ORIGINAL RESEARCH PAPER

Technology

THE ROLE OF THE DARK WEB IN FINANCIAL CRIMES

KEY WORDS:

Akshit Singh Designation- BBA.LLB Student at Amity University, Lucknow Campus

ABSTRACT

Literature Review The dark web is a characteristic of a particular overlay distributed system that exists on top of the worldwide internet and offers the functionality of remaining untraceable while also promising to be a haven from prying eyes, mostly law enforcement. New strategies to extend the existence and viability of the dark web have been made possible by technological advancements. **Methodology:** In this research paper the data for the present study is collected mainly through secondary sources the objectivity of historical and current writings has been used to develop a frame work of the study and to arrive at an unbiased conclusion. The data collected with a view to identify and analysis the constant rise of cybercrime in India.

Introduction

These days people use internet in everyday life but that's surface web. The internet has two building blocks namely: "Surface Web" and "Deep Web". We already have idea of websites like Amazon, Wikipedia, Facebook, YouTube, etc these sites come under the surface web that can be indexed by search engines like Google, Bing, Yahoo, etc. Surface web is well-known as "Visible Web". But surface web is not all about the internet. The surface web is the compact section of the internet and it covers 4% of the internet which can be accessed by the general public. There are some sites which are hidden and not available to the general public that is 96% of internet. This un-common space is where the Deep Web exists. Validation is compulsory to access the data like net-banking or private accounts. Websites on the deep web provides confidentiality to the users. If these websites are indexed then anyone can access data by searching your name and the personal information will be revealed to the people. That's why validation secured pages are unindexed so that confidentiality stays maintained. Dark web basically is a small fraction of the Deep web. Dark Web is also a "Invisible Web". Dark web cannot be accessed by the general public unless they have good knowledge about what they are doing and what software they have to use to surf the dark web. To use the dark web special software, authorization, configurations, etc are required to access. It provides confidentiality and are not indexed by the search engines. Dark Web can only be accessed by special anonymous software installed in browsers namely: TOR (The Onion Router), Subgraph, Waterfox, I2P (Invisible Internet Project), etc. Using TOR is the easiest way to browse the dark web. Dark web can be accessed through the Tor browser which was created by the U.S. Naval Research Lab, 1995. It may be used for legal as well as illegal activities. Data is encrypted like the layers in an onion in TOR. Encryption in TOR keeps the privacy of the users safe. Due to the high degree of anonymity and inability to trace the person's IP address, criminals take advantage to conduct and promote their illegal activities such as drug trafficking, dealing in guns, firearms, buying drugs, credit cards etc. While some people use the dark web for legitimate reasons also such as people who wish to protect their data from government monitoring may need to cover up the dark nets. Whistleblowers. They may want to share huge volumes of insider knowledge with journalists, but they don't want a paper trail. Dissidents in oppressive regimes that require anonymity in order to keep the world aware of what is happening in their region. Approximately 45,000 Dark web sites are available which is only 0.01% of the Internet.

- Types of financial crimes happen on the dark web.
- Criminals here use the dark web to buy & sell payment cards data as well as full identity packs for identity theft. Selling of "cybercrime as a service" which can include the tools to commit cybercrimes or hacker services are also common here. Though, all the transactions here are done in crypto currencies such as bitcoin, Ethereum etc.

Major Financial Crimes or most popular financial crimes fall under the following categories:

1. Phishing is one of the most common attacks because it is incredibly effective and relatively easy to perform. Criminals use fraudulent communication, such as fake emails, SMS, phone calls, or websites to steal private information which is then sold or used to access further company data.

2. Malware. It is the software designed to damage or compromise networks or devices such as computers, tablets, or mobile phones. The gleaned data is often used to infect other devices and access personal information, financial accounts and can cause loss to the victim.

3. Identity theft is the taking of personal information that is then utilised to pass for the victim. Virtual identity theft enables thieves to construct fictitious internet profiles and accounts by using information such as names, addresses, birthdays, Social Security Numbers, and more, as opposed to physically stealing Ids.

4. Money laundering. It happens online because the Dark Web enables the transfer of illegal payments to and from several anonymous accounts, assisting thieves in securing unjustified riches.

5. Carding is an alternative method of money laundering that entails using stolen credit cards to make unauthorised purchases of real or fake goods. Today thieves may easily carry out these attacks using digital numbers, and they can purchase this card information from other hackers who have obtained the data from infected networks.

6. Counterfeit Documents: Bank statements, checks, false credit cards, and counterfeit money are just a few examples of the fraudulent and counterfeit documents that are available in dark web marketplaces. The majority of the time, these records can be printed out and then utilised to fraudulently legitimise actions that are supported by bank statements.

7. A lot of these attacks are often used with one another, making them highly complex schemes that are difficult to detect.

- Statistics on the usage of the dark web in India.
- In comparison to Australia and South America, India has the largest market for dark web users.
- According to ZDNet, the ShinyHunters hacking collective attempted to sell 73 million users' data on the dark web. Over ten organizations had their security compromised, including the South Korean fashion portal Social Share, printing provider Chatbooks, and online dating app Zoosk.

- Over 500,000 zoom accounts were compromised in April 2020 and sold for less than one rupee each, claims cybersecurity company Cyble.
- Arxiv discovered that the majority of users of the dark web—70.6% of them—were men, compared to just 29.4% of women.
- According to the Arxiv, if we look at the data by category, we may summarise them as shown in the table below.

Category Group	Percentage of users using the dark web
18-25	35.9%
26-35	34.8%
36-45	16.8%
46-55	8.8%
56-65	3.1%
Above 65's	0.6%

While the dark web is certainly not that bad to surf on, there is still danger, and it isn't a safe place. Some sites are also legitimate, and users can reap benefit from them. If thieves only stole credit cards to use for personal purchases, financial crimes wouldn't be as serious. The issue is that these crimes frequently have a significant negative impact on the online economy. For instance, one business decided to employ financial criminals to obtain any information about their rivals. This isn't the market's natural mentality, and it's unpredictable. As a result, many people may lose their jobs if their business is suddenly shut down. To prevent this, people should spread awareness about this situation. Many thefts can be stopped even with a simple line of defence.

Autoshop Marketplaces

One of the most prevalent financial crimes on the deep web and dark web is selling the personal financial accounts, with some estimates putting the number of credit cards for sale on dark web to millions.

There is specific name for these marketplaces that specialize in selling of credit cards, debit cards or bank account information, as well as credentials, cookies and remote access needed to take over online accounts. The place is known as "autoshops" which refers to the transaction process being more automated and faster than any other dark web markets. Autoshops offer totally digital products for sale, which allows for quick delivery of the purchased item to the customer with little to no vendor involvement. This automation also give insight to how sophisticated the sale of financial information has become now. The top autoshops (which currently are the likes of Blackpass, 2easy, Russian Market) they regularly post 10,000s of new listings per week which demonstrates how big this problem is. Autoshops are structured and run differently from other dark web marketplaces. Dark web markets are typically run by administrators that charge a fee in exchange for letting numerous independent sellers sell their goods there (known as an escrow marketplace). Autoshops, in comparison, often have a lot fewer sellers, and occasionally all of the listings come from the site operator alone. Moreover, autoshops are more likely than other markets to have a "clear web" presence, either in place of or in addition to their dark web website.

Source Of Stolen Financial Data

Autoshops obtain the financial goods they illegally market from a variety of sources.

Historic data breach sets: On the dark web, there are numerous databases containing financial institution card details for sale, although they are sometimes treated with suspicion in criminal forums because they are sometimes old and contain few "active" credit cards for hackers to use.

Attacks against e-commerce sites: Web skimming is a method used by cybercriminals to acquire credit card information from customers' accounts on websites. Automated software, famously utilised in the Magecart hacks on British Airways, Ticketmaster, and Newegg, enables attackers to steal payment information from thousands of clients if they remain undiscovered.

Phishing sites: clients are misled into providing their credit card information on a fraudulent website, which frequently resembles a reputable and well-known brand. On the dark web, spammers can purchase phishing websites, reverse proxy servers (like Modlishka and Evilginx), and spamming tools to get around two-factor authentication used by banks.

Banking trojans and stealer malware: Malware that is loaded straight onto a user's computer to collect card info. In markets and forums, banking trojans and theft malware can be purchased together with user manuals that explain how to use them. Zeus, Emotet, and Trickbot are notable examples.

Insider threat: Financial institution staff members sell customer information.

How To Avoid Becoming A Victim Of A Financial Crime On The Dark Web?

Financial services organisations can take steps with the help of dark web intelligence to combat this planned targeting of their clients.

For instance, a bank may discover all of its credit card information exposed on autoshops, pastebins, and forums by searching the dark web for its Bank Identification Numbers (BIN), the portion of the card number that identifies which bank a card belongs to. After the bank has recognised the stolen card information, it can block the cards, alert clients to any unusual account activity, and alert the police to the operation of the autoshop, preventing fraud on a large scale. To determine when and how their customer base is being targeted, financial institutions could potentially detect products sold on dark web markets, such as banking trojans or 2FA bypass tools. With this information, they could then put protective safeguards in place for their clients' accounts, preventing the collection of their financial information altogether.

You can prevent falling victim to a financial crime on the dark web by following a few basic procedures, including:

1. Carefully Review Company Policies: In their policies, the majority of businesses specify exactly how they will get in touch with you. For example, the great majority of banks will expressly specify that they would never send you an email with a link to their website.

This implies that you will be aware of any attempted phishing scam if you do receive an email with a link or attachment and you are aware that it is against the company's policy.

2. Install Up To Date Antivirus Software

You should make sure that antivirus software is installed on all of your devices to prevent falling victim to malware or ransomware attacks. This can identify and eliminate any incoming threats before they have a chance to affect your financial information.

3. Report A Potential Scam

When someone tries to trick you with a phishing scam, it typically means that they have gained access to at least part of your personal information, most notably your contact information. If nothing is done, there is a potential that the situation will worsen.

Inform the business that the thieves are claiming to represent of these problems. You can bring up the matter with the

Information Commissioner's Office if you don't believe the appropriate action is being taken.

4. The Internet Is A Scary Place…

You can see that there are certain defences against financial crime, but they aren't always sufficient. The best course of action is to closely monitor your bank account and credit report and to immediately report any unusual activity. It's crucial to be cautious since the dark web is a never-ending tunnel of criminal activity.

What happens to stolen data on the dark web?

On the dark web, stolen data is sold and resold numerous times during the course of its existence. It usually serves criminals the best at the beginning of its lifecycle, which is also the most difficult and expensive time to acquire. The cost of the data decreases as it is more readily accessible, but the value to criminals decreases as well.

For instance, if someone's Social Security number is stolen, it is worth more before the victim realises it was taken, and it loses value over time if the victim places holds on their credit bureau reports or takes other steps to protect their identity.

The stolen data may initially be sold or traded amongst colleagues. Then it might be listed for sale on a forum with very severe membership requirements, then on a forum with a less strict membership requirement, and finally on a forum that is available to everyone. Ultimately, the information may be freely shared on a paste-bin website, which is only a website where users may readily share text.

Conclusion

Dark Web networks such as TOR have created a wide variety of ways for criminal individuals to trade legitimate and illicit "goods" anonymously. Dark Web is a growing commodity, especially in the field of illegal resources and activities. Protection processes should be proactive in resolving these problems and taking steps to remove them. This paper explores the financial crimes happening in dark web and precautions to be taken care while surfing dark web.

Acknowledgement

First and foremost, I am grateful to the children and families who participated in this study, generously sharing their experiences and insights. I would like to thank my research supervisor for his guidance and support throughout the project, providing valuable feedback and suggestions that greatly improved the quality of the research.

I would also like to thank the faculty and staff of the department of law for their support and encouragement, as well as the resources they provided.

I would like to acknowledge the contribution of my colleagues who assisted with data collection, transcription and analysis, without whom this research would not have been possible.

Finally, I would like to thank my family and friends as their unwavering support helped me to stay focused and motivated to complete this research paper.

REFERENCES:

1. https://fraudwatch.com/the-evolution-of-financial-crime-in-the-dark-web/
2. https://www.slcyber.io/financial-crimes-on-the-dark-web/
3. https://www.slcyber.io/cybercriminals-targeting-financial-institutions-from-the-dark-web/
4. https://sqnbankingsystems.com/blog/the-role-of-the-dark-web-in-financial-crimes/#:~:text=What%20types%20of%20financial%20crimes,commit%20cybercrimes%20or%20hacker%20services.
5. https://www.researchgate.net/publication/350466645_Dark_Web_A_Breeding_Ground_for_ID_Theft_and_Financial_Crimes
6. https://www.researchgate.net/publication/357839318_CYBER_CRIME_IN_INDIA
7. https://arxiv.org/ftp/arxiv/papers/2104/2104.07138.pdf
8. https://deliverypdf.ssrn.com/delivery.php?ID=910024021106116081095105071110099126039006020032019035067003091010126083094065075007039055026029057040105066020116123087071087119055089076076127110101078091068020072033041079097115006113065067119116101094085008113089065002018103096092002126120084084096&EXT=pdf&INDEX=TRUE
9. https://www.researchgate.net/publication/331867659_Dark_Web_and_Its_Impact_in_Online_Anonymity_and_Privacy_A_Critical_Analysis_and_Review
10. file:///C:/Users/aksze/Downloads/JETIREQ06074.pdf
11. https://blog.ipleaders.in/laws-relating-dark-web-india/