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.

What Lies Beneath:
The Risk of the Dark Web for Your Organization

The Internet consists of interconnected computer networks utilizing common protocols to link devices worldwide. This web of connections enables near instant transmission of data, allowing users to harness its incredible power for good and evil. Notably, the *Surface Web* (publicly accessible sites, crawled, scraped, and indexed by search engines like Google), the *Deep Web* (privately accessible sites, such as corporate networks that require credentials), and the *Dark Web* (sites that are technically designed to limit access and detection, requiring special, albeit freely-available, software) all exhibit elements of good and evil. This article, however, explores the dark web's participants, activities and growth, as well as highlights why prudent organizations and their legal counsel must understand the risks and possibilities in a dark-web world.

Surfing the Dark Web: the Who and the What

The modern lexicon associates darkness with badness, and the Oxford English Dictionary defines badness as: “a lack of or failure to conform to moral virtue; wickedness; evil”. Although objectively "bad" things certainly exist on the Dark Web, many participants make legitimate use of it. Journalists rely on the pseudonymity of the Dark Web to safely report stories. Book club participants utilize the protection afforded by the Dark Web to discuss marginalized political, financial, societal, and even sexual ideologies. The line between legitimate and nefarious uses is quite blurry, especially because categorization depends on the perspective of the observer. Inherently, the Dark Web challenges those who seek to reduce potential harms caused by Dark Web activities and content, because there are no *clear* paths back to the source. Tracking sources of activity and content requires cyber forensics experts, such as Digital Mountain, and can also require coordination with law enforcement agencies.

Illegitimate content currently residing on the Dark Web includes data dumps of sensitive records and intellectual property of corporations, law firms, and government agencies, as well as hacked data repackaged and available for purchase with digital currency through online marketplaces such as AlphaBay, Dream Market and Crypto Market. Cyber criminals sift through hacked data sets and repackage into files for purchase, known as “Fullz”. Fullz consist of enough identifying information that the purchaser can easily commit identity theft. In the early days of the Dark Web, Fullz of a US citizen (the most valuable victims) could be sold for as high as $100, but dark marketplaces aren't immune to market forces: supply, demand, and quality impact prices. For example, in 2015 and 2016 hackers targeted the medical industry at unprecedented levels, resulting in a flood of patient medical records appearing on dark marketplaces, depressing the price per individual record between $20 and $40 less than its previous prices. Economies of scale are also at play: if a purchaser is willing to buy a set of more than 50 Fullz, the price per record drops to approximately $7.

Our Dark Web Future

Irrespective of disputes over encryption and its applications, encryption is no longer classified as a non-exportable munition, and is most definitely here to stay. The Dark Web is essentially an application of encrypted communication, and it's also here to stay. The Dark Web's staying power is perhaps most evident in the explosive growth of its drug sector, which has tripled since 2013 with total revenues for January 2016 alone exceeding $20M. With that said, it's apparent why organizations must engage with the Dark Web: because your friends, enemies, and employees will increasingly access the Dark Web, switching between the different layers of the web (Surface, Deep, and Dark) more seamlessly than ever before.

Consequently, organizations will need to develop relationships with service providers such as Digital Mountain that assist in monitoring the Dark Web for content that may harm the interests of organizations, and develop policies for reacting to increased activities and interaction with the Dark Web. Admittedly, at the outset, this is a task easier said than done, but with the right experts your organization can shine light on targeted parts of 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: