Dark Web

Overview

You may have heard the term "Dark Web" used by others or in the media and wondered "*what is the Dark Web*?" or "*should I be doing anything about it*?". Today we explain what the Dark Web is and what it means to you.

What Is It?

The Dark Web consists of systems on the Internet designed for communicating or sharing information securely and anonymously. There is no single "Dark Web"; it is not something like Facebook where it's run by a single organization. Instead, the Dark Web is collections of different systems and networks managed by different people used for a variety of purposes. These systems are still connected to and are part of the Internet; however, you will generally not find them using your normal search engines. You often also need special software on your computer to find or access them. One example is the Tor Project. To access this Dark Web, you download and install the Tor Browser. When you connect to web servers using the Tor Browser, your encrypted traffic travels through other computers also using Tor. As it hops through these computers, the source IP address is changing—meaning that when you get to the web site, your online activity is anonymized. Other examples of Dark Webs include Zeronet, Freenet, and I2P.

Who Uses It?

Cyber criminals are big users of the Dark Web. They maintain websites and forums in the Dark Web to enable their criminal activities such as purchasing drugs or selling gigabytes of hacked data—all anonymously and securely. For example, when a cyber criminal hacks a bank or an online shopping store, they steal as much information as they can, then sell that information to other cyber criminals on sites in the Dark Web.

There are also legitimate uses of the Dark Web. For example, people in countries where censorship is rampant can use Dark Web networks to share information and see what else is happening in the world while protecting their privacy and remaining anonymous. Journalists, whistleblowers, and privacy-minded people can use the Dark Web to increase their anonymity and

bypass censorship. In addition, individuals like these can use technologies like the Tor Browser not only to access the Dark Web, but anonymously browse the regular Internet.

What Should I Do?

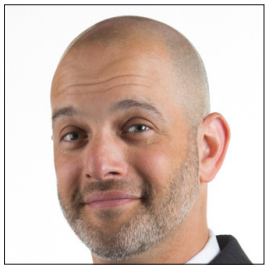
Unless you have a specific reason to access the Dark Web, we caution you against it. Some Dark Web sites are used for illegal purposes; many of the sites will use your computer in a peer network to accomplish their goals, and in some cases your computer may even be probed or attacked. Some companies offer monitoring services to let you know if your name or other information has been stolen by cyber criminals and found on the Dark Web. The actual value of these services is questionable. The best way to protect yourself is to assume some of your information is already in the Dark Web being used by cyber criminals. As a result:

- **Be suspicious of any phone calls or emails pretending to be an official organization and pressuring you into taking an action, such as paying a fine. Criminals may even use information they found about you to create a personalized attack.**
- **Monitor your credit card and bank statements; perhaps even set up daily alerts on any transactions that happen. This way you can detect if any financial fraud is happening. If you do detect it, report it to your credit card company or bank right away.**
- **Put a freeze on your credit score. It does not impact how you can use your credit card and is one of the most effective steps you can take to protect yourself from identity theft.**

Subscribe to OUCH! and receive the latest security tips in your email every month - www.sans.org/security-awareness/ouch-newsletter.

Guest Editor

Micah Hoffman *(@WebBreacher) is the Principal Investigator at Spotlight Infosec LLC, a Certified SANS Institute Instructor, and the author of the SANS OSINT courses. Micah's passion for cyber and open source intelligence shows in his projects, courseware, and teaching style.*



Resources

Personalized Attacks:	https://www.sans.org/u/RfW
Social Engineering:	https://www.sans.org/u/Rg1
Identity Theft:	https://www.identitytheft.gov
Credit Freeze:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor Browser:	https://www.torproject.org/
SANS OSINT Course:	https://sans.org/sec487