The Dark Web:
Hidden Access to Internet Today

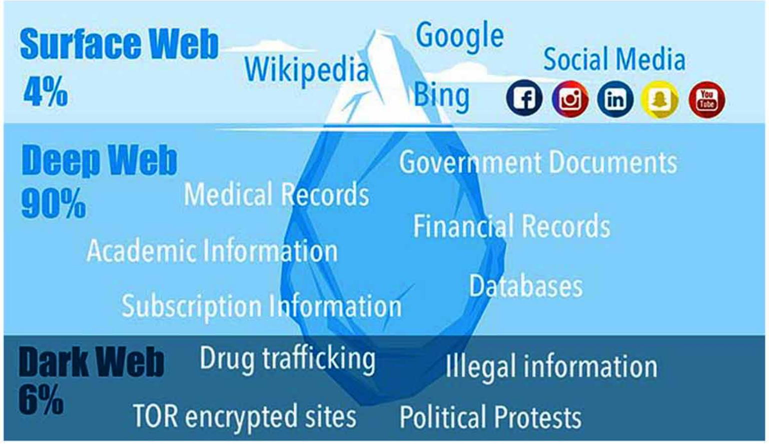
Ramanujam Elangovan
https://orcid.org/0000-0003-1450-9097
Thiagarajar College of Engineering, India

INTRODUCTION

Internet is a hardware asset consists of multiple nodes where each node is a server/ client systems such as laptops, computers, etc. In earlier days, the data are transferred or shared using the Internet. In 1994, Berners-Lee et al introduced web in which the data are accessed through hyperlink text or web pages. Web is software which runs over the internet to provide the service to users. Only 4-6% of the whole web or the web pages (surface web) are indexed in search engines such as Google, yahoo, etc. However, web which is not indexed in search engines is 400 times larger than surface web also known as deep web. The deep web (Bergman, 2001) can only be accessed through a special link or with special permission to access the data in the cloud or specialized servers which cannot be found on any of search engines. Government sectors, private bank data, cloud data, etc are examples of the deep web. The data in the deep web are so sensitive and private which are to be kept in secret. These data are allowed to access only by specific people. There is a subset of deep web termed as dark web (Chen et al, 2008). Figure 1 shows the difference of Surface web, Deep web and Dark web.

Dark web allows a user to host a website on a specific network termed as dark net which remains anonymous always. The network used by the user to maintain anonymity is dark net. Dark net is a network build over the internet which is completely encrypted. Traditionally, when a user visits any sites,

Figure 1. Difference of surface web, deep web and dark web
Source: LeMacnalle



DOI: 10.4018/978-1-5225-9715-5.ch008

they are tracked via their Internet Protocol (IP) address. However, the dark net maintains privacy through specialized anonymity software and configurations to access. One such dark net is Tor ("The Onion Routing" project) (Dingledine et al, 2004).

TOR AND DARK WEB

The TOR architecture provides two basic services – anonymous browsing and hosting of anonymous information exchanges. These services are provided by one piece of special software – 'Tor Browser'. There is no special technical requirement for these services to be bundled. Indeed, browsing is more popular than hosting. No Tor users have visited any hidden website at a *.onion address. Most probably, all the users merely use Tor browser to browse the internet's conventional address space more securely. For example, Mary, who lives in a small town, wants to buy a pregnancy test but doesn't want to be seen doing so by the shop owner. Peter, a friend of Mary's father, wears a mask, walks detours and pay in cash. Peter will not be able to identify or trace. Also, Mary's privacy and anonymity are assured. Anonymous browsing is not actually a part of 'dark web', but it is a legitimate and impressive service provided by Tor. The underlying purpose was to create a distributed, anonymous easily deployable and encrypted network to be used by those who needed it. Specifically, it was offered as a free service to promote unfettered access to the internet in locations where online censorship was heavily enforced. Chaum in 2003 provided a way for this access through onion routing. In order for a user to access the website securely, the person has to be routed through a series of intermediary servers. The resulting pathways between servers were labeled 'circuits'. Each packet of information to be relayed over the network would be encased in multiple layers of encryption, each to be sequentially peeled away only by the subsequent node in the circuit. Consequently, intermediary nodes could only decrypt one layer of the encryption, preventing access to the underlying data and its originator. The final such hop – or exit node – would reveal the original packet and proceed to deliver it to the desired destination, thus protecting the sender's identity. As a result, intercepting and decoding the information along its path would be significantly harder – albeit not impossible – to accomplish. The dark web attracted the people who do illegal stuff such as trade, forums, media exchange for terrorists, etc. without getting caught. "Silk Road" is a dark web site which is used to sell drugs and was taken down already by FBI (Cubrilovic, 2014). Friend-Friend and Free net is also a dark web provided by darknet used to transfer file anonymously.

THE SIZE OF THE DARK WEB ECONOMY

The dark web, an ocean of illicit activity often carried out by persons to trade stolen data, dollars, etc. In 2016, the economist reported that usage of dark web by drug side grew from $15 in 2012 to approximately $225 million in 2019. On estimating the world economy, the dark web has frustrated every attempt of money and other information transactions. In the year 2023, the dark web cybercrime will be an increase of 175% increase as reported by Juniper research. Dark web is increasingly used by hackers like hire, hitmen and other service providers who can't advertise over traditional channels. Also, the year 2017 has been recognized as the most notorious year for selling ransomware for Dark web. Even a casual news consumer can feel the ransomware attacks cost an estimated worldwide business of $1 billion this