Wireless Personal Communications
https://doi.org/10.1007/s11277-020-07143-2

Dark Web: A Web of Crimes

Shubhdeep Kaur[1] · Sukhchandan Randhawa[1]

Abstract
Internet plays an important role in our day to day life. It has become an integrated part of all daily activities or lifestyle. Dark Web is like an untraceable hidden layer of the Internet which is commonly used to store and access the confidential information. But there are number of incidents which reported the misuse of this platform for conducting the criminal and illegal activities in a hidden manner. In this paper, an overview of dark web and various browsers which are used to access dark web are presented. An insight into various aspects of Dark Web such as features, advantages, disadvantages and browsers are discussed. An overview of the different types of attacks, exploits and malwares is also presented. There are different types of criminal activities and incidents which take place over the Dark Web are discussed so that reader can become aware of such types of activities and can take appropriate preventive measures for these activities.

Keywords Internet · Dark Web · Darknet · TOR · Onion routing

1 Introduction

With the advancement in technology, digitalization has resulted in generation of different types of attacks. Web security has become a major area of concern as most of users visit online to get their needs fulfilled. As the Internet continued to grow in the mid-to-late 1990s it had come to transform so many things on a global scale. The biggest change came in the form of instant communication. As long as you have an Internet connection, you can talk to anyone. The main concern is that the Internet was not designed with factors like privacy and anonymity in mind. So everything can be tracked or traceable. But some people are very concerned about their privacy and in the mid-1990s one such group of people was US Federal Government. A team of computer scientists and mathematicians working for one of the branch of the US Navy, which is known as the Naval Research Laboratory (NRL), began development of new technology called as *Onion Routing*. It allows

✉ Sukhchandan Randhawa
sukhchandan.95@gmail.com

Shubhdeep Kaur
shubhdeep.randhawa@gmail.com

[1] Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, India

Published online: 28 January 2020

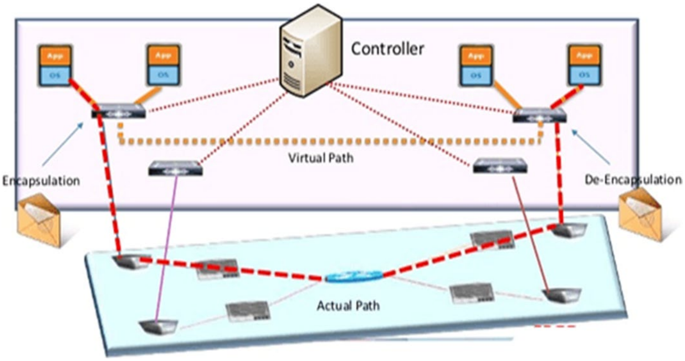
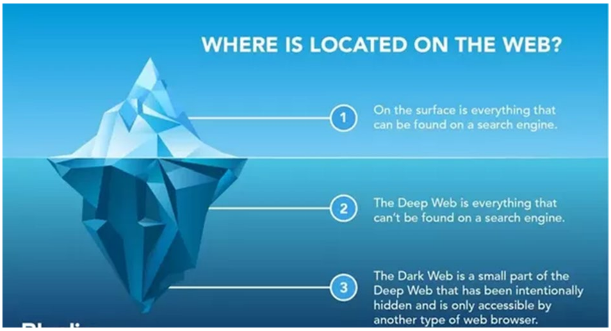


Fig. 1 Overlay network

Fig. 2 Layers of internet


WHERE IS LOCATED ON THE WEB?
1
On the surface is everything that can be found on a search engine.
2
The Deep Web is everything that can't be found on a search engine.
3
The Dark Web is a small part of the Deep Web that has been intentionally hidden and is only accessible by another type of web browser.

an anonymous bi-directional communication where the source and destination cannot be determined by third-party [1]. This is accomplished by creating Overlay Network. An overlay network is a network that is built on top of another network. Here, in our case that network is Internet. In this scenario, the traffic goes through an overlay network as shown in Fig. 1.

A network using the onion routing technique is classified as a *Darknet*. With the combination of all these different darknets, *Dark Web* came into existence. People at NRL soon realized that for network to be truly anonymous it has to be available to everyone and not just the US Government. So, the NRL was forced to release their Onion routing technique to the public under an Open Source License and it became The Onion Router (TOR) [2].

2 Structure of the Internet

The World Wide Web (www) consists of three parts i.e. *Surface Web, Deep Web* and *Dark Web* as shown in Fig. 2. The *Surface Web*, which is also known as the *visible* or *indexed* web is readily available to the public through the standard web search engines. Only 0.03% results are retrieved through surface web search engines.

The *Deep Web* [3] is opposite to the surface web and is not accessible by the general public. It is also called as the *Invisible* or *Hidden* web. It is estimated that 96% of Internet is deep and dark web. It is mostly used for confidential purposes. Some of the deep web examples are: Netflix, Online banking, Web mail, Dynamic pages and Databases and everything that is password or paywall protected.

The *Dark Web* [4] which also refers to World Wide Web content but it is not the part of the surface web due to which it is also not accessible by the browsers which are normally used to access the surface web. It began to grow with the help of the US Military, which used it as a way to communicate with intelligence assets stationed remotely without being detected. The dark web is that part of the web where most of the illegal and disturbing stuff takes place. The Dark Web is also used as an illegal platform for Terrorism, Hacking and Fraud Services, Phishing and Scams, Child Pornography and much more. Dark Web is a part of the Deep Web. Dark Web provides hidden services, which are ended with onion extension. Example, Facebook operates a hidden service. Another example is Duck Duck Go search engine. There is special kind of browsers to access the Dark Web. The various browsers which are used to access the Dark Web are The Onion Router (TOR), FreeNet, Riffle, Invisible Internet Project (I2P) and Whonix.

3 Organization of the Paper

The various aspects of the Dark Web which are presented and discussed in this paper. Section 3.1 discusses the tools and protocols used to develop the Dark Web. Section 3.2 presents the browsers which are used to acces the Dark Web. Methods used in Dark Web for anonymity and confidentiality are discussed in Sect. 3.3. Section 3.4 discusses the various types of crimes which take place on the Dark Web. The various types of security breach attacks and their defence mechanisms are presented in Sects. 3.5 and 3.6. The impact of Dark Web on cyber-security, Internet governance and its legal implications and pros of Dark Web are discussed in Sects. 4 and 5 respectively. Sections 6 and 7 present some interesting facts regarding Dark Web and Conclusion of the findings respectively.

3.1 Elements of the Dark Web

There are number of protocols and tools which have been utilized in order to develop the Dark Web. The essential components of the Dark Web are *browsers* in order to access the dark web, *encryption technique* in order to encrypt the data, *Virtual Private Networks* for transmitting the data and *routing algorithm* [5]. To access the dark web it is very important to stay anonymous. Browser is not enough to stay anonymous but also you need to use a good Virtual Private Network(VPN). It could be paid Nord VPN or phantom VPN. *NordVPN* act as a personal VPN service provider. It has desktop applications for macOS, Windows and Linux for iOS and Android. In case of *Phantom VPN* the Internet usage is not tracked and is kept safe from ISPs, online snoops and advertisers.

Encryption is key feature which is used in Dark Web. Multiple layers of complex encryption are used by TOR browser and *random routing* is used to protect your identity. If you are on dark web and you don't want to use some centralized communication system then that data is available to third party. It means you shouldn't share any information that could be a problem if third party gets their hands on it. Anonymity solves this problem for the most of the cases. But the problem is still there as the third party can still reads the messages you send or receive. Then the encryption technique known as Pretty Good Privacy (PGP) [6] comes into play. It is a powerful encryption technology that has been protecting all sort of sensitive information or communication. It was designed to provide security aspects such as integrity, authentication, privacy and non-repudiation. PGP is basically based on the asymmetric encryption. In asymmetric encryption, two different keys i.e. Public key and Private key are used to encrypt and decrypt the data. The key which is publicly available to anyone is Public Key. In this type of encryption if someone encrypts a message with your public key then you are the only person who can decrypt it and read it. PGP can also be used for authentication purpose. For authentication, PGP works in a different way. It uses a combination of hashing and public key encryption. To provide privacy, it uses a combination of secret key encryption and public key encryption. Therefore, one secret key, one hash function and two public–private key pairs are used in digital signatures as shown in Fig. 3.

There are number of benefits of using PGP Encryption. Firstly, the information is always protected as it cannot be viewed or stolen by anyone on Internet. The information or data can be shared securely over Internet. Deleted messages or other sensitive information cannot be recovered once they are deleted. Secondly, the emails or messages cannot be infected by attackers. This encryption technique verifies the sender's information so that it is not be intercepted by the third party. It is easy to use. Confidentiality is provided by

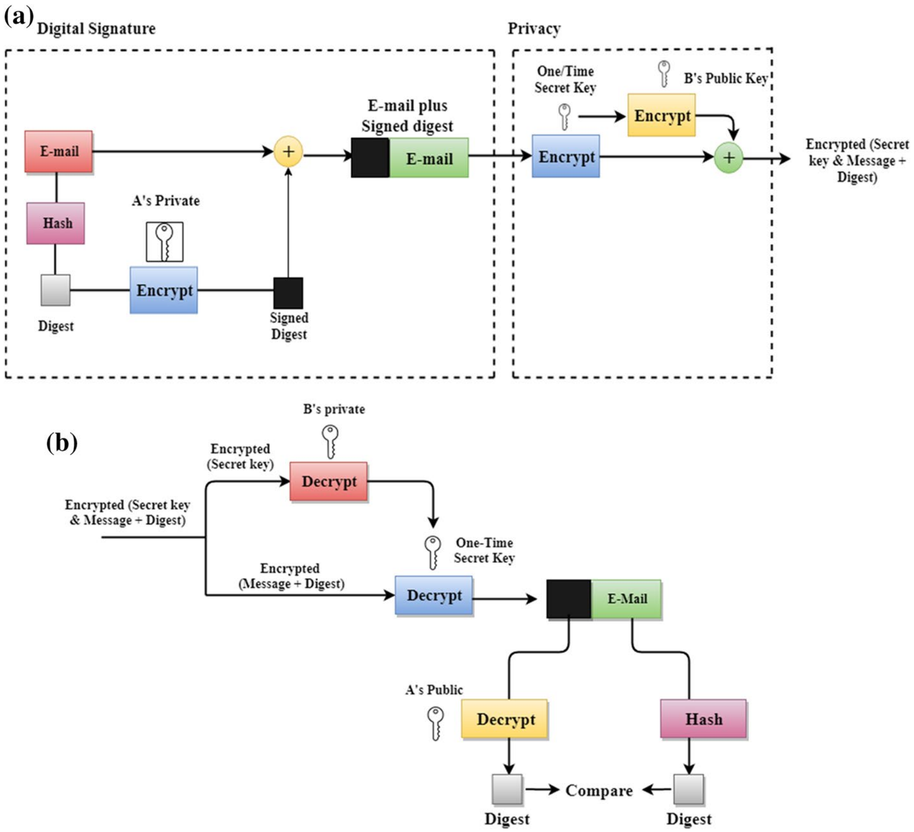


Fig. 3 **a** PGP at sender site (A). **b** PGP at the receiver site (B)

using symmetric block encryption. Digital Signatures provides the mechanism of authentication. It provides compression using radix-64-encoding scheme.

There are numbers of *browsers* which have been developed in order to access the Dark Web. A detailed discussion regarding the various features of the browsers has been presented in Sect. 3.2. The most commonly used browser for Dark Web is The Onion Routing (TOR). It was developed by Paul Syverson, Michael G. Reed and David Goldschlag at the United States Naval Research Laboratory in the 1990s. TOR was written in *C, Python* and *Rust*. The alpha version of TOR was launched on September 20, 2002. It works on the onion routing technique [7]. In this method the user's data first gets encrypted and then data gets transferred through various *relays (intermediate computers)* present in the network. Thus, it creates a multi-layered encryption based network.

The more number of relays would be results into more bandwidth and also it will be more difficult to track any user. By default, there are three relays through which TOR shares connections as discussed below [8]:

1. *Guard and Middle Relay*: The guard and middle relay is also known as non-exit relays as shown in Fig. 4. It is a basic relay which helps in making the TOR Circuit. The middle relay neither act as guard relay nor exit relay, but it acts as second node between the two. The guard relay must be fast and stable. It requires minimum maintenance efforts. Initially the real IP address of the client or user who tries to connect to the TOR Circuit can be seen. There are websites through which the currently available guard relays and their details can be seen [9–11].
2. *Exit Relay*: It is the final relay in the TOR Circuit. It is the relay that sends traffic out to its destination. The clients will see the Exit relay's IP address only instead of their original IP addresses. Each node only has the information about its predecessor and descendant (Fig. 5).
3. *Bridge*: As discussed previously, TOR users will deal with relay's IP addresses only. But still TOR can be blocked by the governments or ISPs by blacklisting the public TOR nodes' IP addresses. Bridges are relatively of low risk and also require low bandwidth to operate.

3.2 Browsers: A Way to Access the Dark Web

Browser acts as a way to access the Dark Web [12, 13]. Table 1 presents the various types of browsers to access Dark Web along with their advantages and disadvantages.

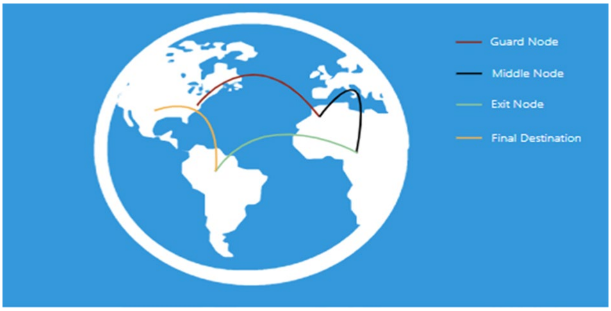


Fig. 4 Relays used in Dark Web

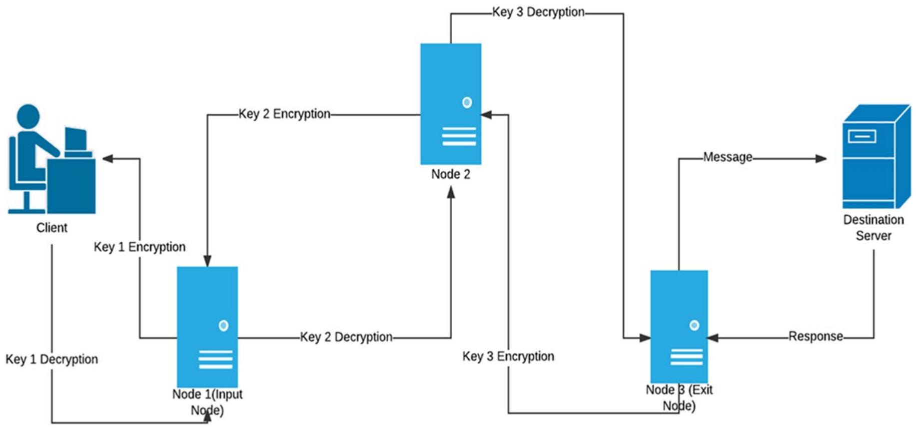


Fig. 5 Data flow in onion routing

The underlying routing protocol used in a particular browser and its features are also listed in table.

3.3 Methods used in Dark Web for Anonymity and Confidentiality

Anonymity and Confidentiality are the key factors based on which the Dark Web is entirely based. To maintain the anonymity and confidentiality, there are few techniques which are used as discussed below:

(i) *Proxy*: It is a service in which the requests are collected from clients and then forwarded to the destination on the behalf of the requestors. After receiving the replies the proxy sends the information back to the requestor. It acts as an intermediate between sender and receiver. For filtering and bypassing, such Internet filtering proxies can be used. To limit users' access to specific websites, proxies are used in some areas.

(ii) *Tunneling/Virtual Private Networks*: A VPN is a most common solution for network tunneling. It is a private network which provides inter-connectivity to exchange information between various entities that belong to the virtual private network. Sometimes VPNs are used to access company's intranet resources. It is another way to bypass the Internet censorship. VPN is more beneficial than Proxy as it uses Internet Protocol Security or Secure Socket Layer which provides secure communication.

(iii) *Domain Name System Based bypassing*: DNS is a mechanism in which translation of domain names to IP addresses takes place. It is easier to access Internet resources using DNS. To visit a web site, we only need to know the address of the website, rest will be handled by the DNS like resolving IP address for that domain name and forwarding request to the server. It is another option for enforcing censorship.

(iv) *Onion Routing*: It is a networking mechanism which ensures that contents are encrypted during transmission to the exit node. It also hides who is communicating with whom during the whole process. It provides anonymous connections. It is different from other methods as discussed previously. The connection takes a long route from Source A to destination B along an encrypted chain, which is known as *Onion.*

Table 1 Browsers to access Dark Web

Browser name	Advantages	Disadvantages	Features	Routing protocol
TOR browser	i. Provides the anonymity to websites and servers. ii. Protects the privacy of the users by hiding their IP addresses. iii. Supports all the. Onion websites which cannot be accessible by any other browser. iv. Provides security by passing the data through different relay servers. v. User's Internet activity is non-traceable	i. Slowing down your browser as the data is passed through numerous hops. ii. It does not attempt to protect against the traffic monitoring. iii. Security at the exit nodes is very low. iv. It cannot provide the end-to-end encryption. v. It is not suitable to work with Bit Torrents or any other torrents as they can somewhere reveal our identity or other information. vi. Low latency is also a factor	i. Overlay network is used to direct the Internet traffic. ii. It is free to access. iii. It is an open source software	Onion routing
FreeNet	i. Inserted data gets transmitted over a large number of hosts. ii. Each node contributes to the speed of downloads. iii. It is esteemed to outperform with Bit Torrent iv. It does not let your browser speed slow. v. It allows fast downloads of big files.	i. High latency of FreeNet does not let the user to do high computation activities such as playing real time games. ii. Poor handling of interested parties. iii. There is no fixed storage size, so it does not guarantee the permanent storage of the file. iv. It does not have its own search system.	Peer-to-peer platform	It uses decentralized distributed data stores to keep and deliver the data.

Table 1 (continued)

Browser name	Advantages	Disadvantages	Features	Routing protocol
Whonix	i. Onion services are safe to access. ii. Software flexibility is also there. iii. It provides the protection against the location and IP address discovery. iv. It also provides automatic routing of all applications.	i. Difficult to set up as compare to TOR browser. ii. A lot of maintenance is required. iii. It has strict hardware requirements. iv. It requires virtual machines and spare hardware. v. Updating process results into slowing down of TOR proxy	i. It provides user privacy. ii. It provides security by isolation. iii. It provides the protocol leakage and fingerprinting protection. iv. It also provides anonymity of IRC, chat and emails etc.	It consists of two virtual machines (workstation and TOR gateway). It utilizes Phantom protocol
I2P(Invisible Internet Project)	i. The network itself is a strictly message based. ii. Due to cryptographic identifiers the sender and receiver need not to reveal their IP addresses to the third party. iii. It makes the timing attacks difficult. iv. It is based on Garlic routing and these messages are more difficult to decipher as compare to Onion routing messages. v. File sharing is more efficient.	i. It best works only on Linux whereas Mac and Windows gets easily tracked. ii. It has reliability and implementation issues. iii. To access the content the user should be logged-in where in case of other anonymous browsers, the user can directly access the content.	i. It focuses on secure internal connections between users. ii. It provides messaging services like I2P Bote which provides anonymity during sending messages and mails. iii. It provides the Internet Relay Chat (IRC) facility. iv. Setting up I2P is easy.	Garlic Routing
TAILS (The Amnesic Incognito Live System)	i. Leaves no trace on the computer which is currently used by the user. ii. It uses cryptographic tools to encrypt the mails, messages and files. iii. It does not need to be installed on your system.	i. It only supports × 86 and × 86_64 architectures. ii. It does not provide protection against the compromised hardware. iii. It does not provide protection against firmware attacks.	i. It can be run under Virtual Box as virtual guest. ii. It automatically upgrades the USB versions. iii. Customization is easy. iv. It provides multilingual support.	Debian Linux

Table 1 (continued)

Browser name	Advantages	Disadvantages	Features	Routing protocol
Sub graph OS	i. It is designed to reduce the attack surface of the OS. ii. It eliminates the user's manual configurations.	i. It is easy to run malicious code containing desktop files. ii. Malware can also bypass Subgraph OS's firewall. iii. Encryption of file system is mandatory for installation process.	i. It only requires to configure the application proxy settings to connect through TOR's built-in proxy. ii. It is resistant to cold boot attacks.	Debian Linux

The whole communication happened within an onion which is encrypted, where each node is called as *relay*, which contains the information about the adjacent nodes. To understand the concept of Onion Routing more precisely let's take an example. Now let's suppose we are using TOR to access YouTube and the current location is China and we don't want government to know about this. The system needs to connect to the server to get the homepage of the YouTube but it doesn't connect to the server directly. It does that task through 3 nodes/servers/routers so that no one can traceback the conversation with that server.

- The client has access to the three encryption keys i.e. key1, key2 and key3 which encrypts the message three times and wrapping it under three layers.
- The encrypted message is sent to the Node 1.
- Node 1 contains the address of Node 2 and key1. It decrypts the message using Key1 and then passes it to Node 2.
- Node 2 contains Key2 and contains the address of input as well as exit node. By using Key2 it decrypts the message and passes it onto exit node.
- Node 3 which is Exit node finds a GET request for YouTube and passes to the Destination server.
- The server fulfills the request of the desired webpage as a response.
- And the whole process takes place in reverse direction with encryption layer using specific key.
- Finally it reaches to the client.

3.4 Crimes

Dark Web is the hub of the criminal attacks [13] as it provides anonymity and act as a gateway to the world of crime. Following are some of the prominent crimes which occur over the Dark Web:

(I) Drug trafficking

The dark web is an illegal dispensary of illicit and dangerous substances [14] that are sold in exchange of crypto currencies. For example, bit coin, Ethereum and ripple etc. The dark web's largest dark net market which was started by a Canadian, was shut down by the U.S Police. Silk Road [14–16] was also the one of the famous marketplace for illegal drugs and unlicensed pharmaceuticals. In 2013, the FBI shuts down this website [17]. Agora is the website which is also shut down last year. Now Alpha Bay is the largest marketplace for drugs. Dream Market, Valhalla and Wall Street Market etc are also marketplaces for drugs. There are number of such websites which are running over the Dark Web for illegal drug marketing and purchase.

(II) Human trafficking

Black Death is a place on the dark web where the human trafficking takes place. Chloe Ayling, the British model is one of the victims of Dark web's human trafficking practice. According to a 2017 report, the most of the survivors of human trafficking were recruited for sex trafficking and labor trafficking.

The other reports have shown that Dark Web has helped to push this crime deeper into secrecy. Black Death is an organization operating on dark web by frequently changing the URLs.

(III) Information leakage

Many platforms such as TOR which supports anonymity are the useful resources for whistleblowers, activists and law enforcement. Dark Web is also a platform for hackers to leak the sensitive data. A hacker group once posted the credit card accounts, login of about 32 million Ashley Madison customers as a 9.7 GB as a data dump on the dark web. Similarly in 2017 over 1.4 billion personal records were leaked over the dark web in the form of plain text which was openly available on the web. Even the dark web hubs pay the workers to leak the corporate information.

(IV) Child Pornography

The study found that child pornography generates the most traffic to the hidden sites on TOR. It is not easy for an average user to find such sites. It is an act that exploits the children for sexual stimulation and abuse of child during sexual acts. It also includes the sexual images of child pornography. A site known as Lolita City which has now been taken down as it contained over 100 GB of photos and videos of child pornography and has around 15,000 members. PLAYPEN was taken down by the FBI in 2015 which may have been the largest child pornography site on the entire dark web with over 200,000 members.

(V) Proxying

The anonymity property of the Tor like platforms makes its users vulnerable to attack. The URL of such a site does not show the typical 'HTTPS' which indicates a secure site. To make sure they are on the legit site they have to bookmark the TOR page. In case of website proxying, the scammer tricks the user so that the user thinks he is on the original page and the scammer re-edits the link to redirect the user to his scam link. Whenever the user will pay the amount in the form of crypto -currency, it gets funneled to the scammer instead.

(VI) Frauds

Carding frauds refers to the stealing and selling of user's credit card credentials and personal information. It is the most common type of crime that happens on the Dark Web. There are number of reasons that make this fraud most popular over the Dark Web. Dark net markets offer the sale of credit and debit cards. These sites have multiple URLs that redirect the user to the same page. The vendors from various forums posts ads in which they specify what they have. The different forums also provide a live chat facility. Vendors offer cards at lower prices. Some money transfer platforms are also susceptible to carding frauds.

(VII) Bit coins scam

Bit coin is the widely used crypto currency used on the dark web. It is also a logical currency for cybercriminals. Proxying and Onion Cloning are the examples of such crimes as

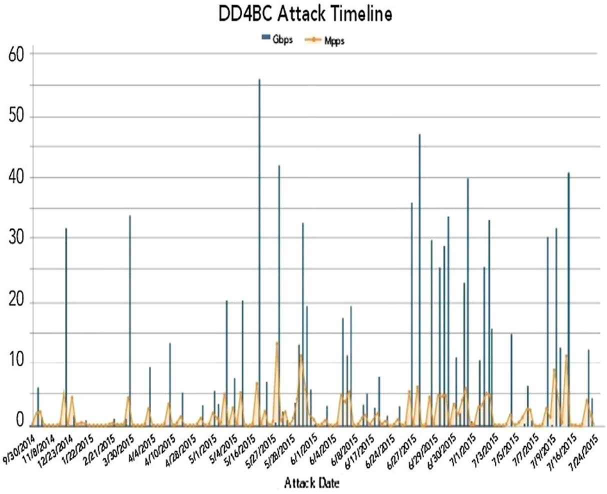


Fig. 6 Graph representing the attack timeline of bandwidth and packets per second of DD4BC

shown in Fig. 6. Europol's officials have expressed their concern that bitcoins have started to play a growing role in illegal activities. DDoS "4" Bitcoin (DD4BC), a group of cybercriminals behind Distributed Denial of Service (DDoS) attacks has attacked over 140 companies since its emergence in 2014. This inspires other groups also and leads to the Cyber Extortion. According to the Europol's officials the DD4BC group first threatened victims via email with a DDoS attack until ransom in the form of bitcoins is not paid. The rise of Bitcoin also leads to rise of Cyber-Terrorists in the world of dark web.

(VIII) Arms trafficking

It is a platform for illegal arms trafficking. According to the study of the RAND Corporation, dark net is indeed increasing the availability of firearms at similar prices as those are available in streets of black markets. It is also found that Europe is the largest source of firearms. Denmark is the second country that is the part of this dark market with the highest share of firearms vendors at 12.98% as shown in Fig. 7. While Germany comes at third with 5.31%, Dark Web has become a platform for criminal gangs and terrorists.

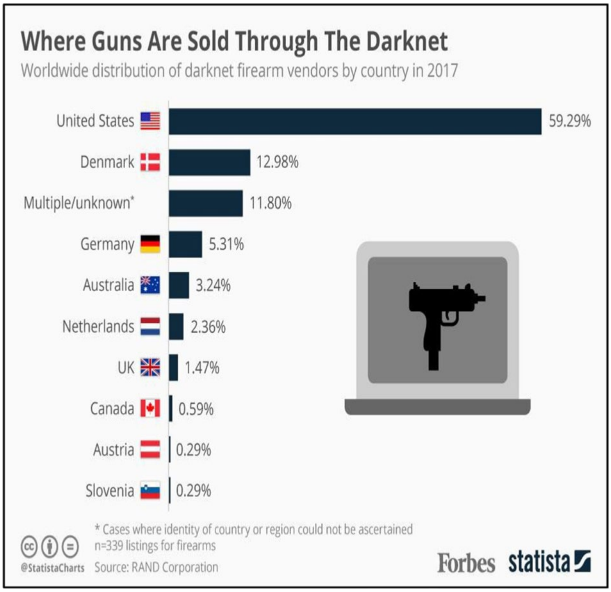
(IX) Onion cloning

Onion cloning is similar to proxy tactic. The scammer makes the copy of the real site or page and updates the links so that the user gets redirected to their scammed sites in order to steal the money from the user side.

(X) Contract killers

Dark web is also a platform for hiring hit men. It is a platform where a professional killer can be hired. Once the hacker named 'bRpsd' breached the website of BesaMafia and leaked its contents online. The leaked content contains user accounts, personal messages,

Fig. 7 Guns Sold over the Dark-Web across the World



38 hit-orders and a folder consists of nearly 200 victim's pictures. Some of the murder-for-hire groups include Unfriendly Solutions, Hit men Network, and C'thulhu. Unfriendly Solution accepts the payment in bitcoins only. Hit men Network which claims to be a trio of contract killers working in the United States, Canada and European Union offers a commission for referring them to their friends.

(XI) Torture

Red Room sites are those sites where users pay in thousands to see streaming murders, rapes, child pornography and different kinds of torture. But there is still no evidence that they exists. If they do exists then they cannot be accessible through TOR as TOR is too slow for streaming live videos. According to some sources, users of a pedophile site paid huge amount of money to watch the videos of Scully's abuse and torture of a young child. It was a series produced by Scully's company i.e. No Limits Fun (NLF). One of his videos, Daisy's Destruction was widely discussed on the forum which was not a sniffed film, but features actual sexual assault and horrifying abuse of a young child. It was streamed on 'Hurtcore' pedophile sites, the site where pedophiles watch torture or abuse of children and babies. On 13 June, 2018 Peter Gerard Scully was sentenced to life imprisonment.

(XII) Revenge porn

Revenge porn is distribution of sexual images and videos of individuals without their consent. Many sites have been shut down. If we talk about surface web, Google has already removed the revenge porn from its search results when it is requested. 'Pink Meth' was originally surface web's site before switching to the dark web. It allows users to submit their content anonymously. Pink Meth gets seized now.

3.5 Cyber Attacks and Defense Mechanisms

There are number of cyber attacks which can be launched via DarkWeb. The biggest disadvantage of the Dark Web is its anonymity which raises the confidence level of the attacker and can easily attack the targeted victim [18–20].

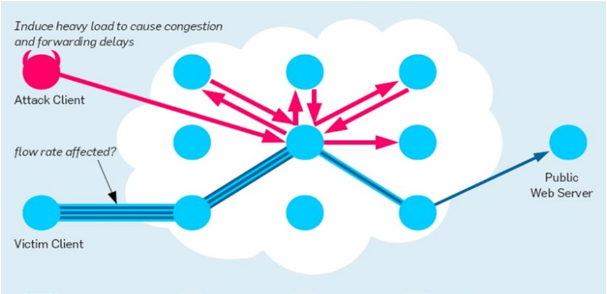
(i) Correlation attacks

It is an end-to-end passive attack. In this type of attack, the attacker controls the first and the last router in the TOR network and uses the timing and data features to correlate the streams over those routers to break the TOR's anonymity. In the past, many government agencies with the help of correlation attack were able to destroy the anonymity of many users. There is no alternative method to prevent this kind of attack because it is a highly sophisticated mathematical method. This kind of attack is not only for softwares but are also used against the users. Example, a dark-market admin writes his details on the site such as his age, previous criminal activities and so on. It will help the agencies to monitor the Internet activities of all the suspects and try to see which one connects to the TOR network when admin comes online. Carnegie Mellon University once attacks on a TOR network which was indeed a correlation attack. The information about the TOR users was then sold to FBI for $1 million. Still the correlation attack is not prevented. The attack was a downfall for many websites like Silk Road 2.0 and other child porn sites. The only defense mechanism available for this type of attack is the selection of the trusted VPN to get rid of this attack.

(ii) Congestion attacks

The congestion attack which is also known as *clogging attack* not only monitors the connection between the two nodes but also creates the path between them. If one of the nodes in the target path gets blocked by the attacker then the speed of the victim's connection should change. It is an end-to-end active attack. In 2005, Murdoch and Danezis described an attack on TOR in which they could reveal all of the routers involved in a TOR circuit, by using clogging attack and timing analysis together. The congestion attack also works on routers having different bandwidths as shown in Fig. 8. This attack is effective as the exit router runs and we have to find only a single node. It also removes the common limitation of DoS by using multiplication of bandwidth technique, which allows low bandwidth connections to use high DoS bandwidth connections. This type of attack can be avoided by not

Fig. 8 Congestion attack



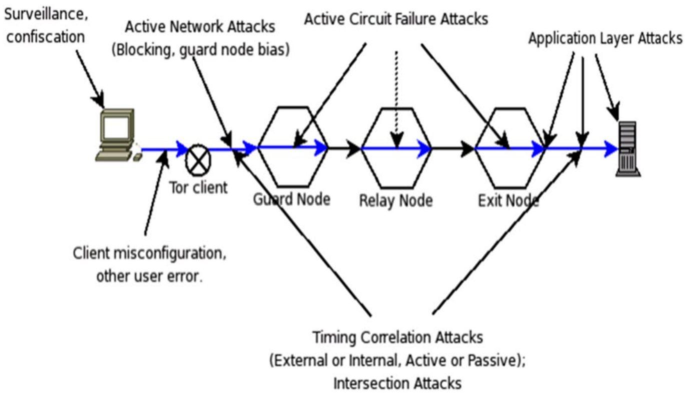

Surveillance, confiscation
Active Network Attacks (Blocking, guard node bias)
Active Circuit Failure Attacks
Application Layer Attacks
Tor client
Guard Node
Relay Node
Exit Node
Client misconfiguration, other user error.
Timing Correlation Attacks (External or Internal, Active or Passive); Intersection Attacks

Fig. 9 Timing attacks in TOR

using a fixed path length. Second, end-to-end encryption can be used. Third, by disabling the JavaScript in clients and by inducing delays into connections, this type of attack can be avoided.

(iii) Traffic and timing correlation attacks

These are end-to-end active attacks [21]. These attacks are another form of de-anonymization attacks. In this type of attack the entry and exit relays of a target get modified as shown in Fig. 9. By determining the flow patterns in traffic flowing from entry relay to exit relay, the attacker can determine to which server a client is communicating. For de-anonymization it is not necessary to use complex mathematical methods. Example, a student of Harvard University was arrested for sending fake bomb threats, via TOR to get out of an exam. According to FBI data, the emails were sent by using Guerilla Mail. Guerilla Mail is an email provider that allows users to create temporary emails. It embeds the IP of the sender in all outgoing emails. The FBI stated that the student sent the emails via TOR. Correlation helped the FBI to identify the student. Traffic and Timing attacks are easy to execute when the number of clients using TOR is relatively small. Otherwise more complex methods of timing and traffic attacks are used to de-anonymize the users. TOR embeds delaying, packets buffering and shuffling approaches in order to prevent such attacks.

(iv) Traffic fingerprinting attacks

It is a single-end passive attack. It is a technique which is used to sniff the website by analyzing the traffic flow pattern without removing encryption. There are two methods to capture the traffic data in TOR. In the first method, the attacker captures the traffic through the entry node. But in this method it is not necessary that the particular victim will connect to the attacker's node. So there is an uncertainty. In the second method, the attacker will play the role of network operator for example, Internet Service Provider (ISP) and will able to capture the traffic between victim and entry node of the TOR circuit. This is an effective method. There are number of defence mechanisms available for this type of attack namely

HTTP with Obfuscation (HTTPOS), pipeline randomization and Guard node adaptive padding and Traffic Morphing etc.

(v) Distributed Denial of Service (DDoS) attacks

The attacker sends the multiple fake requests to the target to slow down the connections or making it unavailable to the victim. It is not used to de-anonymize users. The sudden disappearance of Abraxas marketplace is the one of the biggest mystery. Till now it is not clear whether the Abraxas marketplace was targeted with a DDoS attack or it was an exit scam. Most of the sources state that it was an exit scam as the marketplace mysteriously disappears when the bitcoin price gets high. There can be possibility that the Abraxas marketplace was targeted with DDoS attack. Before it gets terminated, users reported very slow server and also difficulty in logging into the marketplace. Secondly, on Reddit Abraxas marketplace admins gives the statement that they have suffered a major DDoS attack and they will be back soon [22, 23]. Multi-variate threat detection can be used to efficiently detect the DDoS attacks in a timely manner.

(vi) Hidden services attacks

Hidden services allow access to resources without revealing the user's identity. *First node attack* aims to reveal the hidden services. The attacker's relay tries to become the relay in the network that is directly connected to the server of the hidden services. By doing this it will immediately reveal the location of the hidden service. The attacker uses the malicious node to get connected to the server. By using time analysis the malicious node determines whether the particular node is first node or not. Another attack which is *Clock Skew* attack can pick the hidden services from the list of various servers. By comparing the timestamps from various servers, the location of hidden services can be revealed.

(vii) Phishing

When the attacker wants to install malware or want some sensitive information from user side, then he often use phishing tactics or pretends to be someone else. In this type of attack, an attacker may send you an email that appears to be from some trusted source. The email will contain the link or an attachment, and you will thereby install the malware. There are three types pf phishing reported in the literature namely Spear Phishing, Whaling and Clone Phishing. When a specific organization is a target then spear phishing is used. This attack is used to target large number of people to get important information. In Whaling, it targets an organization's senior or C-level executives. The attackers use focused messaging to trick the victim. In Clone Phishing, targets are presented with a clone or copy of a message they had received earlier. This attack is based on the previously seen message, so it can easily target the user.

Preventive Measures for Phishing:

The following preventive measures can be taken in order to avoid such types of attacks:

- *Filter on Malicious URLs*: Quarantine messages contain malicious URLs. Some attackers use image as a phishing message. The image contains text, which is usually gets ignored by some of the filters. Character-recognition based filter technology can detect these messages.

- *Filter Suspicious Attachments*: Remove and quarantine incoming attachments as they are known to be utilized in malicious ways.
- *Promote Good Credential Behavior*: Passwords must be strong, they should contain numbers, alphabets, special characters. Passwords must be changed frequently. The use of 2 step-verification is recommended.
- It is also a good practice to regularly scan user and infrastructure systems for malware.

(viii) Session Hijacking and Man-In-The-Middle Attacks

When a user is requesting for specific websites or services to the server, the server fulfills the request and sends the information that has been requested previously. The session between the computer and the remote web server given a session ID which is unique and also which is supposed to be private between two parties, the attacker can hijack the session by capturing the unique session ID. The attacker can also hijack the session by inserting themselves between the computer and the remote server, pretending to be the other party. This allows the attacker to intercept the information in both directions and is known as Man-in-the-Middle attack. There are various types of attacks: *ARP Spoofing, Rogue Access Point, mDNS Spoofing and DNS Spoofing.* Address Resolution Protocol (ARP) resolves the IP address to physical MAC addresses in a LAN. When one host wants to communicate with other host, it refers to the ARP cache. Devices with wireless cards try to auto-connect to the access point. In *Rogue Access Point* attack, attackers create their own wireless access point and trick the nearby devices to join their domain. The attacker manipulates the target's network traffic. Multicast DNS is done on a Local Area Network (LAN) using broadcast. Users don't have the information to which addresses their devices are communicating with. In *mDNS Spoofing*, at some point when the app needs to know about the device address, attacker can easily respond to that request and takes control over it. DNS resolves domain names to IP addresses. In *DNS Spoofing*, the attacker introduces corrupt DNS cache information to host and hence tries to access another host using their domain name. This whole process leads to the target sending sensitive data to malicious host.

Preventive Measures:

The following preventive measures can be taken in order to avoid such types of attacks:

- *Strong Router Login Credentials*: It is important to change the default router login as well as Wi-Fi password. The attacker can find the login credentials of router and can change DNS server to malicious server.
- *Virtual Private Network (VPN)*: Use VPNs as they provide secure environment for the sensitive data. VPNs use key based encryption for secure communication.
- *Force HTTPS*: HTTPS can be used for secure communication for public–private key exchange.
- *Public Key Pair Based Authentication*: RSA for public key pair based authentication can be used to ensure whether the things you are communicating with are actually the things you want to be communicating with.

(ix) Cross site scripting (XSS) attacks

If the attacker targets the vulnerable website to get the information, this is called SQL injection Attack. But if the attacker targets the website's user then this attack is Cross Site Scripting Attack. Both attacks are similar, as both involve injecting malicious code into a website. But in this type of attack, the website itself is not being attacked. The malicious code only runs in user's browser. Such type of attacks damages the website's reputation by placing the user's information at risk without any indication. There are three types of attacks namely *Reflected XSS, Persistent XSS* and *DOM-based XSS.* In Reflected XSS, the data is accepted by vulnerable site. An attacker crafts up a URL that passes a malicious script. This malicious script gets injected into the webpage that the victim's browser is loading and is executed by browser. In Persistent XSS, code for attack is stored on the vulnerable server. In the simple example the attacker posts a message to forum hosted on a vulnerable website. The post content contains the malicious script. When a user will visit the forum post, browser loads and executes the script. In DOM-based XSS attack, the vulnerability exists in the client side scripts. This attack is different from the other two attacks. The client side scripts deliver the malicious script to the target's browser. There are number of cons of this type of attack as users' sensitive data gets exposed. The websites can be redirected to the harmful locations. The malicious programs can be uploaded and online accounts can be seized by attackers.

Preventive Measures:

The following preventive measures can be taken in order to avoid such types of attacks:

- Encode the output to prevent potentially malicious user-provided data from automatic load and execute by a browser.
- Limit the use of user provided data.
- Utilize the content security policy as it provides additional levels of protection against XSS attacks

(x) SQL injection (SQLI) attack

Many of the servers, stores critical data by using Structured Query Language (SQL) to manage the data. SQL injection attack usually targets such kind of servers. It can be serious if the database has the information regarding customer's details such as bank details, credit card number or other sensitive information. There are three types of SQL injection attacks which have been reported in the literature: *Unsanitized Input, Blind SQL Injection* and *Out-of-Band Injection*. In *Unsanitized Input*, the attacker provides the input to the user which is not properly sanitized or input is not validated. *Blind SQL Injection* is also called as inferential SQL Injection attack. It doesn't reveal data directly. The attacker closely examines the behavior. The revealing of data depends upon the attacker's requirements. *Out-of-Band Injection* is complex. It is used when the attacker is not able to get the information through any other form of attack. The attacker craft the SQL statements, which when gets triggered, creates a connection with the external server and that external server gets controlled by the attacker to get the data or the desired information.

Preventive Measures:

- Don't use dynamic SQL.
- Stored procedures are safer as compared to dynamic SQL.
- Always prefer to use prepared statements and parameterized queries.

- Don’t leave sensitive data into plain text.
- Encrypt the sensitive data and also salt the encrypted hashes as it provides another level of protection.
- Limit the database permissions.
- Attackers can use the error messages to gain information, so avoid displaying the error messages directly to the user.
- Use Web Application Firewall (WAF) for web applications that access database.
- Keep the databases updated.

(xi) Credential reuse

As we know, we should not use same username and password everywhere. But still there are some users who practice this thing. Once attackers have a collection of Username and Passwords (can be easily acquired from number of black market websites), the attacker know there will be the chances of using the same login credentials and there is a chance they will be able to log in. Various password managers are available and are really helpful when it comes to managing the various credentials you use.

Besides these preventive measures, there are various softwares and tools are available that help us to protect from various damages and attacks on the Dark Web. They closely monitor the activities and help us to protect from the negative effect. DarkOwl Vision, Alert Logic Dark Web Scanning, ACID Cyber Intelligence, Cybersprint for risk monitoring are some examples of these softwares.

3.6 The Dark Web and Malware

The dark web market is a spot for the buying and selling of illicit materials. There are number of malicious software and services available over the Dark Web. Users with bad intent are trading these services and making a lot of money out of it. A recent report by Positive Technologies, a security firm, highlights the flourishing Dark Web market. The report is based on 25 Dark Web trading platforms with over 3 million users. Over 10,000 ads were analyzed and interesting results were drawn based on this analysis. Malware plays a vital role in several cyber-attacks. Several types of malware were up for sale, each with varying costs. According to popularity based on the ads found, cryptominers were at the top of the list in popularity. Some of the popular malwares are discussed below:

(I) Data Stealing Trojans

They steal passwords from the clipboard, intercept keystrokes, are capable of bypassing or disabling antivirus software and can also send files to the attacker’s email. A stealer costs about $10. The stolen data gotten by using these stealers can cost a lot more.

(II) Ransomware

Ransomware encrypts your system or files and demands a ransom before decryption. The average cost of getting such malware is $270. Ransomware is a form of malicious attack which will take the control of the system of user and denies the access to that system to the user. There are several different ways attackers choose the organizations they target with ransomware. Some organizations act as tempting targets because they seem more likely to pay a ransom quickly. For instance, medical facilities and government agencies often need immediate access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise suppressed and these organizations may be uniquely sensitive to leakware attacks.

(III) Remote Access Trojans (RATs)

Remote Access Trojans lets an attacker track user actions, capture screenshots, run files and execute commands, turn on the webcam as well as microphone and download Internet files. Popular RATs include: DarkComet, CyberGate, ProRAT, Turkojan, Back Orifice, Cerberus Rat, and Spy-Net. The cost to get one is around $490. Some RATs developed as legal programs for remote management of computers have a monthly subscription that costs around $1000.

(IV) Botnet malware

The prices for malware to create a botnet start at $200 in the shadow market. A full package with server programs and modules will cost $1000–1500. It is a multi-purpose malware that provides proof of how cybercriminals are diversifying their attack methods. The malware comes with ransomware, keylogger and botnet capabilities. Virobot is an example of Botnet Ransomware. After Virobot infects a machine, it becomes part of a spam botnet that pushes the ransomware to more victims. The ransomware encrypts the data on the targeted system via RSA encryption. Meanwhile, the botnet's keylogger feature steals victims' logged data and sends it to the C2 server. Virobot's botnet function uses an infected machine's Microsoft Outlook to send spam emails to all everyone on the user's contact list. The malware is still under development and was first detected on September 17.

(V) ATM malware

These Trojans are used for stealing money from ATMs. ATM hacking is profitable, considering the fact that single fact that single ATM could contain about $200,000. ATM malware prices begin from $1500 and are considered the most expensive of all malwares. Furthermore, a single malware can be used to attack several ATMs.

Exploits identify a system or software's vulnerabilities and takes advantage of them. The exploits listed on the dark web are tailored for multiple platforms. Windows based exploits are most popular, due to a wide market size. In the 2017–2018 period, the average price of an exploit is around $2540. Exploits for the MaCOS family ranged from $2200 to $5300. The charges of Malware Developer start from $500 around. Malware obfuscator could earn about $25 monthly, if on a subscription basis. Malware distributor earns $15 on average.

3.6.1 Best Practices Against Malware Attacks

The following precautionary measure and practices can be followed in order to avoid the Malware attacks.

- *User Education*: It includes:
  - Training users not to download and run any random unknown software on the system.
  - How to identify the potential malware (i.e. phishing emails etc.).
  - There should be security awareness training as well as campaigns.
- *Use Reputable Software*: Suitable A/V installed software will detect and remove any existing malware on a system as well as monitor the activity while your system is running. It is essential to keep it up to date with the vendor's signature.
- *Perform Regular Website Security Audits*: Scanning your organization's website regularly is important for vulnerabilities. As it can keep the organization secure and also protect the customers.
- *Create Regular, Verified Backups*: Having a regular backup can ease you to recover your all the data or any other information in case of any attack or a virus.
- *Ensure Your Network is Secure*: Use of IPS, IDS, Firewall and remote access through only VPN will help to minimize the exposure of organization in case of attack.

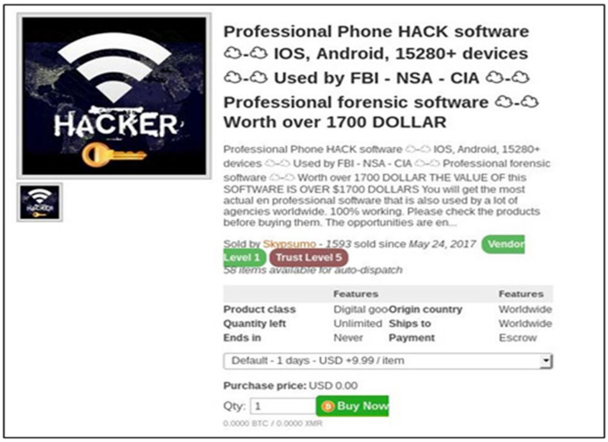
4 Impact of Dark Web on Cyber-Security, Internet Governance and Its Legal Implications

There are number of crimes which take place over Dark Web as discussed in Sect. 3.4. There is huge adverse effect of Dark Web on Cyber Security (discussed in Sect. 4.1). There are number of threats for the cyber security at national and International level [24, 25].

4.1 The Adverse Effect of Dark Web on Cyber Security

In order to characterize the Dark web from a national security perspective, below are some points that detail issues of national security relevance [1].

(i) Sale of Unmanned Aerial Vehicle (UAV) Sensitive Documents: The security researchers at Recorded Future discovered a sales listing within Darknet marketplace



Professional Phone HACK software ☁-☁ IOS, Android, 15280+ devices ☁-☁ Used by FBI - NSA - CIA ☁-☁ Professional forensic software ☁-☁ Worth over 1700 DOLLAR

Professional Phone HACK software ☁-☁ IOS, Android, 15280+ devices ☁-☁ Used by FBI - NSA - CIA ☁-☁ Professional forensic software ☁-☁ Worth over 1700 DOLLAR THE VALUE OF this SOFTWARE IS OVER $1700 DOLLARS You will get the most actual en professional software that is also used by a lot of agencies worldwide. 100% working. Please check the products before buying them. The opportunities are en...

Sold by Skypsumo - *1593* sold since *May 24, 2017* Vendor Level 1 Trust Level 5
58 items available for auto-dispatch

	Features		Features
Product class	Digital goo	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +9.99 / item

Purchase price: USD 0.00

Qty: 1 Buy Now

0.0000 BTC / 0.0000 XMR

Fig. 10 Repurposed US Government zero-day capabilities for sale on Dark Web marketplace

for information of MQ-9 Reaper drone used by US Air Force in 2018. The seller also listed several other documents, including an M1Abrams tank manual and tactics to defeat improvised explosive devices. The seller demanded $150 or $200 for providing classified information. In 2015, *United States Office of Personnel Management* (OPM) announced that it had been a victim of a data breach in which the information contained 21.5 million records. This data was then passed to cyber criminals who attempted to legitimate the stolen data on the forum called “Hell” where the seller’s personal details were mentioned for sale.

(ii) Terrorist Use of Dark Web to Engage in Financing and Weapons Acquisition: Ahmed Sarsur named individual was charged for his attempt to access the Dark Web to acquire weapons and provide financial support to terrorists in Syria by Israeli Authorities in December, 2018. According to the authorities, Ahmed attempt to purchase explosives, hire snipers and provide financial support.

(iii) Zero-Day Exploits: From the national security’s point of view the proliferation of zero day exploits raises many concerns. *Stuxnet,* a malicious computer worm, had potentially delayed the Iranian nuclear program by several years. Figure 10 illustrates how US government zero day exploits have been repurposed by those with malicious intent and monetized on the Dark web.

4.2 Internet Governance and Legal Implications

The tactics must be defined by the government for regulating the Dark Web. These should be defined in such a way that criminal Web activity which takes place over the Dark Web must be suppressed and anonymity of innocent users must be protected to its maximum. The capabilities of different government agencies can be combined effectively to deploy the policies of the Dark Web. Computer and Internet Protocol Address Verifier (CIPAV) is utilized by the FBI to identify the suspects which were disguising their location using

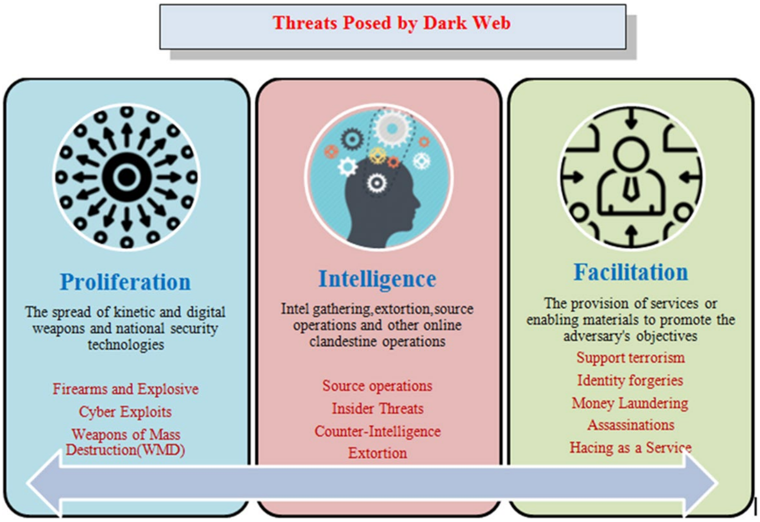

Threats Posed by Dark Web
Proliferation
The spread of kinetic and digital weapons and national security technologies
Firearms and Explosive
Cyber Exploits
Weapons of Mass Destruction(WMD)
Intelligence
Intel gathering,extortion,source operations and other online clandestine operations
Source operations
Insider Threats
Counter-Intelligence
Extortion
Facilitation
The provision of services or enabling materials to promote the adversary's objectives
Support terrorism
Identity forgeries
Money Laundering
Assassinations
Hacing as a Service

Fig. 11 Threats posed by Dark Web

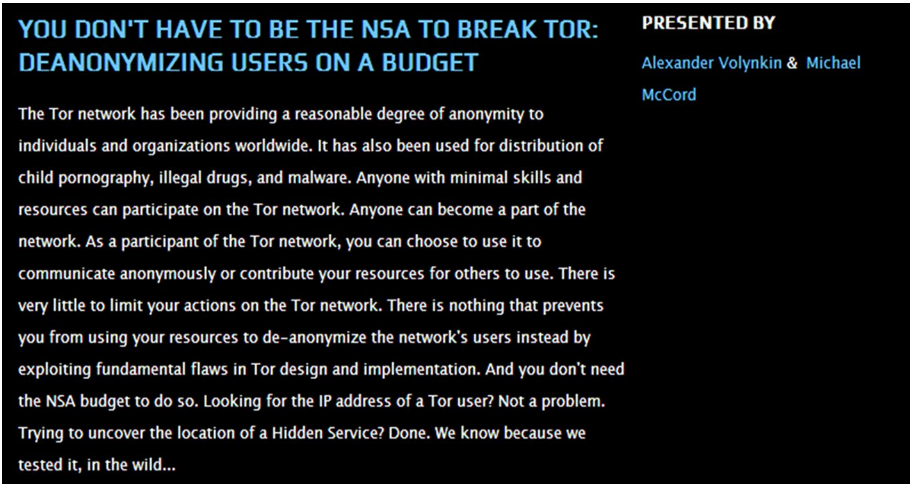
anonymity services or proxy servers [26]. It seperates the regular Internet traffic from TOR traffic. It helps FBI to narrow down the search while doing any investigation. A tool named as "Memex" is developed by Department of Defense's Defense Advanced Research Projects Agency (DARPA) which uncovers patterns to identify the illegal activity. It uncovers only suspects based on specific patterns rather than exposing all kind of users. A hacking tool is also used by FBI to identify the IP addresses of users who were accessing a hidden Tor child abuse site named as Playpen. FBI seized the server of Playpen and transferred the site to an FBI server under a warrant which was issued by a federal magistrate judge in the Eastern District of Virginia in February 2015 [27.

So, there is a need of legal frameworks which are essential in supporting criminal investigations.

There have been number of scenarios which have been reported in the literature which shows the spectrum from ineffective to effective enforcement. Still there is a need to deploy a strong legal framework which can be given to government agenices at National and International level to conduct such kind of investigations successfully.

There are number of threats which are posed by Dark Web as shown in Fig. 11. The following areas need to be monitored for the successful Governance of the Dark Web:

(i) *Mapping the hidden services directory*: The distributed hash table system is used to hide the database in TOR. The deployed nodes could monitor and map the nodes.
(ii) *Customer Data Monitoring*: As there is no such mechanism for customer monitoring, but rather destination requests to track down the top-level domains. This can be done without intruding user's privacy as the destinations of the web requests need to be monitored. For example, The FBI has special tools for going back to *Carnivore* (software to monitor email and electronic communication) in 1997 and before.
(iii) *Monitoring of Social Sites*: This includes monitoring of some popular social sites to find the hidden services.



YOU DON'T HAVE TO BE THE NSA TO BREAK TOR: DEANONYMIZING USERS ON A BUDGET

PRESENTED BY

Alexander Volynkin & Michael McCord

The Tor network has been providing a reasonable degree of anonymity to individuals and organizations worldwide. It has also been used for distribution of child pornography, illegal drugs, and malware. Anyone with minimal skills and resources can participate on the Tor network. Anyone can become a part of the network. As a participant of the Tor network, you can choose to use it to communicate anonymously or contribute your resources for others to use. There is very little to limit your actions on the Tor network. There is nothing that prevents you from using your resources to de-anonymize the network's users instead by exploiting fundamental flaws in Tor design and implementation. And you don't need the NSA budget to do so. Looking for the IP address of a Tor user? Not a problem. Trying to uncover the location of a Hidden Service? Done. We know because we tested it, in the wild...

Fig. 12 Statement published by researchers

(iv) *Monitoring of Hidden Services*: The new services or sites must be captured ("snapshot") by the agencies for later analysis before they disappear quickly or may reappear under new name.
(v) *Semantic Analysis*: There should be a database of hidden site activities and history.
(vi) *Marketplace Profiling*: There should be a tracking mechanism for sellers, buyers and intermediary agents which commit illegals acts. So that one might able to understand what activities a particular buyer has been involved in.

4.3 Law Enforcement in Criminal Investigations

Law enforcement deals with variety of crimes. Initially surface web has been used as a platform to commit crimes or criminal activities. Craigslist and Backpage are the websites which were popular for crimes such as Human Trafficking, robbery and murder. Closure of Backpage by U.S Department of Justice is a great example of active law enforcement. On 4 July, 2014, the TOR project organization has learned about the attack by Carnegie Mellon researchers on the subsystem of the hidden services. Later, it was revealed that the researchers were paid by the FBI. Even the organization put the whole information about the attack on its personal blog including its technical details and suggest its users to update TOR [28]. The following statement was published by the researchers as shown in Fig. 12.

For law enforcement, TOR is most commonly used tool. There are main three activities for law enforcement's use:

- *Online Surveillance*: TOR allows officials to surf web sites and services which are questionable without leaving any traces.
- *Sting Operations*: TOR's anonymity feature allows law officers to engage in undercover operations.
- *Truly anonymous tip lines*: Anonymous tip lines are truly popular. Although a name or email address is not attached to information, server logs can identify them quickly.

4.4 Limitations of the Existing Methods Against Cyber-Attacks Based on the Dark Web

There has been a tremendous rise in the number of dark net listings which are potentialially harmful for the various dimensions based on the report of cyber criminal markets [29]. There are number of limitations which have been analyzed from the literature. Still, there is a need of "heavy-handed" approach in law enforcement to suppress the cyber criminal activities by shutting down sites. Near about 70% of the sellers do not communicate regarding buying the malware over the Internet. They use encrypted messaging applications such as Telegram to take conversations beyond the reach of law enforcement. There is no generic pattern of the malwares or malicious activities as these are customized based on the target and requirement of the buyer. Dark Net vendors also offer the various means to create convincing lures for phishing campaigns using official documentation and genuine company invoices. These genuine official documentation and company invoices can be bought via DarkWeb.

4.5 Future Directions

There are number of future directions in which organizations and users can work in order to protect themselves from such kind of criminal activities which take place over the Dark Web. For organizations, there is a need of deep understanding of the threats which are posed by the Dark Web and those posed by custom remote access Trojans and malwares particularly. Organisations should utilize their ability to use the Dark Web for intelligence gathering by monitoring dark net marketplaces for the trade of company or customer data, malware and for potential brand misuses, such as the sale of spoofed web pages and invoices etc. It has been reported in the literature that the companies are exploring the Dark Web for things like competitive intelligence gathering, recruitment and secure communications. But still there is a danger in exploiting those opportunities, which includes unwittingly collaboration with criminals by giving them access to the own networks. Organisations must adopt layered defence mechanisms which utilizes application isolation to identify threats, as well as having in-depth threat telemetry to stop cyber criminals from getting into corporate networks.

5 Positive Side of Dark Web

One of the report states that 54.5% content on the dark web is of legal government organizations, tech companies such as Facebook, journalists, activists, US State Department, 17.7% constitutes the dead sites. 12.3% is related to drugs trafficking and 1.3% is related to fraud and hacking. Every coin has two sides. It has its own advantages and disadvantages depending upon what a user want to search. Some of the advantages of the Dark Web have been discussed below:

- The biggest benefit of using Dark Web is its anonymity. Not every user who is accessing dark web has bad intensions. Some users may concern about their privacy and security. They want their Internet activity to be kept private.
- The user can find the products cheaper than streets. The vendors also offers discount when the user purchases the product in bulk.
- We can buy the products that are not available in the market or in the country.
- Convenience is another reason why people order on the dark web.
- Due to the existence of strong community on the *Dark Web* the users strongly share their views about products or vendors.
- Dark Web is widely used by those countries which have limited access to the *Clear Net* (surface web). Example, Russia, China and many other countries that use dark web more frequently for many reasons.
- It has its own search engines and secure email browsers.
- Many countries try to contribute in TOR project. US has some laws that are applicable to various activities of dark web. Example, Computer Fraud and Abuse Act (CFAA) bans unauthorized access, damaging computers, trafficking etc. Russia has made efforts to de-anonymize TOR for political reasons. China tries to block the access to TOR.

6 Some Interesting Facts About Dark Web

- Dark web is a huge marketplace for criminals and is said to generate at least $500,000 per day.
- A study done in 2001 by University of California discovered that dark web had 7.5 PB of information.
- Users use mostly Bitcoins because they are virtually untraceable.
- ISIS has been using the dark web as propaganda, recruiting and fund raising tool.
- Intelligence agencies like NSA have been using software like XKeyscore to know the identity of TOR users.
- Besides all the illicit stuff there is *book fan club* also. The founder of Silk Road also started a book bazaar on it. The book fan club usually has conspiracy theory books and banned books.
- There is a network called '*Strategic Intelligence Network*' with tons of information about how to survive with any crisis.
- According to Israeli intelligence firm Six gill criminals were discovered selling fake degrees, certifications and passports.
- People hired hackers to break into University systems and change grades.
- There is no doubt that dark web is full of scams. 80% of web traffic relates to child pornography.
- It contains nearly 550 billion individual documents.
- Over 30,000 websites were hacked every day.
- All types of match fixing and illegal betting take place over Dark Web.

7 Conclusion

Darkweb is a part of the Internet which is usually used by the users to do some activity in a hidden manner without leaving any traces. It has become a hub of criminal activities like child pornography, arms trafficking, drug trafficking and onion cloning etc. The main reason of these activities is the anonymity which is provided over this platform. There are number of attacks which are launched over this platform and the ransom amount is taken in the form of bit coin over the Dark Net. It is also used by governments of the different countries for the sake of confidentiality. An overview of the different attacks, exploit, browsers and crimes of Dark Web. It can be concluded that the pros and cons of Dark Web depend upon the intentions of the user.

References

1. Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal Cyber Policy, 2*(1), 26–38.
2. Ciancaglini, V., Balduzzi, M., & Goncharov, M. [Online]. Retrieved December 20, 2019, from https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor.
3. Mirea, M., Wang, V., & Jung J. (2019). The not so dark side of the darknet: a qualitative study. *Security Journal, 32*, 102–118.
4. Mirea, M., Wang, V., & Jung, J. (2018). The not so dark side of the darknet: A qualitative study. *Security Journal, 32,* 102–118.

5. Çalışkan, E., Minárik, T., & Osula, A.-M. (2015). Technical and legal overview of the tor anonymity network. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.
6. "PGP Encryption." [Online]. Retrieved December 16, 2019, form https://www.technadu.com/pgp-encryption-dark-web/57005/.
7. "Onion Routing." [Online]. Retrieved December 16, 2019, from https://www.geeksforgeeks.org/onion-routing/.
8. "Types of Relays." [Online]. Retrieved December 14, 2019, from https://community.torproject.org/relay/types-of-relays/.
9. "TOR Nodes List." [Online]. Retrieved December 20, 2019, from https://www.dan.me.uk/tornodes.
10. "Welcome to the Tor Bulk Exit List exporting tool." [Online]. Retrieved December 20, 2019, from https://check.torproject.org/cgi-bin/TorBulkExitList.py.
11. "Relay Search." [Online]. Retrieved December 16, 2019, from https://metrics.torproject.org/rs.html.
12. Rudesill, D. S., Caverlee, J., & Sui, D. (2015). The deep web and the darknet: A look inside the internet's massive black box. Ohio State Public Law Working Paper No. 314.
13. Naseem, I., Kashyap, A. K., & Mandloi, D. (2016). Exploring anonymous depths of invisible web and the digi-underworld. *International Journal of Computer Applications, NCC*(3), 21–25.
14. Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy, 24*(5), 385–391.
15. Foltz, R. (2013). Silk road and migration. In: *Encyclopedia of global human migration*. https://doi.org/10.1002/9781444351071.wbeghm484.
16. Lacson, W., & Jones, B. (2016). The 21st century Dark Net market: Lessons from the fall of silk road. *International Journal of Cyber Criminology, 10*(1), 40–61.
17. Finklea, K. (2017) Dark web report published by Congressional Research Service.
18. "Types of Attacks." [Online]. Retrieved December 16, 2019, from https://www.rapid7.com/fundamentals/types-of-attacks/.
19. Cambiaso, E., Vaccari, I., Patti, L., & Aiello, M. (2019). Darknet security : A categorization of attacks to the TOR network. In: *Italian Conference on Cyber Security*.
20. Evers, B., Hols, J., Kula, E., Schouten, J., Toom, M. den, Laan R. M. van der, Pouwelse J. A. (2015). "Thirteen years of tor attacks". [Online]. https://github.com/Attacks-on-Tor/Attacks-on-Tor. Accessed 18 Nov 2019.
21. Nasr, M., Bahramali, A., & Houmansadr, A. (2018) "DeepCorr : Strong flow correlation attacks on tor using deep learning". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1962–1976).
22. Zillman, M. P. (2015). *Deep Web Research and Discovery Resources 2015*.[Online]. Available: https://www.llrx.com/2019/01/deep-web-research-and-discovery-resources-2019/. Accessed 15 Nov 2019.
23. "Distributed Denial of Service Attack." [Online]. Retrieved March 18, 2019, from http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=2&time=16438&view=map.
24. Schäfer, M., Fuchs, M., & Engel, M. (2019). BlackWidow : Monitoring the dark web for cyber security information. In: *Proceedings of the 11th international conference on cyber conflict (CyCon)*, 1–21.
25. Chertoff, M., & Simon, T. (2015). *The impact of the dark web on internet Governance and cyber security" Global Commission on Internet Governance*. Paper Series No. 6.
26. "Dark Web." [Online]. Retrieved November 15, 2019, from https://www.fas.org/sgp/crs/misc/R44101.
27. Satterfield, J. "FBI Tactic in National Child Porn Sting under Attack." [Online]. Retrieved November 20, 2019, from http://www.usatoday.com/story/news/nation-now/2016/09/05/fbi-tactic-child-porn-stingunder-%0Aattack/89892954/.
28. "Confirmation Attack." [Online]. Retrieved December 10, 2019, from https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack.
29. Ashford, W. "Firms face targeted bespoke cyber attacks, dark web study reveals." [Online]. Retrieved December 10, 2019, from https://www.computerweekly.com/news/252464660/Firms-face-targeted-bespoke-cyber-attacks-dark-web-study-reveals.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Shubhdeep Kaur is pursuing her Master's in Computer Science from Thapar Instituite of Engineering and Technology, Patiala, Punjab, India. Her research interests include security, metasploit framework and security issues in IoT. She is an active researcher in field of security and has number of certifications and reputed publications in this field. She received B.E. degree in Computer Science and Engineering from Chandigarh University, Gharuan, Punjab, India in 2017. She had done Diploma in Computer Science and Engineering from R.I.M.T Polytechnic College, Mandi Gobindgarh, Punjab, India in 2014.

Sukhchandan Randhawa received Doctorate degree in Wireless Sensor Networks from Thapar University, Patiala, India. Sukhchandan received M.E. degree in Computer Science and Engineering from Thapar University, Patiala, India in 2012. She received B.E. degree in Computer Science and Engineering from Chitkara Institute of Engineering and Technology, Rajpura, Punjab, India in 2010. She had done Diploma in Information Technology from Thapar Polytechnic, Patiala, India in 2007. Her research interests are focused on Wireless Sensor Networks, power efficiency, network security data aggregation and load balancing algorithms in Wireless Sensor Networks and Data Analytics. She has joined Thapar University as Lecturer in 2012 and currently working as Assistant Professor. She is active researcher in field of Wireless Sensor Networks and Cloud computing and has number of publications in SCI, SCIE, Scopus Indexed journals and International Conferences. She is also reviewer of some highly reputed SCI journals and IEEE International Conferences.