The Dark Web and the Role of Secure Human Behaviors

Dark web concepts are helpful for preserving the privacy and security of its users. These hidden corners of the Internet provide anonymity for people who are oppressed by their governments, free speech to journalists, and secure communication channels for the layman and the expert alike. These are a few ways the dark web is being used for ethical purposes.

For example, The Onion Router (Tor) is a specially configured version of the Firefox web browser, which routes users browsing traffic through the Tor anonymous network, making it difficult to track a user's actual Internet Protocol (IP) address. Tor provides its users anonymous communication capabilities when used as recommended by the Tor project. This free tool was developed to provide anonymity for its users through multilevel encryption and proxy connections throughout the world. There are several popular dark web gateways including, but not limited to:

- Tor, again, is the most popular and easiest of all dark web gateways that support multiple platforms such as Android.
- ZeroNet was developed based on blockchain technology and a decentralized network model to give each user power over their instance of the platform.
- Invisible Internet Project (I2P) was developed to provide secure messaging capabilities using garlic routing and method drives from onion routing.
- Freenet is another highly encrypted, decentralized platform that provides capabilities for its users for secure and private communications.

It is important to spread awareness of dark web concepts by educating the community on understanding well-known gateways and the role secure behavior plays in the ethical or malicious use of these concepts.

Background

Dark web concepts are often discussed without context. This is mainly because the concepts are

Babur Kohy
Is an accomplished cybersecurity professional in cyberdefense, cloud security, threat/risk management and organizational resilience. He lectures extensively on deep and dark web techniques for the identification and exploitation of dark net gateways to enhance personal security and anonymity. He is the ISACA® academics director for the Greater Washington DC Chapter. He is the founder of CyTalks.com, a platform for cybersecurity training and discussions.

Warren D. Holston
Is a technical operations officer and has worked in the intelligence and defense industry, including at the US Department of Defense (DoD), for more than 30 years. He has served as a US Navy explosive ordnance disposal diver, a collection officer and senior manager at the US Central Intelligence Agency (CIA), and a subject-matter expert for the US DoD Special Operations Command. He has managed and conducted counterterrorism, covert action and technical collection operations worldwide and has contributed significantly to the national security of the United States.

Ibrahim Waziri Jr., Ph.D.
Is a senior manager with Microsoft Azure Government Engineering working on cloud security compliance engineering and automations. He is also an adjunct professor of cybersecurity at Marymount University (Arlington, Virginia, USA). His research focuses on cloud infrastructure security; virtualization and hypervisors; identity and access management; network security; robotics process automation (RPA); open-source intelligence (OSINT); secure digital development policies; and cybersecurity governance, risk management and compliance (GRC) strategies and policies. He has more than a decade of working experience within the industry, including in US federal and national security agencies in the defense, intelligence, treasury, international trade and health sectors.
misunderstood and misrepresented. It takes research, practical experience and hands-on investigation to really understand what the dark web is.

The dark web most often makes headlines regarding breached data and illegal activity such as buying or selling drugs, pornography, financial data dumps, and selling or trading weapons. The dark web also serves as an anonymous communication platform to many in oppressed regions of the world. In fact, the layered networking and encryption concepts used for the dark web today were developed to promote anonymity at the US Naval Research Lab (NRL) in the 1990s. The well-known and most widely used of all gateways, the Tor browser, reported an average of 2 million users in November 2020.

For the purposes of this discussion, the web can be categorized into three main categories:

1. **Surface web**—This is open access to anyone with an Internet connection and a web browser.
2. **Deep web**—This refers to any website that cannot be readily accessed through any conventional search engine such as Google or Yahoo. The concept is used by businesses, academia, governments, and anyone who stores information that requires authentication and authorization. It is estimated that the deep web could be 500 times bigger than the normal web. This assumption comes from the fact that most of the content on the web is hidden behind some type of a gate and requires a key, such as a username and password, to access it.
3. **Dark web**—This is a series of private portals running either on the open Internet backbone or on a private network that is not indexable to search engines. Governments, law enforcement professionals, activists, researchers, journalists and oppressed populations use the dark web for secure, private communications and anonymous searching. However, it is also used for illegal activity.

---

**Early Days of Connecting Computers**

The concept of connecting computers started in the late 1960s with the development of the Advanced Research Project Agency Network (ARPANET), a US Department of Defense (DoD) project. The purpose of this project was to connect the DoD-funded research and development institution computers to optimize communication and streamline information sharing. The United States developed this network of decentralized computers during the Cold War to make it impossible for the enemy to attack one central location to take out all communications systems in case of escalating of hostilities. The development and launch of the ARPANET digitized communication and information sharing between multiple DoD locations, which enabled agencies to share information like never before to aid them with their missions. Within a few years, a network of isolated and secretive connections began to appear; some of which were called the “darknets” or “dark web.”

**Dark Web Gateways**

There are four decentralized gateways: ZeroNet, FreeNet, Tor and I2P.

**ZeroNet**

ZeroNet is a newer gateway that uses bitcoin cryptography and the BitTorrent network. The platform user interface is modern and has many features such as the capability for email, message boards, web hosting and blogging, as shown in the ZeroNet landing page in figure 1. The network is completely decentralized, similar to blockchain technology concepts. Even though it is highly encrypted, that does not mean it is foolproof. Users need to be proactive and exercise good judgment by ensuring that they are not oversharing personal information, and their connections are further secured by turning on the Tor relay feature before engaging with the platform. Without critical thinking, good behavior and a well-developed plan, users can get entangled in unsecure and compromising situations very quickly.
FreeNet

FreeNet is a free program that lets users anonymously browse the web, share files and chat on forums no matter where they are located. With FreeNet, users can browse websites, post on forums and publish files within the network with strong privacy protections. The developers of the platform describe it as censorship resistant, which means it is not completely censorship proof.

Because the gateway is not censorship proof, it is vital for users to practice good behavior when investigating this gateway. Behaviors such as reading platform documents, understanding network communication security, and testing the capabilities between dark web and surface web configurations enhance the user experience and reduce the risk of being identified. The platform can be used successfully and with the utmost privacy as long as the user has a good plan of action before downloading and using.

Tor

Tor can help users defend against tracking and surveillance and circumvent censorship. Tor is arguably the easiest gateway to download, install, configure and use. This is mainly because most people are accustomed to using browsers to access the Internet. Dark web sites through Tor requires a .onion address for access. Tor uses a relay system for encryption with a minimum of three relays before the user exits the network and enters the Internet. This reduces the chance of attribution by anyone monitoring the network.

Even with all the technical capabilities Tor provides, it cannot protect the user from bad behavioral habits. The key to effective use of Tor is to practice sound cyberhygiene and follow the Tor project rules carefully. For example, Tor project has many recommendations on what not to do with the browser, and these recommendations should be closely followed. Historically, technology has not
highly secure encryption and routing makes the network extremely slow. The only way to investigate this platform securely is to practice secure behavior such as patience, critical thinking and fact-based investigation. Without good behavior and a solid plan of action, this platform has the potential to get the user in trouble quickly.

Governing the Dark Web

It is extremely difficult to govern the dark web, portals and networks, because the concepts were developed with decentralization and peer-to-peer encrypted connections. Decentralized means there is not a single repository of registered domains, no single point of failure, complex networks of proxy servers and single-key encryption. Since each user has control over the domain they deploy on the dark web, they avoid participating in any form of governance. Further, multiple layers of encryption are applied using private encryption keys. The use of bulletproof hosting providers further strengthens the user’s

Figure 2 illustrates Tor browser use and the number of relays (hops) Tor uses before getting the user to its intended website (e.g., Google). The same action is done twice using two separate browsing sessions to showcase relay changes each time a site is requested.

I2P

The I2P network provides strong privacy protections for communication over the Internet. This gateway is set up as a peer-to-peer network where users can launch websites, start forums, and send and receive encrypted emails. Even though some features are similar to other gateways, the platform is much slower in performance than any other. Users need to ensure that the network is up and running for many hours before they can access the data. The

Figure 2—Tor Browsing Sessions Illustrating How Relay Changes
privacy and security because these domain service providers are more lenient with users about the types of content hosted or shared. Bulletproof hosting providers do not usually answer to government requests and do not share information about their customers. Decentralization, layered encryption and bulletproof hosting provide the user better control over their data and communications.

Conclusion

Dark web concepts have been around for decades providing security, privacy and anonymity to its users. There are multiple gateways to access the dark web such as Tor, Freenet, ZeroNet and I2P. Each of these are layers that operate on top of the Internet, enabling peer-to-peer networking. Dark web networks are highly decentralized and use advanced encryption during communication. Decentralization and advanced encryption make it extremely difficult to govern the dark web. Secure behaviors, having a plan of action and critical thinking are keys to success while operating in the gateways. This research can be expanded on by researching governance, ethical vs. malicious use, content analysis for each individual gateway, and by resolving identities relating to the dark web.

Endnotes

1 Greenberg, A; “How to Use Tor and Go Anonymous Online,” Wired, 9 December 2017, www.wired.com/story/the-grand-tor/
3 The Tor Project, Inc., “History,” www.torproject.org/about/history/
4 Tor Metrics, “Users,” www.metrics.torproject.org/userstats-relay-country.html
5 Sheils, C.; “Enter the Deep and Dark Web if You Dare (and Get Ready for a Surprise),” Digital.com, 5 August 2020, digital.com/online-privacy/deep-dark-web/
9 Ibid.
12 Freenet, https://freenetproject.org/index.html
13 The Tor Project: Privacy and Freedom Online, https://www.torproject.org/
14 Invisible Internet Project, https://geti2p.net/en/about/intro