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.

Combatting the Dark Web

A typical static Dark Web site, such as a bulletin board, provides its visitors with URLs to both legitimate and nefarious Dark Web domains. The inclusion of said nefarious URLs raises the question of should the bulletin board site be targeted for a takedown operation or only the nefarious site? And how does an organization concerned about content on a Dark Web site, including valuable intellectual property or its customers' and employees' personal information, accomplish such a task?

A fundamental challenge is that Dark Web site administrators operate within frameworks (technical and ideological) that are not aligned with typical business norms. For example, the Digital Millennium Copyright Act provides procedures for copyright owners to serve takedown notices to site operators when copyright owners believe sites (or their users) are violating its copyrights. In the case of a "hidden service," which is the term used to denote a Dark Web site, it is difficult to locate the operator and provide notice of copyright violations; and even if the operator is tracked down, it's not likely such a notice will result in a takedown by the site operator of the hidden service.

On December 1, 2016, however, the US Supreme Court enacted procedures permitting magistrate judges to issue warrants to unearth and copy data through the seizure of media or by *remotely accessing and copying* such data, so long as the data "…has been concealed through technological means" or involves an "…investigation of a violation of [the Computer Fraud and Abuse Act]". Although championed by the US Department of Justice, this amendment is unprecedented in the reach it provides to the government. Notably, even certain data transmitting on the Surface Web is “concealed through technological means”.

For organizations, the importance of the December 1, 2016 amendment to Rule 41 of the Federal Rules of Criminal Procedure is that as business operations increasingly require confidentiality

and security and organizations utilize technology to facilitate increased security, the US government, as well as foreign governments that pass copycat legislation, will have proper legal footing to hack organizations' networks where "activities related to a crime *may* have occurred...". Until now such sweeping powers were not permitted, and government agencies had to rely on "old-fashioned" investigative techniques and human sloppiness to catch bad actors on the Dark Web (like the infamous 2013 takedown of Ross Ulbricht, former operator of the crypto market the Silk Road, who's now serving life in prison). Though the impact of this amendment has yet to be widely felt, for better or for worse, it will certainly become an often-used tool for illuminating 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: