WINTER 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their cybersecurity, computer forensics and e-discovery needs. For this E-Newsletter, we shine light on the Dark Web and the information security, legal and financial impact it has on organizations.

Demystifying the Dark Web

Imagine the Dark Web as an alleyway cloaked by the night: you don't want to be there without protection, especially if you'll be surrounded by criminals. An unnerving prospect for sure. So, why and how should one access the Dark Web? This article explores the technical aspects of accessing the Dark Web and provides tips on how to safely (or somewhat safely) dive deep into the shadows.

Dark Web sites, known as “hidden services”, end with ".onion", which is a special-use top level domain suffix. The suffix is derived from a software project originally launched by the US Naval Research Laboratory to enable anonymous communication, The Onion Router or Tor. Tor works by encrypting data within the application layer of a communication protocol. Such data, including the content of the message and the originating and destination IP addresses, are encrypted in multiple layers and routed through a randomly constructed virtual circuit of nodes within the Tor network (hence, the “onion”). Each node decrypts only the destination of the next node in the virtual circuit, ending with an exit node that ultimately displays the message or points to a destination. Theoretically, these encryption layers maintain zero knowledge of the originating IP, and therefore, determining who initiated such request is *near* impossible (vulnerabilities do exist in Tor, especially if a bad actor controls the exit node).

Although Tor obscures the computers and networks, it is crucial to note that the data transmitted and received is eventually unencrypted. Thus, if such data includes identifying information, the goal of anonymity is foiled. Beyond the content of transmitted and received messages foiling anonymity, settings within the Tor software and how and when it is used on a device can also impact anonymity. Furthermore, the stability of the Tor network, which consists of nearly 7,000 volunteers providing free bandwidth, can also result in error messages that provide identifying

information. Below are two best practices for accessing the Dark Web that will eliminate certain pitfalls in the configuration and use of Tor:

- *Instead of using your organization's computer or personal computer, use Tails.* Tails is a USB bootable operating system with baked in privacy features including Tor. This will minimize the risk of network errors retrieving identifying information.

- *For browsing, download the Tor Browser Bundle and use the default configurations*. The Tor Project funds research and developers that focus on emerging vulnerabilities, and seeks to update and configure the software to protect its users.

Ultimately, Tor can be used to defend against traffic analysis and keep business and personal communications and browsing activity confidential from surveillance activities. For those interested in the Dark Web, but not confident enough to venture into the darkness, much can be learned from Surface Web sites, such as DeepDotWeb.com, which tracks newsworthy developments happening on the Dark Web.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

February 2017
The Sedona Conference Institute 2017 eDiscovery Negotiation Training
Miami, FL: February 8-9, 2017

RSA Conference
San Francisco, CA: February 13-17, 2017

March 2017
The 11th Annual Sedona Conference Institute Program on eDiscovery:
Discovery in a Dynamic Digital World
Houston, TX: March 2-3, 2017

ABA TECHSHOW 2017 Conference and Expo
Chicago, IL: March 15-18, 2017

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: