before reaching the destination. Hence, privacy and anonymity of the users are prevailed as a result. It is the need of the hour to comprehensively investigate the current happenings in the darknet for the sake of security of our community [2].

B. THE ONION ROUTER

The darknet and its associated elements can only be accessed via a dedicated protocol and browser. One of the prominent examples is the Onion Router [1]. When a user sends a request, it is passed via three (3) relay nodes which act within the TOR network. Every relay node decrypts the request before forwarding to the next relay. The exit relay forwards it to the destination upon

decryption. Hence, privacy and anonymity are upheld since the true source cannot be determined.

C. RELATED WORKS

A vast majority of research studies have focused on determining the maturity of business dealing with drugs on the darknet while very few have focused their objective towards threats against cybersecurity which emerge from the darknet and its associated elements. It is now understood that majority of the products on the darknet are related to drugs as indicated in [2]. The most popular marketplace operating for the sale of illegal drugs was the Silk Road [4]. However, it was later seized by FBI in the United States. Since then, many marketplaces have popped up and enable the business operations.

It has also been investigated and concluded that Ransomware-as-a-Service is now gradually evolving [4]. However, the authenticity and integrity of those services are still questionable. The analysis conducted in [4] emphasize the importance of conducting a research on the structure of the economy as well as its dynamics. The insights to be gained can then be utilized to deploy controls at technical, operational, tactical and strategic level [4].

The exploratory research conducted in [5] illustrates the catalogue of products and services being offered on the Empire Market. It is now understood that such markets are constructed similar to legitimate and legal e-commerce platforms with features such as searching, filtering, choosing payment methods and also enables to view how many times a product or service has been sold [5]. Out of the many products being offered, Drugs represented almost 62.4 % of the catalogue as per findings in [5].

III. METHODOLOGY

A. RESEARCH METHODOLOGY

This research shall utilize netnography as a method for the purpose of conducting an effective study. Netnography [6] can be considered as digital ethnography. However, netnography is highly appropriate since the fieldwork in this research is online and the source of data is computer mediated. Netnography refers to the studies of online traces that exist on social networks [6]. Since darknet marketplace and forums consists of members who leave their digital footprint and traces behind, netnography is considered highly appropriate for this research.

For the purpose of an efficient and effective research, the following flowchart as suggested in [6] [6] shall be utilized:

1. Definition of Research Question, Social Sites to Investigate
2. Community Identification and Selection
3. Data Collection
4. Data Analysis and Iterative Interpretation of Findings
5. Write, Present and Report Findings as well as implications

The steps outlined above represent a simplified view of netnography as a method. Since this research aims to investigate online communities of actors involved on the darknet, a standalone netnography based research is highly appropriate. A blended ethnographic/netnography approach would be suitable if the communities exist outside the cyberspace which is not the case with darknet. Since the context created by the cyberspace constraints the flexibility, this research shall tweak parameters such as adaptability, anonymity, archival and accessibility in order to configure netnography as much as possible as per the suggestions mentioned in the publication [7].

Netnography shall be utilized on the online traces which will be the primary source of data in this research [7]. Just like best research practices, the collection of ethnographic data shall culminate if new insights cannot be gained any further. The collection phase may involve archival or fieldnote data. Co-created refers to the interactional data which the researcher shall proactively produce as a result of his active participation [7]. However, interactional data will not be considered for this study. On the other hand, fieldnote simply means to engage in participatory observation. Appropriate data collection methods shall be applied whenever feasible and suitable. Once data is captured or saved, data analysis phase shall utilize the qualitative coding of the content. Content analysis software may be used in order to expedite corresponding tasks. Open source content analysis tool

B. ETHICAL CONSIDERATIONS

Traditional ethnography differs significantly from netnography and therefore a certain number of ethical dilemmas need to be considered. Moreover, darknet being a target of law enforcement agencies, it is highly imperative to uphold the ethical values with respect to best research practices. Researcher collected archival data from the marketplace and forums without actively disclosing about the presence as suggested by [7]. Cases where data is collected from a blog, the necessary

citations shall be stated. Every user on the darknet uses a pseudo name for the purpose of hiding its identity. The fieldnotes collected will be altered and/or modified so that personal information is not exposed. This research does not try to deceive or mislead the audience and shall not be utilized as evidence to any prosecution.

C. Data Collection

Netnography as an approach was utilized for the purpose of the entire research. Netnography requires that the field be restricted to online sphere. Therefore, data collection methods utilized were customized for this purpose [6]. As mentioned before, data collection was limited to two categories of data such as archival data and field notes. Archival data refers to already posted comments, advertisements and descriptions of products and services on the darknet. To begin this study, the active darknet marketplace was determined from [3]. Black Pass and Dark Bay as determined from [3] were investigated. The collection of archival data involved significant effort as a lot of irrelevant data had to be filtered. Archival data carries with itself a significant amount of importance as it enabled the researcher to analyze the cultural context, feelings, mindset of the community and more. After having filtered the data, the target dataset was recorded. One basic procedure followed was to copy-paste the text into a plain text file. Certain photographs were captured by means of screen capture tool provided by native windows operating system. Automated tools were discarded for this project as it could have hampered the researcher's ability to comprehend the large amass of data to solve the research question. Archival data for this project basically consisted of texts, descriptions of products and services, profile pictures, layout of the advertisement and user generated data.

The second category of data which was generated during the process of data collection was that of field-notes. Field-notes were basically the reflections which the researcher incurred because of gathering the archival data as well as during exploration [8]. The immediate thoughts and opinions produced by the researcher was noted down again in a separate text file for the purpose of analysis. Field notes also carried an equal amount of significance as it conveyed critical details which the archival data could not have exhibited [8] .

D. Sampling

Due to limitations such as opportunity, time and consent, the sampling strategy utilized was to include only relevant items of interest to the define research question. Hence, automated solutions were not adopted but rather manual filtration and selection were adopted. Therefore, purposive sampling was used for this study. Purposive sampling refers to selecting only those data items which are of interest to the research question [9]. The samples under consideration consists of attributes which enabled the researcher to solve the define research question.

E. Data Analysis Method

The data collection phase of this study encompassed specific procedures to record and collect raw data. The sampling strategy resulted in data sets including texts, description, photos and screen captures. As suggested by the article [8], open coding was a technique was utilized for the purpose of analyzing the collected data. Absolute numbers were not recorded. Hence, qualitative data analysis was considered to gain new insights. Thematic data analysis enabled the researcher to gain new insights by means of coding, forming themes and drawing connections among them. Qualitative data analysis enabled the researcher to understand the cultural and emotional implications of the data as generated by the community members. The results obtained after qualitative analysis enabled the researcher to gain new knowledge and insights. Basic procedures involved in thematic analysis include skimming and scanning the data resources. Upon completion, an overview of the assets is obtained. Subsequently, terms which were either relevant to the research question or appeared frequently were labelled using a particular code. Once open coding procedure was finished, all the relevant and related codes were labelled using an abstract term called a theme. Once a set of themes were obtained, relationships or connections among them were determined to solve the research question. In order to efficiently execute data analysis, a commercial software tool was utilized. Upon conducting a thorough research, it was concluded that MAXQDA provides a rich user interface along with professional means of open coding. Specific tasks under thematic analysis included coding or labelling, creating categories, and finally forming themes.

IV. RESULTS

A. Overview

As determined by Dnstats [3], the two prominent marketplaces DarkBay and Blackpass were accessed. Additionally, the discussion forum Dread was also considered for investigation. The onion link was fetched from [3]. Upon accessing the page, a new account had to be created before gaining access to the internal marketplace.

For screenshots, see Appendix section

A pseudorandom word was used as a username with a very strong password.

Upon logging in, a wide range of products and services offered were visible. Since this research question addresses cyber threats, a filter was applied and limited to cyber related products and services eventually. The structures of marketplaces vary but not significantly. Every marketplace has a standard layout with products and services arranged in some form of a hierarchy.

Corresponding screen capture can be found in Appendix.

The predominant product offered was that of credit card details. Identity theft is one of the services that is quite mature and on-going. Various filtering options were also available to customize the results as desired.

Corresponding screen capture can be found in Appendix.

The minimum price starts at 2.1 USD and increases with the value of the information being sold. Transactions are executed by means of Bitcoin. Second category of identity theft is that of Social Security Number. The Social Security Numbers of US citizens were also being offered as a product.

Darkbay marketplace was more dynamic and vibrant as compared to Blackpass. All services and products being offered were organized in a fashion commonly seen at e-commerce web shops. As per latest access, 57695 products were available, 86165 customers were registered, and 608 vendors were offering their services and products. Every category had a sub-

category which basically lists individual products and services with its individual price, description, contact info and payment options. The major categories which relate to cyber threats included social engineering, fraud software and guides & tutorials. Each of the categories consisted of sub-categories which listed individual product and service types.

Dread as determined by [3] is one of the prominent discussion forums on darknet. Upon accessing the forum, numerous threads and topics of interest exist with multiple sub-threads. Since the question of interest is cyber threats, a filter was applied and resulting data sets were fetched for analysis.

B. Findings

Upon conducting thematic analysis on the raw data collected by means of netnographic data collection procedures, the following codes and corresponding themes were generated.

Individual Codes	Themes
Credentials for Sale	Identity Theft as a Service
Credit Card information for sale	
Comments for Sale	Social Engineering as a Service
Likes for Sale	
Authentication Compromise Service	Malware as a Service
Change configuration for Sale	
Software to hack bank card	
Software to hack and control Android	
Software to hack Wi-fi	
Software to drop exploits for sale	
Hack package for sale	
Keylogger for sale	
ATM hack software for sale	

Generic hack	Hacker for hire
Victim finder	
Doxing as a Service	
Harassment as a Service	
Skilled insider as a Service	

The codes formed in the above representation were relevant to the research question. Each code reflects the service being offered on the darknet marketplace or forum or both. The terms which occurred frequently or related to the research question were labelled using a code as suggested in the publication [9]. After enough codes were formed, some of these related and relevant code were grouped together to form a theme. A theme represents an abstract concept [9]. A theme consists of many codes and represents an umbrella term for all the products and services being offered on the darknet which can be considered as threats by entities concerned with information security.

V. DISCUSSION

The themes which have been generated intend to answer the defined research question. The theme “Identity Theft as a Service” concerns with the sale of personally identifiable information on the darknet. When investigating the above-mentioned marketplaces and forums, vendors were advertising their service which leads to the sale of assets such as credit card details, account numbers and various credentials of social media accounts. Depending on the value of the information being traded, the selling price also varied. The more balance the corresponding card held, the higher was the associated price tag. Credit card details being sold also had the options of filters. A client may apply various filtering parameters such as country of origin, minimum balance, verified, issuing bank name, issuing card name and maximum balance to filter out the desired results.

The theme indicated as “Social Engineering as a Service” also contributes to answer the define research question. Numerous vendors were advertising themselves for the purpose of executing social engineering attacks. As per the conducted investigation, social media was the most popular target for vendors. Potential adversaries may either direct message, like or comment as a legitimate connection but will later act maliciously. Discussion forum also provided the

members to seek a skilled insider who may act maliciously once he/she gets access to the internal resources.

“Malware-as-a-Service” is one of the significant themes identified during this study. Vendors were claiming to sell verified software packages for the purpose of executing malicious payloads. Various types of malwares were being offered either on darknet or some tips/guidance on the discussion forum. Most common included ATM hack malware, Keylogger to capture keystrokes, packages consisting of various exploits, exploits targeting SQL databases, wireless network malware, remote administration of android operating system and malware to hack a credit card. Every malware had a distinct set of features.

Last but not the least, “Hacker for Hire” was the one of the themes which could be generated out of the collected data. Vendors were offering their services as full-time hackers who claim to have abilities to successfully drop payloads depending on the offers. Black hat hackers posted advertisements about their offerings and some description of their tasks.

Confidentiality is difficult to measure since it is almost impossible to even detect. Hence, various counter measures should be utilized in order to ensure sustainability of confidentiality. Typical controls may include encryption and strict access control mechanisms. On the discussion forum, users were found to have sought for individuals who are expert at doxing.

After having conducted this research, social engineering assignments and tasks are certainly also on the rise. Vendors are mostly offering services that target popular social media platforms such as Instagram. Fake comments and likes might be able to deceive a legitimate account user and may fall into the trap crafted by the social engineer. Possible countermeasures maybe applicable in this case could be user awareness and training.

The second most popular service being offered is that of malicious software or commonly referred to as malware. Vendors have been offering various kinds of toolkits, software packages and exploits which claim to have the ability to accomplish malicious intentions. The feature set provided by every vendor is distinct. On the discussion forum, the users were mostly found to have shared pieces of source code or tutorial on crafting a custom exploit.

Finally, the generic term “Hacker” was both being offered as a service and also being sought. Various roles and tasks were being demanded. On the marketplace, hacker as a service was being offered with various packages and price offers. They claimed to have successfully accomplished tasks in the past and let their results speak. On the discussion forum, community members either sought a hacker for personal reasons such as harassment, rivalry, revenge or even for a cause such as “Black Lives Matter”. Discussion forum such as Dread consists of multiple postings about the advertisements seeking competent hacker for personal gains. Once the potential freelancers receive clarity on the exact job descriptions, they usually communicate privately. The exact details of their implementation could not be revealed as the members usually communicate privately.

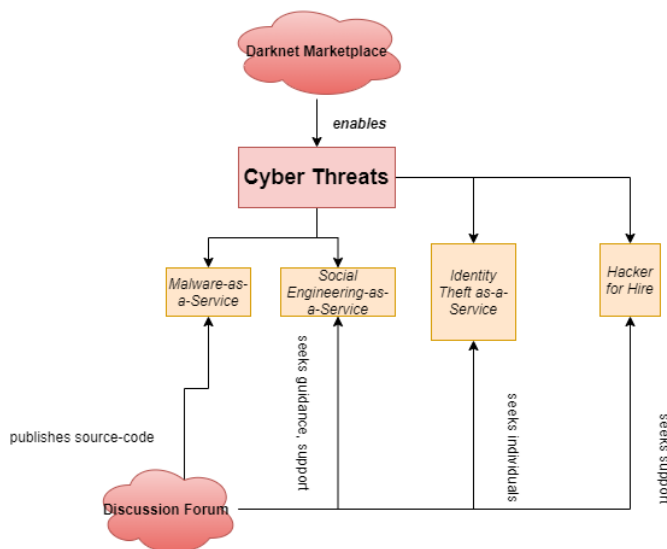


Figure 1: Relationship among themes

The darknet marketplaces and forum studied as part of this study revealed interesting insights about the cyber threats which originate from such platforms. The most dominant threats determined to have their presence on the dark platforms seem to have increasing their maturity at all instants. The most common threat is that of identity theft. Cyber criminals might have less cost of acquiring the sensitive information and compromising confidentiality. All major banks and credit card companies have been targeted. However, their authenticity is difficult to verify. It is therefore, very important to secure the sensitive information an entity

VI. COMPARATIVE ANALYSIS

A brief comparative analysis of this study with previously conducted works can reveal critical characteristics which may enable to distinguish this study distinctly. This study provides an overview of cyber threats which are likely to arise from the darknet platforms. Limited scope is one of the advantages of this approach. Hence, the threats which only address cyber

and information assets are presented in the results of this study. Upon assessing the results published by this study, an entity can measure its risks and treat them accordingly since all objectives of cyber security are most likely under threat. Services are either being sold to compromise the objectives of security or products are being sold after the threat has finished being realized. However, cons such as absence of specific details such as business ethics, deals, structure and conditions of service level agreement are missing from this study. The work published by [5] illustrates the overall situation of the economy within darknet marketplace. The products covered in the scope in the work of [5] are mostly physical in nature and therefore has a lot of implications on the delivery and supply chain. The study conducted in [2] takes the opportunity to explore the darknet marketplace in general. Their results and analysis claim that illicit street vendors are offering drugs on the darknet and executing transactions by means of bitcoins [2]. Drug being a physical item of interest is not a threat to cyber space. Additionally, threats addressing cyberspace have not been explored in work published in [2]. The results obtained after this study may enable an entity to visualize the current threat scenario which exists. The threat sources as well as threat events can also be known and be aware of. Therefore, suitable countermeasures and controls can be deployed to block the potential harm by these cyber threats.

VII. FUTURE RESEARCH

This research primarily focused on cyber threats which originate from dark avenues such as the marketplace and discussion forum. The accuracy of this study can certainly be increased by devoting more resources such as time and manpower to elicit more information about the products and services being offered across all the marketplaces and discussion forums. Further research might be conducted on determining an overview of how an agreement between a vendor and a client is established and the structure of the service level agreement if it even exists. However, extreme care and caution must be taken to engage in conversations with a potential cybercriminal. It is highly likely that the vendor might be a law enforcement personnel posing a vendor. Extra precaution must be taken when dealing with vendors on darknet, especially with respect to research ethics and applicable laws.

VIII. CONCLUSION

It is now evident that darknet is no longer popular just for physical items and services as determined by previous works of research. All forms of electronic and semi-electronic services and products are now being offered on sale as a service. The implications of the service and products vary significantly depending upon the nature of those items. Physical items such as drugs will need to be very cautiously delivered to a client while electronic product and services such as cyber threats can be delivered anonymously. The likely hood of being caught and detected is lower in this case, Those services and products which are offered give rise to major cyber threats which can certainly compromise the confidentiality, integrity and availability of cyber resources. Entities which are concerned about the secure state and operations of their business should be aware of the range of services and products being offered on the darknet. The themes and the relationships among the themes enabled the researcher to answer the research question. The complex question defined earlier also has a complex solution. The economy of cyber threats is mature to a certain extent but varies as per the type of threat being offered. Vendors offers products and services with claims of authenticity and accurate results. Clients on the forum either seek support, tips or individuals offering their desired services. The range of products and services being offered is also quite extensive. Almost every objective of cyber security is under threat of being compromised in the face of these cyber threats which originate from the darknet. The Dread forum is an active discussion forum with numerous threads and sub-threads. Discussions on almost every topic of interest can be discovered and followed upon. A filter can also be applied to narrow down the search results for better accuracy. The darknet marketplaces- Blackpass and Darkbay differ in terms of their offerings. Blackpass is popular for the sale of identity theft and corresponding assets. Filter can be applied to narrow the results based on multiple parameters. Darkbay on the other hand is very vibrant and exhaustive. A wide range of threats are being offered as products and services by numerous vendors.

IX. REFERENCES

- [1] M. Perry, E. Clark, S. Murdoch and G. Koppen, "The Design and Implementation of the Tor Browser [DRAFT]," 15 June 2018. [Online]. Available: <https://2019.www.torproject.org/projects/torbrowser/design/>. [Accessed 30 April 2020].
- [2] V. Adewopo, B. Gonen, S. Varlioglu and M. Ozer, "Plunge into the Underworld: A Survey on Emergence of Darknet," in *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, 2019.
- [3] "Featured Sites," DNStats, [Online]. Available: <https://dnstats.net/>. [Accessed 30 April 2020].
- [4] P. H. Meland, Y. F. F. Bayoumy and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," *Computers & Security*, vol. 92, no. 101762, 2020.
- [5] F. Hellström, T. Olsson and R. Wennerstrand, "A Darknet Market Rises: An Exploratory Single Case Study of the Empire Market," Stockholm, 2019.
- [6] R. Kozinets, "The Method of Netnography," in *SAGE Internet Research Methods*, London, SAGE Publications Ltd, 2012, pp. 101-118.
- [7] R. R. V. Kozinets, "Netnography for Management and Business Research," in *The SAGE Handbook of Qualitative Business and Management Research Methods: Methods and Challenges*, London, SAGE Publications Ltd, 2018, pp. 384-397.
- [8] R. V. Kozinets, D. Pierre-Yann and E. Amanda, "Netnographic Analysis : Understanding Culture through Social Media Data," in *Sage Handbook of Qualitative Data Analysis*, London, Sage, 2014, pp. 262-275.
- [9] B. Lewis, M. S. Bryman and L. T. Futing, *The sage encyclopedia of social science research methods*, Thousand Oaks, California: Sage Publications, 2004.

APPENDIX

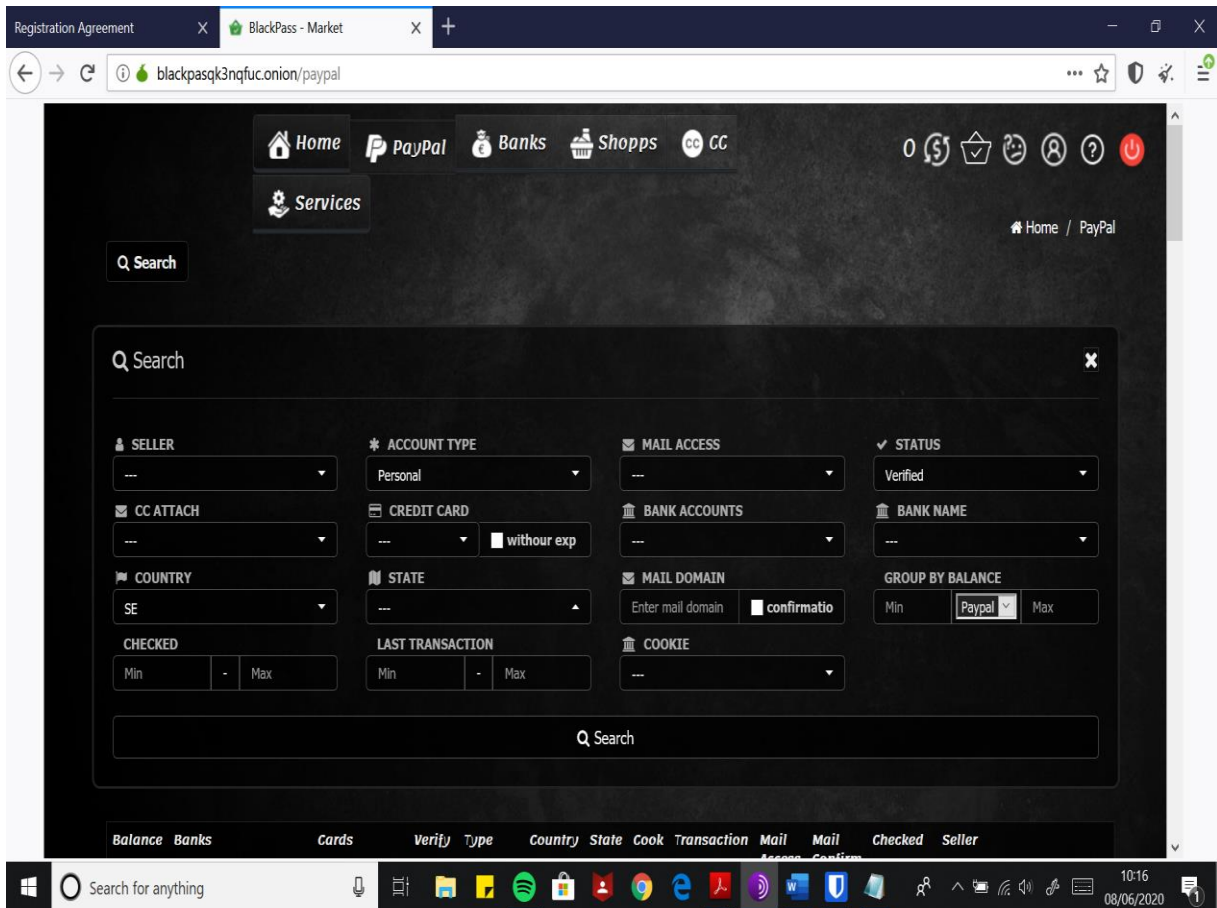


Figure 2: Filters for Identity Theft

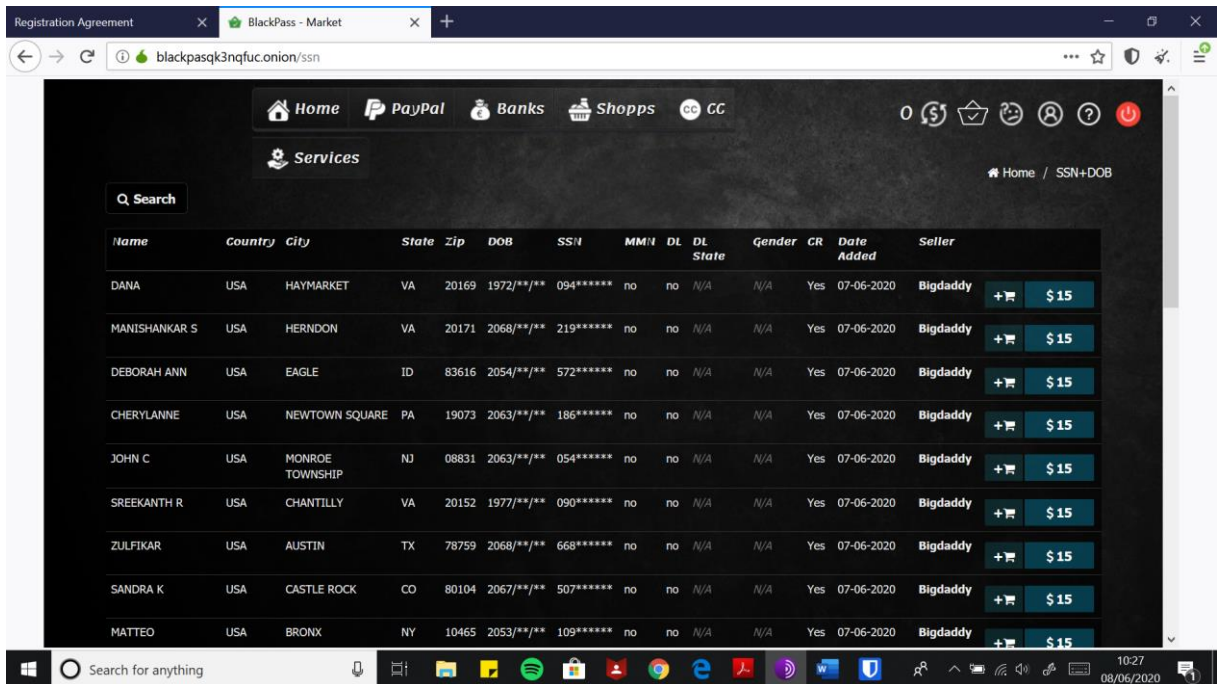


Figure 3: Social Security Number for Sale

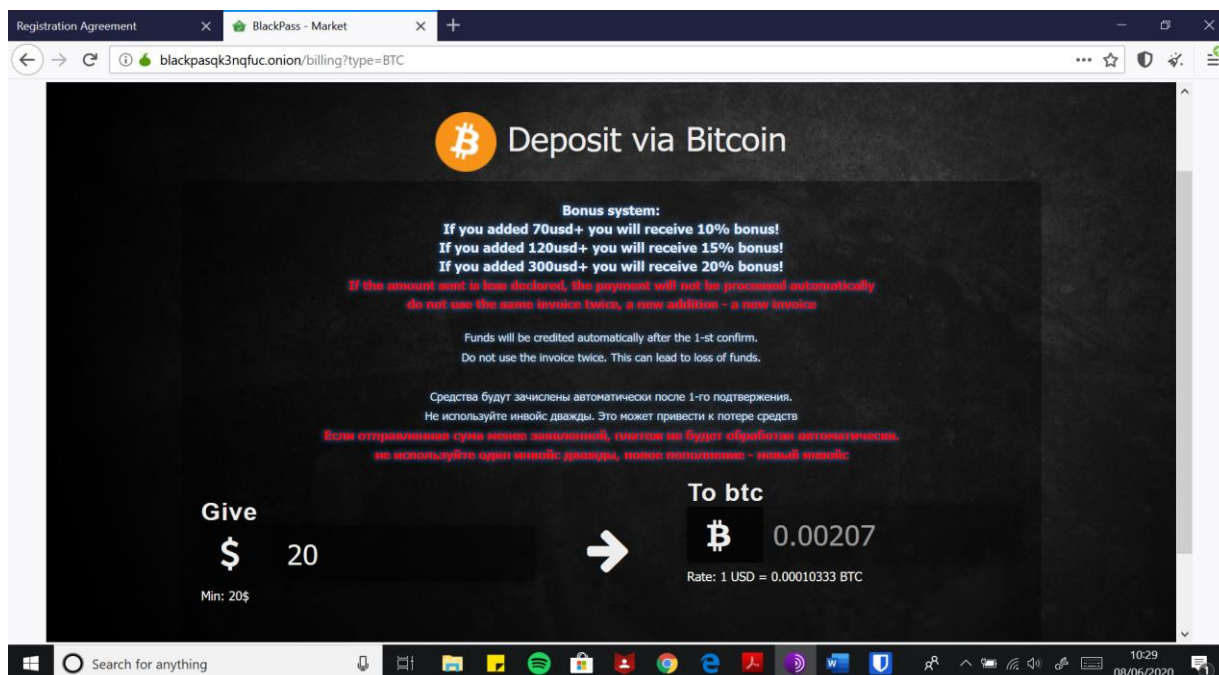


Figure 4: BlackPass Wallet

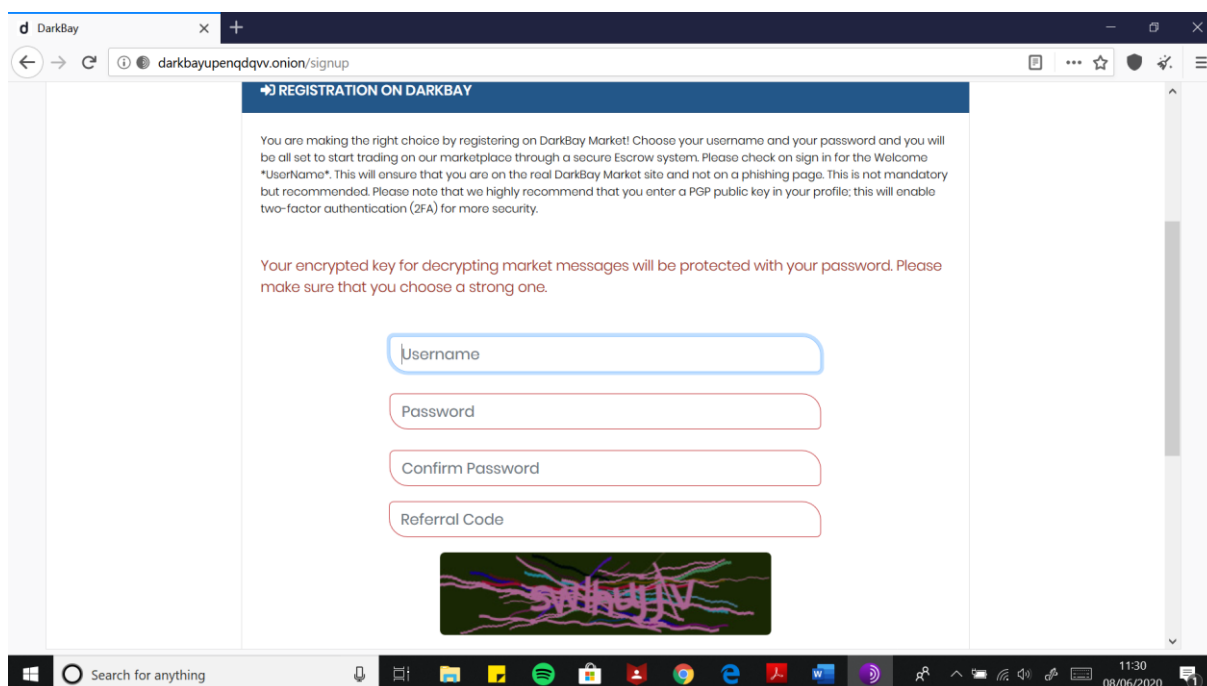


Figure 5: DarkBay Marketplace Registration

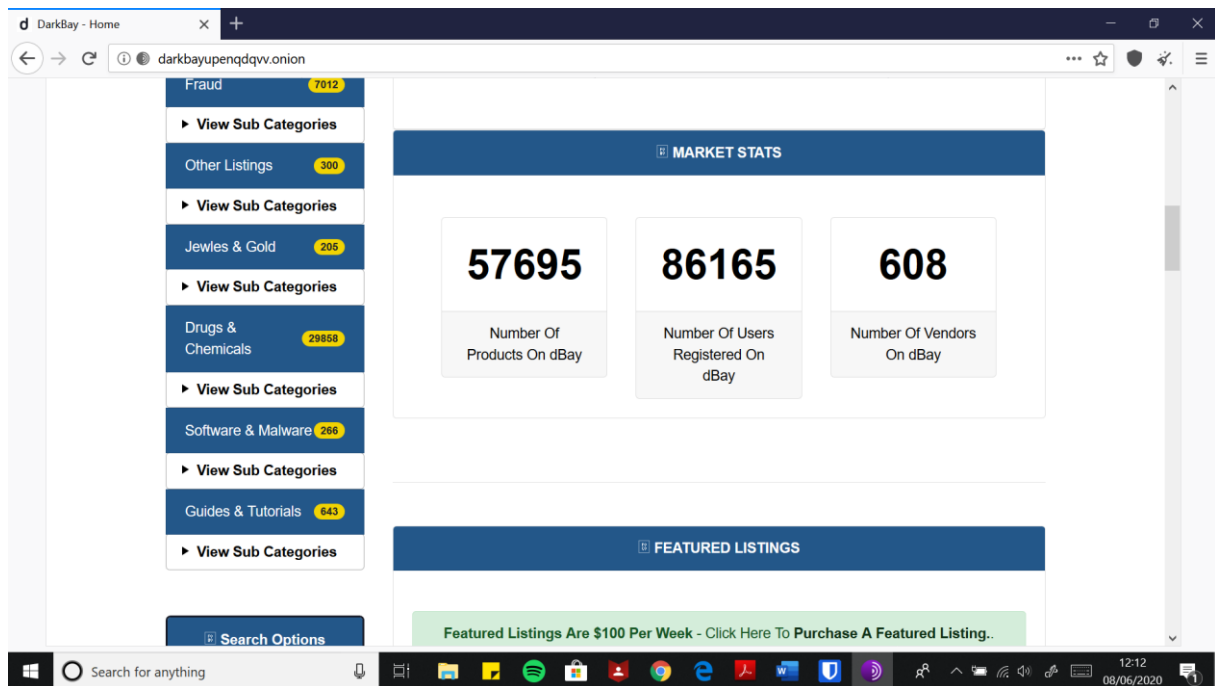


Figure 6: Overview of Products & Services in DarkBay Marketplace

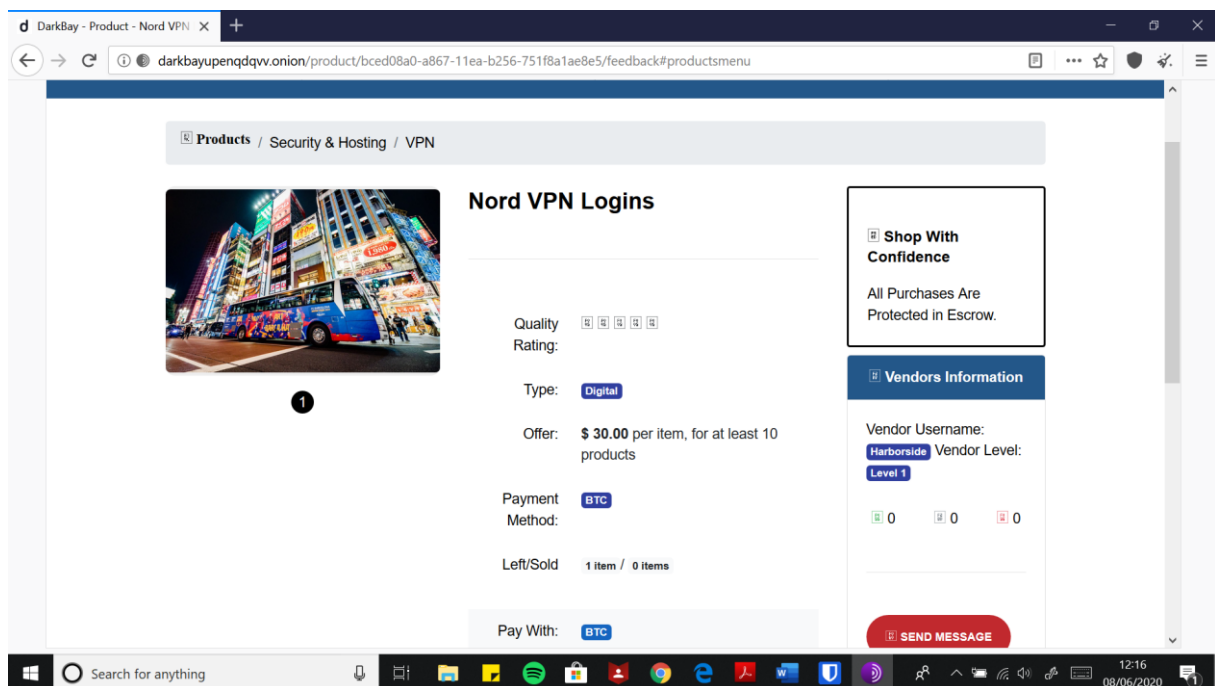


Figure 7: VPN credentials for Sale

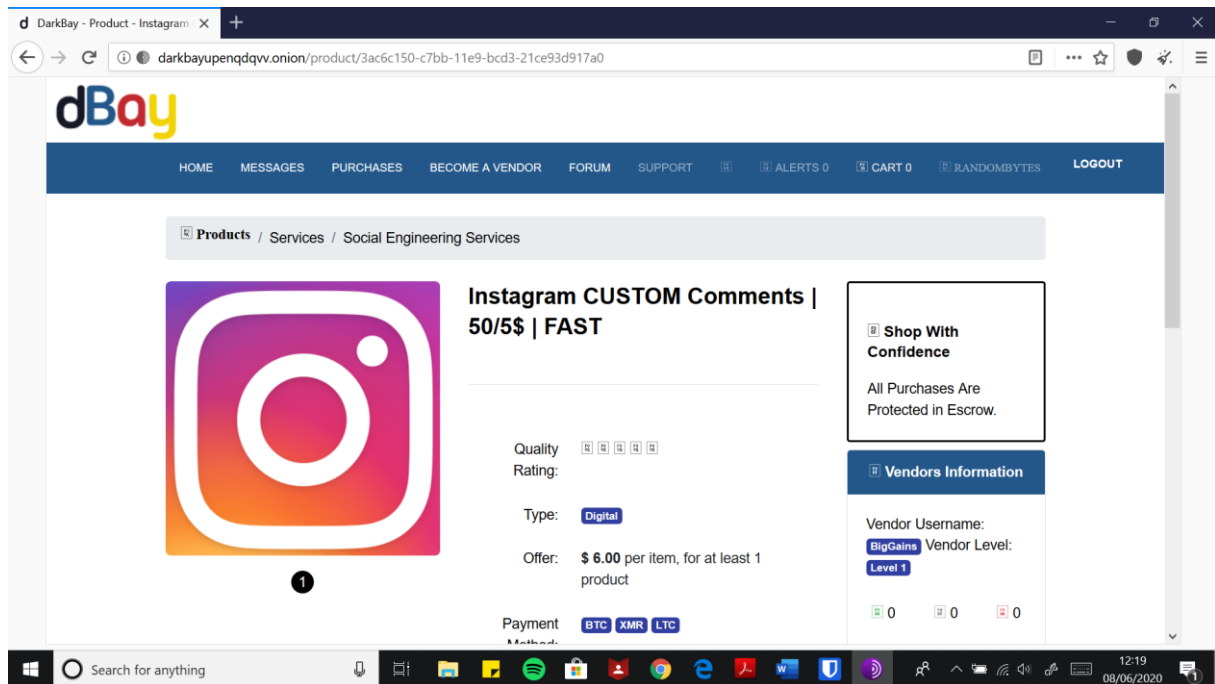


Figure 8: Social Engineering Service for Sale

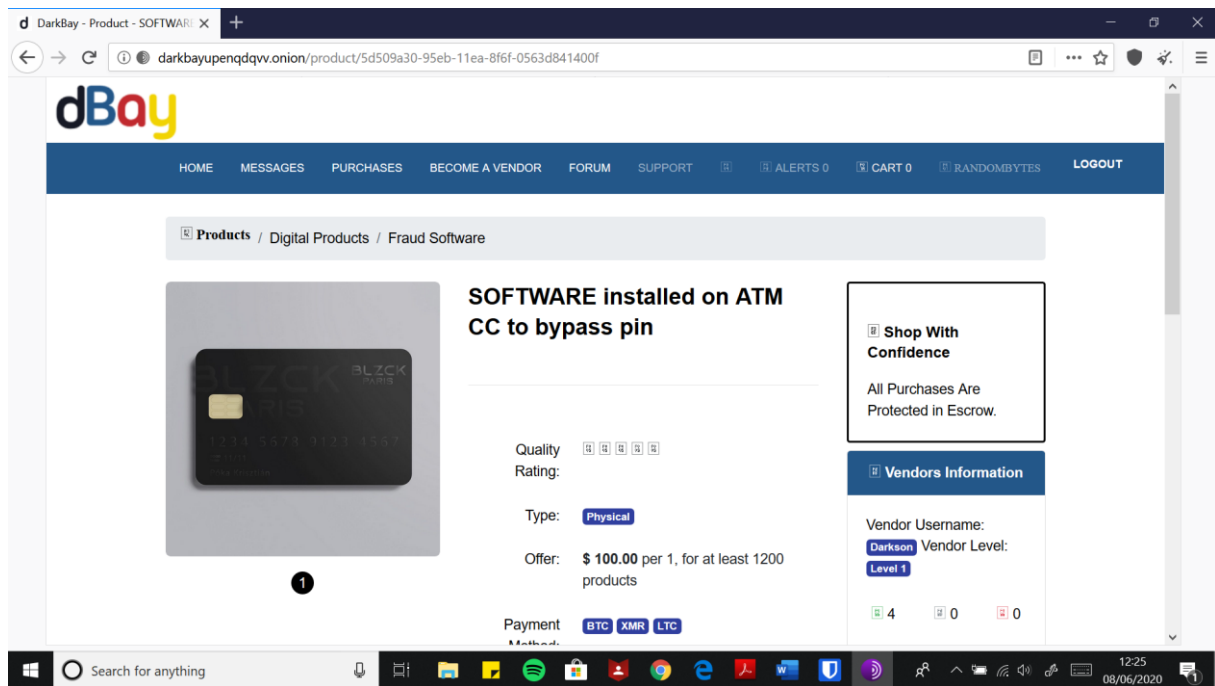


Figure 9: ATM Authentication bypass malware for sale


DarkBay - Product - ANTIDETE

darkbayupenqdv.onion/product/885c99e0-e14e-11e9-8765-e78123c5943a

dBay

HOME MESSAGES PURCHASES BECOME A VENDOR FORUM SUPPORT ALERTS 0 CART 0 RANDOMBYTES LOGOUT

Products / Digital Products / Fraud Software



ANTIDETE FF BROWSER FOR Carding, Paypal, Bank Accounts

Quality Rating: [5 stars]

Type: Digital

Offer: \$ 3.00 per item, for at least 1 product

Shop With Confidence
All Purchases Are Protected in Escrow.

Vendors Information

Vendor Username: **tvman** Vendor Level: **Level 1**

0 0 0

Search for anything

12:28 08/06/2020

Figure 10: Anti-detect malware for Sale


DarkBay - Product - HACKER

darkbayupenqdv.onion/product/517391c0-7379-11ea-a213-73af541ec81c

dBay

HOME MESSAGES PURCHASES BECOME A VENDOR FORUM SUPPORT ALERTS 0 CART 0 RANDOMBYTES LOGOUT

Products / Digital Products / Other Digital Products



HACKER FOR HIRE SERVICES

Quality Rating: [5 stars]

Type: Digital

Offer: \$ 12.00 per Hacks, for at least 1 product

Payment Method: BTC

Shop With Confidence
All Purchases Are Protected in Escrow.

Vendors Information

Vendor Username: **sire25** Vendor Level: **Level 1**

0 0 0

Search for anything

12:33 08/06/2020

Figure 11: Hacker as a Service

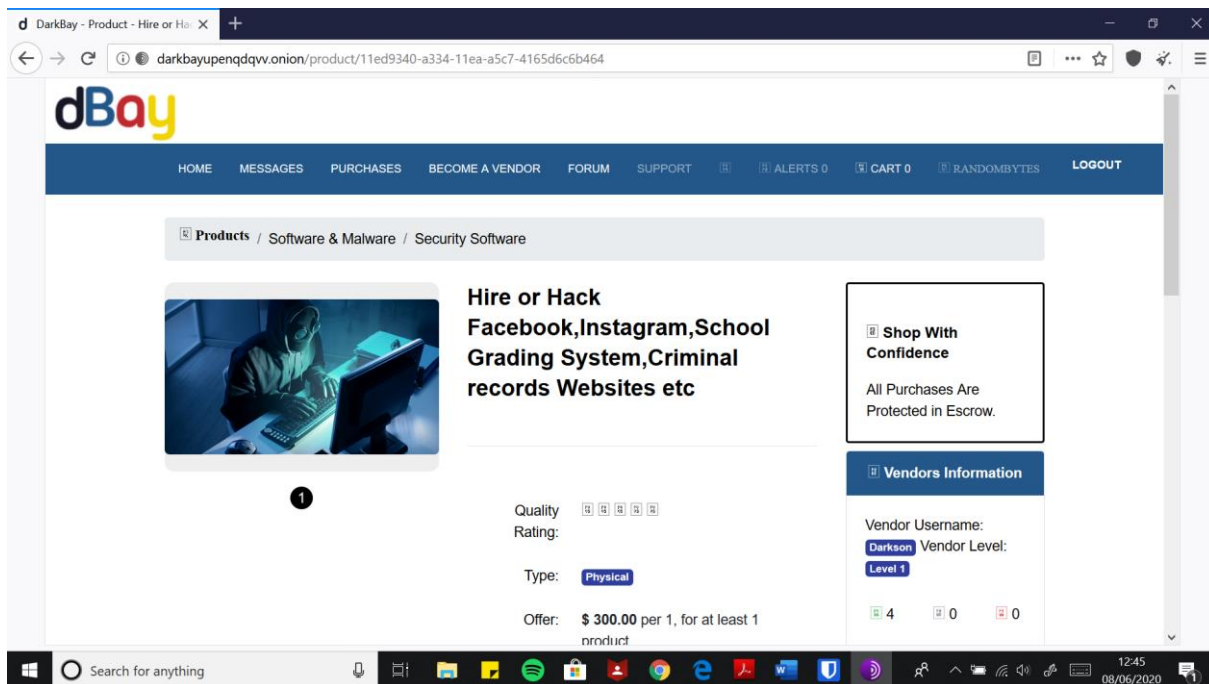


Figure 12: Hack as a Service

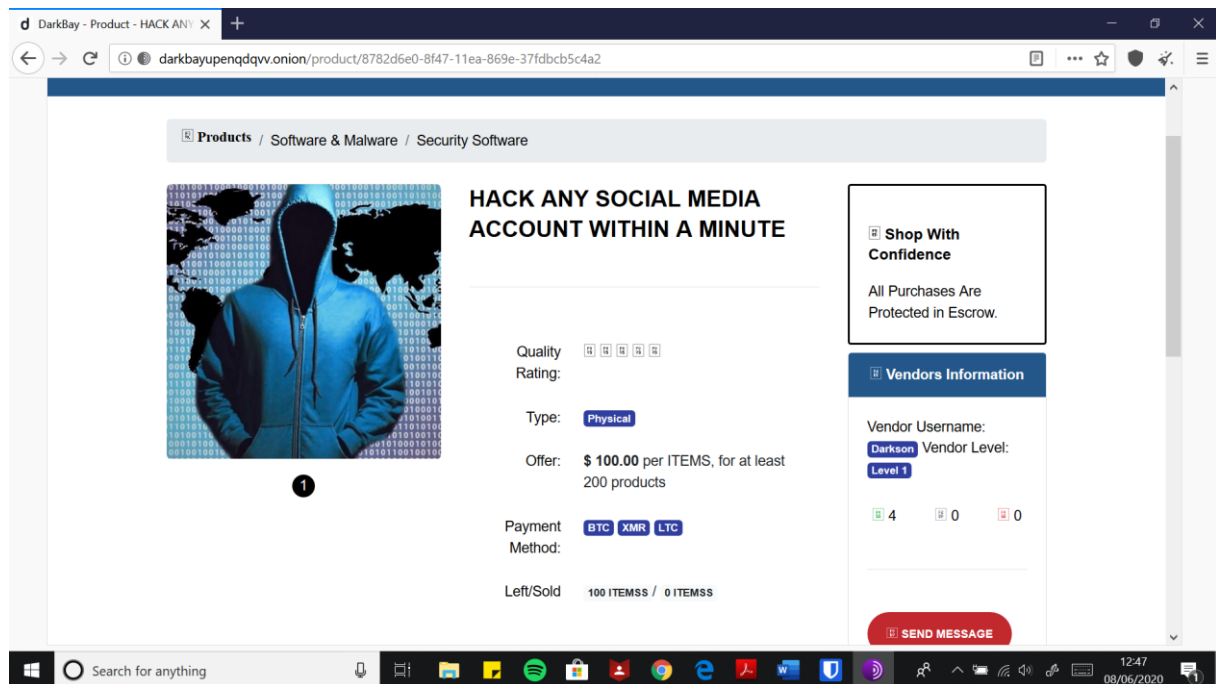


Figure 13: Social Media hack as a Service

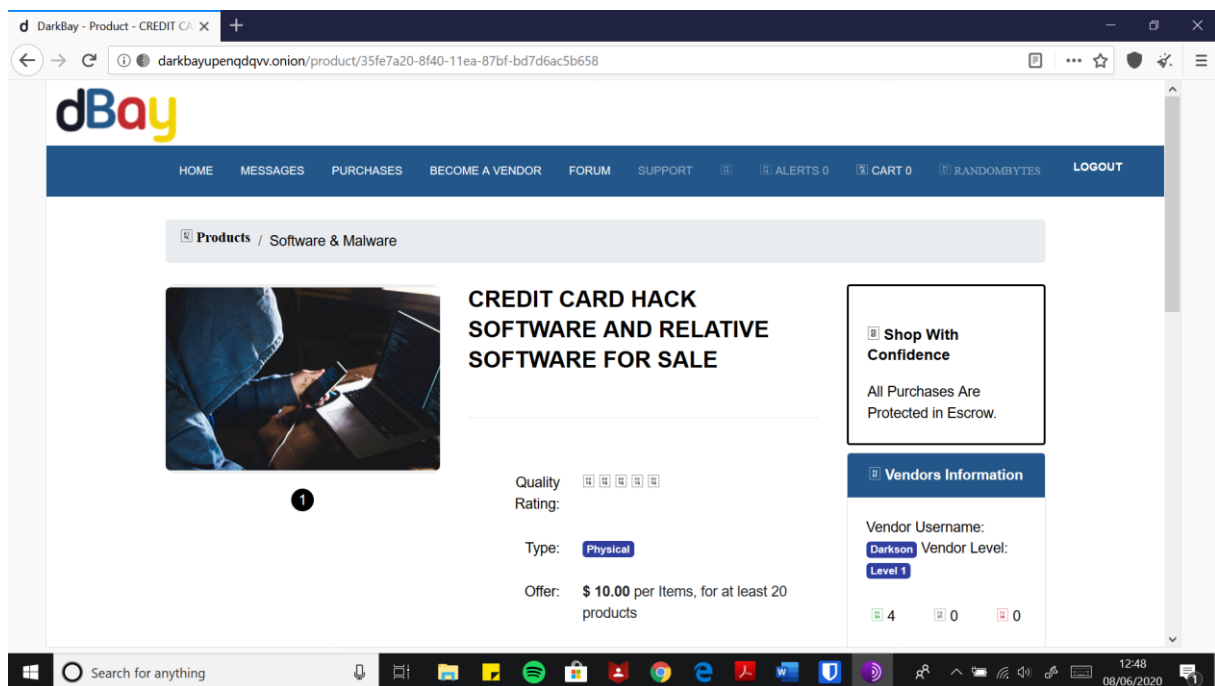


Figure 14: Credit Card Hack malware

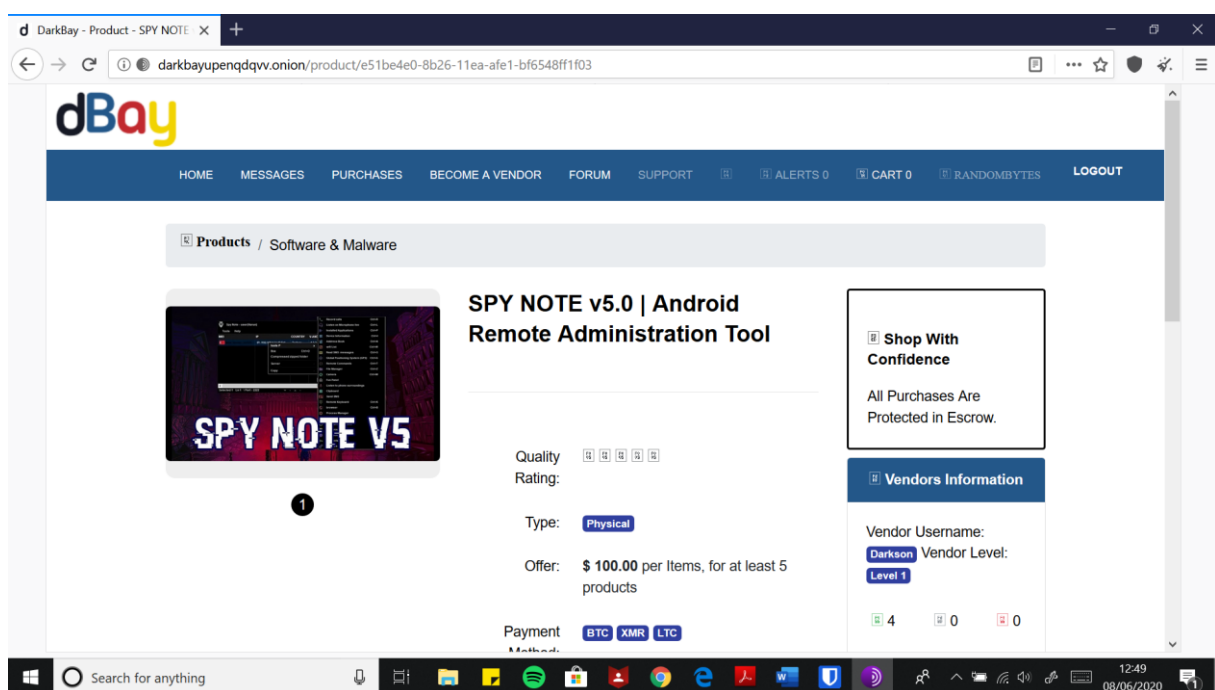


Figure 15: Android Remote administration tool



Figure 16: Wi-fi hack malware

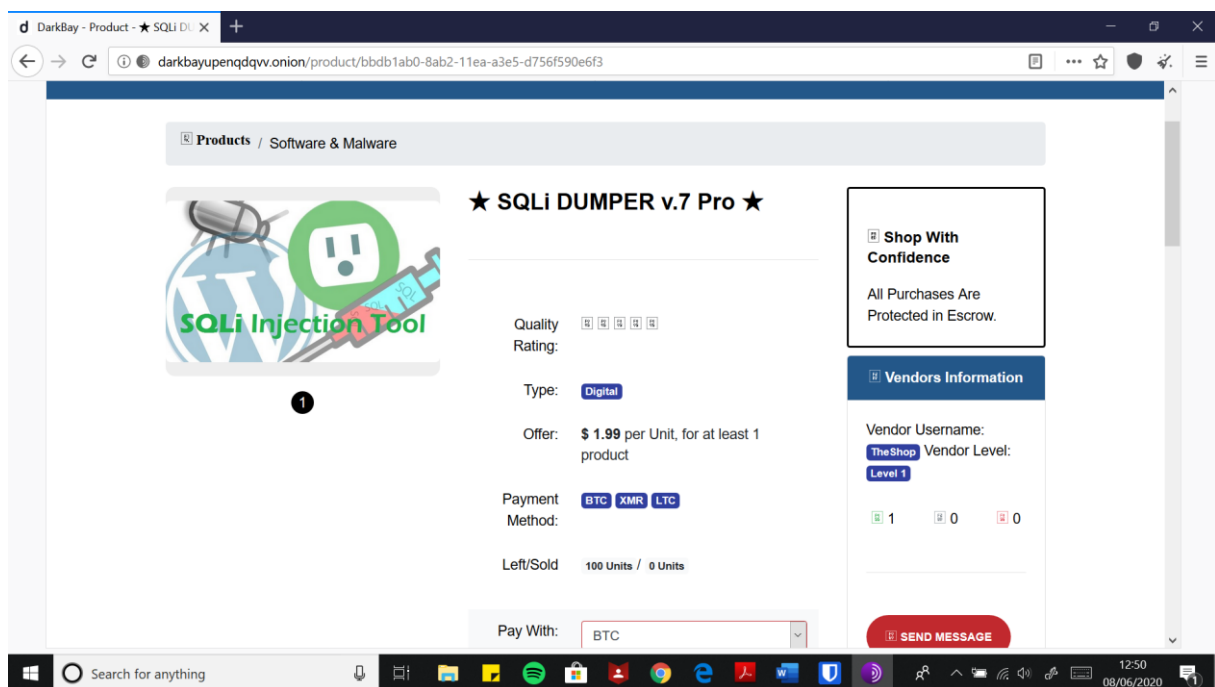


Figure 17: Web Security Toolkit

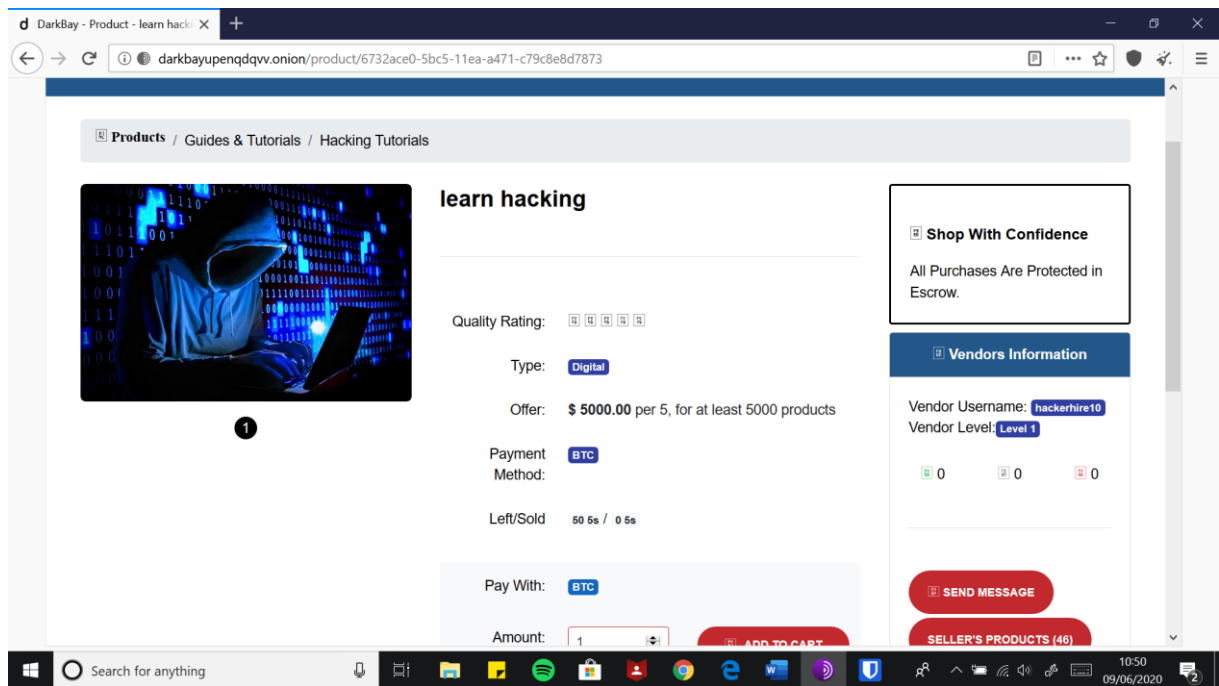


Figure 18: Tutorial for Hacking

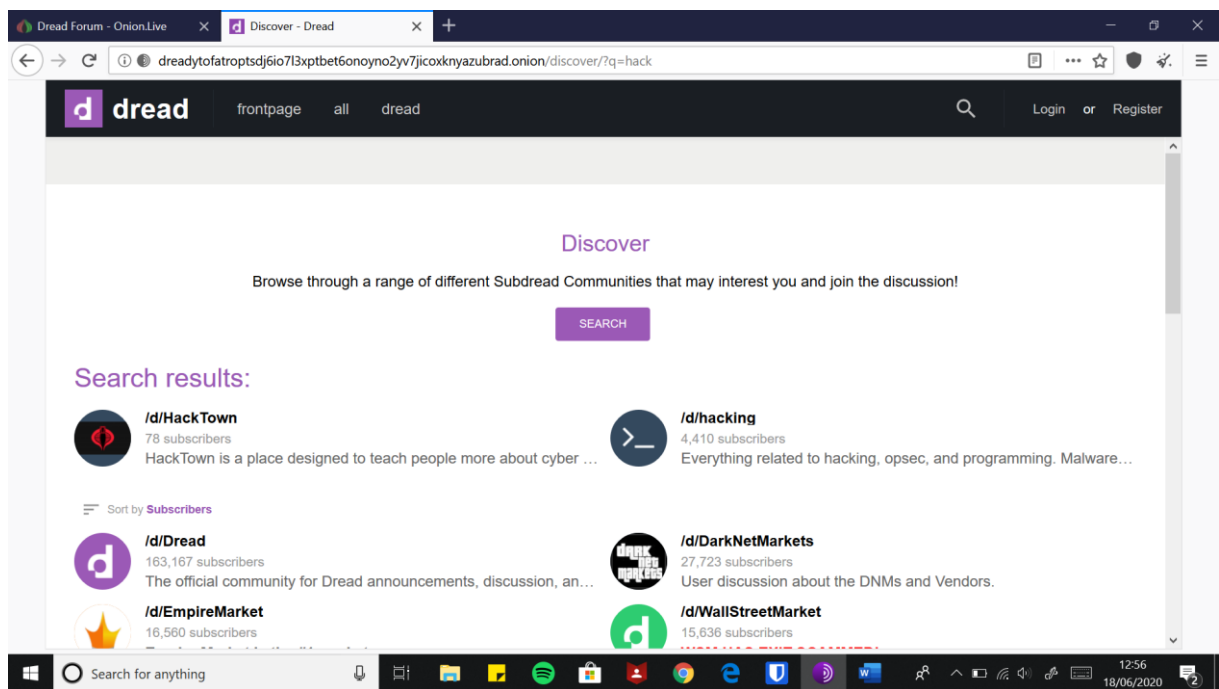


Figure 19: Dread Discussion Forum

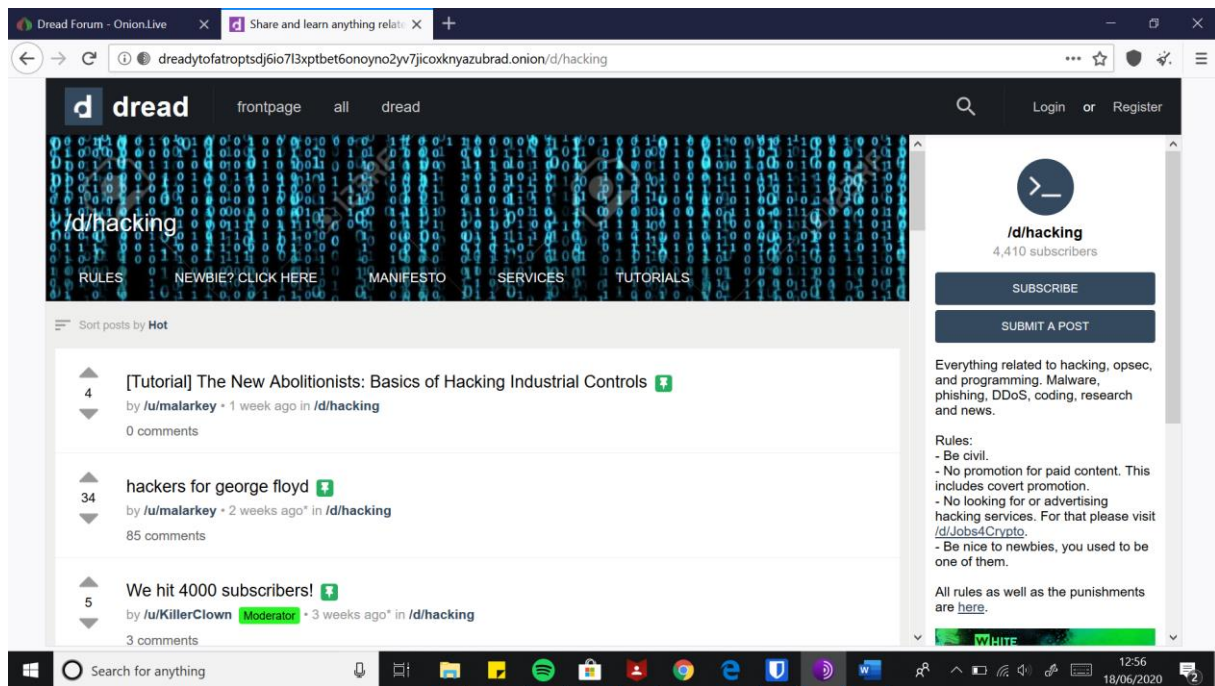


Figure 20: Thread