IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 1, January 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101014 |

Dark Web: Threats give Rise to Society

Shivam R Patil[1], Aditya V Gurav[2], Prof. Anjali S. Gaikwad[3]

Department of MCA, Institute of Management, Kolhapur, Bharati Vidyapeeth (Deemed to be University), Pune, Maharashtra, India[1,2,3]

ABSTRACT: In latest years, the Darknet has emerged asone of themaximum explored subject'swithinside the cyber securitynetwork. Current educationalresearch and media reviewstend to factor up how the nameless nature of the darknet is used to ease crook activities. This paper reports on a recent study in four Darknet forums that reveals a different aspect of the Darknet.

Further, our research memberspoint out the achievement of effective socio-political values through the use of the Darknet. This achievement is enabled by various elements that are rooted in the Darknet's technological structure, such as anonymity, privacy, and the use of cryptocurrencies. These characteristics come up with a wide range of opportunities for good as well as for evil.

KEYWORDS: Darknet • Anonymity • Privacy • Cryptocurrencies

I. INTRODUCTION

To most users, the Internet gives the ideaofanever-ending virtual world of global e-Commerce and figures. Goods can be bought and delivered to your doorstep in 2 days or less, information can be accessed at the swipe of a finger, and dreams arise true. But the Internet has anunsafe, giant secret: the Dark Web. Today's number one source for stolen information, illegal things, and criminal services is as interesting a talking point as it is dangerous to browse. Whether we are talking about the huge amount of sensitive personal information takenfrom the Equifax breach, particular healthcare information stolen in the Anthem breach, or the credit/debit card information stolen in cases like the Target breach, they all have at least one element in common: this stolen data, in the end, makes its manner to the Dark Web to be bought and purchased.

II. DARK WEB

While the Internet appears to be a flat ecosystem on its outward, there are numerous different layers at play. In authenticity, there are three (3) major areas of the Internet to differentiate between: the Surface Web, the Deep Web, and the Dark Web. When on the topic of the Dark Web, the Deep Web may be scared out of your wits or used interchangeably, but the two different Internet layers vary quite a bit, especially with regards to the content.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101014 |

Concept of Dark Web

Fig-[1]

A: The surface web includes publicly searchable websites (blogs, shopping sites, news sites, YouTube).
B: The deep web consists of sites that require a login to access (email, banking portals, subscription services).
C: The dark web requires special tools to access, like Tor Browser, and isn't indexed by search engines.

Not like the Surface Web and the number of Deep Web content, the Dark Web cannot be accessed through regular web browsers such as Internet Explorer, Google Chrome, or Mozilla-Firefox. The most common tool for accessing the Dark Web remnantsis a browserreferred to as***TOR*** [The Onion Router] which was created by the military to protect foreigninfrastructures. Tor was eventually released to the public in 2004, leading to a group of developers creating the Tor-Project, the method most use to access the Dark Web today. While not every site on the Dark Web supports illegal activity, ahugenumber of black market activity occurs on the Dark Web today. The Tor-Project, Inc., became a 501(c) (3) non-profit in 2006, but the idea of "onion routing" began in the **mid-1990s.**

Access the Dark Web

The fastest way to access the dark web is to download and install the Tor Browser, which will route your traffic through the Tor network and allow you to access the dark web.On Tor, you can go into any URL you want to visit, including (.onion) domains on the dark web.

Disclaimer!- Before going any further, you need to understand that many things on the Dark Web can be very illegal. No matter what precautions you take, it's very unlikely that you'll be able to remain anonymous. Step into your own risk!

Dark Web Market

Now that you have a complete picture of the Dark Web, let's discuss the markets that can be found on this burgeoning social network. Just as users can purchase products through sources like Amazon and eBay on the Surface Web, *Tor*handlers can purchase illegal products or services through their Dark Web partners. There are many different marketplaces available on the Dark Web that sell a wide variety of stolen and illegal goods, including weapons, drugs, and stolen information. Recently,[146]million US citizen information was stolen through the Equifax breach, so you can assume there is a 50% chance (there are just over 300 million in the US).today) whose Social Security number (minimum) is currently being sold on the Dark Web.

When you check Dark Web prices for information, you might be quite surprised how cheap and easy it is to buy your stolen information. In a recent article published by Experian (one of the big three credit bureaus), the price range of information sold on the Dark Web was detailed (shown below). You'll probably find that it doesn't take much to steal someone's personal or financial information.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101014 |

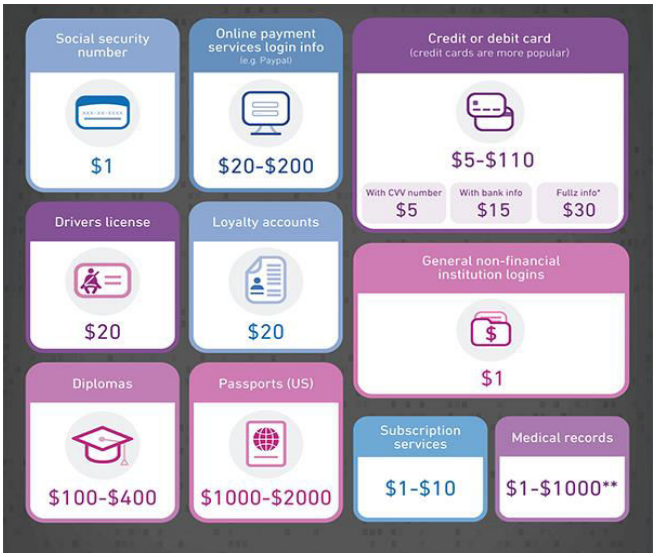

Fig-[2]

There are also more specialized markets to buy cybercrime services, which shows us why cybercriminal activity is so pervasive. These virtually anonymous cybercrime marketplaces make it easier for less experienced cybercriminals to spread malware or target businesses. Some of the products and services available include:

- *$7 hourly DDoS service*
- *$50 mailing list for 500,000 emails*
- *$60 daily botnet*
- *$10 average malware flask*
- *Ransomware Kits – Free - $1000*
- *Compromised Website - $10 – $15*
- *ATM Skimming Devices - $400*
- *Online hacking tutorials – 0$ - $500*
- *Money mules for hire - % of the money*

Whistle-blowers on Dark Web

Whistle-blowers (also written as whistle-blower or whistle-blower) is a person, usually, an employee, who discloses information or operate within a perceived private, public, or governmental organization that is illegal, illegal, dangerous, fraudulent, or abusive.taxpayerfunds. Those who become whistle-blowers can choose to bring information or accusations internally or externally. The company will solve and fix the problem. Externally,whistle-blowers can bring to light allegations by contacting the third party outside the organization, such as the media, government, or law enforcement. The most frequently reported type of retaliation was an abrupt shutdown.

News outlets like *The Guardian*, *The Intercept*, and *The New Yorker* all host dark web drop sites for anonymously leaked tips and documents. So does WikiLeaks, which popularized the concept and recently relaunched its submission system.

NEW YORKER: *strngbxhwyuu37a3.onion*
GUARDIAN: *33y6fjyhs3phzfjj.onion*
INTERCEPT: *y6xjgkgwj47us5ca.onion*
WIKILEAKS: *wlupld3ptjvsgwqw.onion*

Child-pornography on Dark Web:

Child sexual abuse material (legally known as child pornography) refers to any content that exhibits child-related pornography. Avatars include photographs, videos, digital or computer-generated images that are indistinguishable from actual minors. The photos and videos involved in recording an actual crime scene will then be released for personal consumption. Recently, direct sexual abuse has begun to emerge. In these cases, individuals pay to watch

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101014 |

child abuse live through a video streaming service. This type of abuse is extremely difficult to detect, due to its real-time nature and lack of digital evidence left behind after a crime is committed.
The playpenis a popular Darknet child pornography website that operated from August 2014 to March 2015. The site operates through a hidden service through the Tor network that allows users to Use anonymous websites. After running the site for 6 months, website owner Steven W. Chase was arrested by the FBI. After catching him, the FBI continued to operate. Website for an additional 13 days as part of Operation Pacifier. When it closed in March 2015, the site had more than 215,000 users and hosted 23,000 sexually explicit images and videos of toddlers.

