

Introduction

There's another Internet web riding along with the one we normally see. It's called the Deep Web, a system of overlay networks that use the Internet infrastructure but require specific software, configuration and allowed access or authorization to use. The Deep Web has a number of uses for business but is especially useful for hackers and cybercriminals. The Deep Web is not indexed and lies beyond the reach of conventional search engines. Therefore, these deep websites are not a part of "clearnet" search results. There may be 500 times more content in the Deep Web than there is in the conventional web.

Credit: Jeff Kabachinski

<http://1technation.com/tech-savvy-dark-side-onion-router/>

The Dark Web

The Dark Web is a small part of the Deep Web. The also un-indexed Dark Web uses protected or encrypted traffic. It's a place where cybercriminals conduct their trade and legit businesses may conduct transactions. Mainly, however, the protected Dark Web is a supermarket for illicit and illegal activity. It's a place for hackers and cyber criminals to conduct business – selling credit card information, electronic health care records and illegal drug transactions.

TOR

One of the main enablers of the Dark Web is "The Onion Router" known as TOR. An onion router system has several encryption layers intended to hide the message's source and destination addresses. (See fig.1). Like an onion, TOR has several layers as shown in the figure. As web privacy continues to erode, TOR promises to maintain free speech and thought. Onion routing is a process for anonymous communication. TOR uses layers of encryption and a series of onion routers.

As shown in the figure – the source of the communication sends the onion to Router A. Router A then determines where to send it next by removing the first layer of encryption. Router A also sees the source address but does not know if it is the address of origination. Router A sends the remaining data to Router B. Router B removes another layer of encryption to find out where to send it next (Router C). Router C decrypts the last layer to send the data to its final destination.

Like a VPN, the secured pathway or tunnel lets users browse to public and secured Dark Web sites without conceding delicate information like IP addresses, cursor movement, your location, and other personal data stored in cookies. TOR helps to prevent deep packet analysis, and protects website data payload and header information.

TOR Router

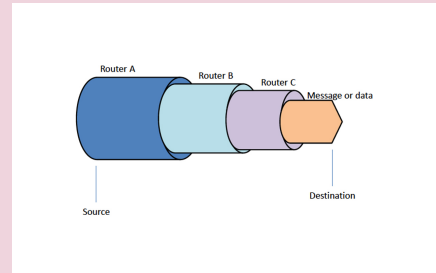


Figure 1

Major Dark Web Uses

- **Botnets:** a network of infected computers with malware that controls a group of private computers without the owners' knowledge. The allocated bot may send spam email messages or with hundreds or thousands of other bots hit a website to the point where 'denial of service' is obtained, essentially shutting it down.
- **Bitcoins:** digital currency where encryption is used to control and regulate the creation of currency units. It also used to validate the transfer of funds, operating independently of a control mechanism like a central bank.
- **Darknet market:** Or "cryptomarket" is a commercial website that operates using TOR.
- **Hacking groups & services****
- **Fraud services:** example cash register hacking that programs the cash register to send credit and debit card information back to the hacker.
- **Hoaxes & unverified content**
- **Phishing & scams**
- **Illegal and ethically disputed pornography**
- **Illegal animal trade**
- **Terrorism**
- **Protected social media**
- **Journalism:** where journalists report and record their findings in private
- **The Silk Road:** was known as a large enterprise on the Dark Web, it included:
 - Secret eBay mostly for illegal drugs
 - Special cryptographic software
 - Anonymous interface & traceless payments
 - Connecting thousands of drug dealers with millions of users
- **Organizations that want to protect** their most confidential information.
- **Multi-national organizations that communicate in places that have fluctuating levels of legal privacy protection.**
- **Government groups (military) that operate in struggling geographical areas that censor web use.**



By **David Pollack** (Davidpol)
cheatography.com/davidpol/

Published 5th April, 2017.
Last updated 5th April, 2017.
Page 1 of 2.

Sponsored by **Readability-Score.com**
Measure your website readability!
<https://readability-score.com>

Major Dark Web Uses (cont)

- **Reporters & whistleblowers** that need anonymity and private communication to hide their identity.

- **General consumers concerned about protecting personal privacy.**



By **David Pollack** (Davidpol)
cheatography.com/davidpol/

Published 5th April, 2017.
Last updated 5th April, 2017.
Page 2 of 2.

Sponsored by **Readability-Score.com**
Measure your website readability!
<https://readability-score.com>