Human Trafficking on Dark Web

Human trafficking is the recruitment, transportation, transfer, harboring, or receiving of people by force, fraud or deception, to take advantage of them for personal gain. Men, women, and children of all ages and backgrounds can be victims of this crime, which occurs in every region of the world. Traffickers often use violence or fraudulent recruitment agencies and false promises of study and employment opportunities to deceive and coerce their victims.
With some 25 million victims of human trafficking worldwide, authorities are still working to identify effective ways to identify and prosecute traffickers, many of whom use anonymity. Of the dark web to commit a crime.
Although a higher number of women have been identified asvictims of human trafficking, since the early 2000s the number oftrafficking for sexual exploitation has decreased while the number of cases of human trafficking for forced labor increased. This shows that rates of trafficking for forced labor are highin Africa and the Middle East, while Europe and North America have higher rates of trafficking for sexual exploitation. Continuedis, and of this total, only 9,568 people were convicted.
Like other criminals, traffickers don't follow the rules.Often associated with global and transnational organized crime, they employ all the tricks of the dark webto avoid detection, including complex encryption and constant switching between profiles and webpage. To navigate all levels of the Internet, including the dark web, to investigate human trafficking and identify and arrest traffickers. On the dark web and even engage with traffickers in complete anonymity by providing more evidence if the individual is brought to justice.

With the seamless integration of new data sources, Cobwebs' intellectual webplatform can also be used to deliver real-time content monitoring capable of digitizing images, and text. Excellent international awareness
While some messages may look benign to the naked eye, survey tools in online intelligence and media platforms can provide valuable intelligence to identify suspects and specific threats of human trafficking.
As investigators collect a mountain of data during a human trafficking investigation, it is important tousebig data to collect and manage the data. Using Cobwebs solutions, authorities then strategically analyze this data while receiving real-time alerts for any similarity from the powered.

Platform and default while traffickers may not use the same identifiers from site to site, they signal customers with content and language, such as advertising and similar interactions. Symbols like these can be identified andused to link different profiles as belonging to the same person and even reveal their cyber identity on the dark web.
The cutting-edge and unparalleled solutions provided by Cobwebs provide authorities with unprecedented perspectives on traffickers' dark web activity.Instead of asking "how to identify human trafficking on the dark web", authorities can nowsay "we have identified and prevented human trafficking on the dark web".

Bad Threads in Dark Web

One of the most commonly asked questions about the Dark Web is, "Did these guys ever get caught?" The dark web makes it difficult for authorities to remove the dark web due to severalfactors including Tor's multi-layer encryption, criminals using anonymous VPNs, websites hosted in different countries (no have strict network laws), and the (virtually undetectable) use of bitcoin or other cryptocurrencies when purchasing illegal goods or services, rather than doing the transaction through a bank.

Regardless of these factors, the short answer is yes; more and more bad guys are caught. There have been several known cases of Dark Web markets being disrupted by the FBI or other authorities. A few examples include Silk Road, AlphaBay, and Hansa, all of which are very popular Dark Web Markets.

Silk Road is one of the largest and most notorious black markets ever held on the Dark Web. Like many Dark Web marketplaces, Silk Road sells drugs, guns, cybercriminal products and services, and pornography. In 2013 following the arrest of the site's founder, Ross Ulbricht, he was ultimately sentenced to life in prison without the possibility of parole. Over $1.2 billion in revenue. Just five weeks after the original website was taken down, Silk Road 2.0 was released by the administrator of the original site. Silk Road 2.0 was online for a year before being taken offline in

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101014 |

another FBI bankruptcy, which resulted in the site administrator being arrested. , Blake Benthall. Silk Road 3.0 is currently active.

III. CONCLUSION

Several attacks are carried out on this platform and the ransom amount is made in the form of bitcoins on the Dark Net. It is also used by the governments of different countries for security reasons. Overview of different Dark Web attacks, exploits, browsers, and crimes. It can be concluded that the pros and cons of the Dark Web depend on the intentions of the users.

Faced with this threat, the natural reflex of free civil societies would be to advocate that Tor remain unsupervised and unsupervised to protect freedom of expression and privacy. The reality of the dark web is much more complex, requiring a nuanced approach from custodians and law enforcement. To prevent activities deemed illegal and immoral in free societies, and to protect the real interests of an anonymous network.

REFERENCES

1. https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.html
2. https://www.avast.com/c-dark-web
3. https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web
4. https://sbscyber.com/resources/an-intro-to-the-dark-web
5. https://www.researchgate.net/publication/338878596_Dark_Web_A_Web_of_Crimes: Dark Web: Web of Crimes by Shubhdeep Kaur ˙ Sukhchandan Randhawa

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details