Report:

Anticounterfeiting on the Dark Web

Anticounterfeiting Committee — U.S. Subcommittee
Public Awareness Task Force

April 13, 2015

New York | Shanghai | Brussels | Washington, D.C.
PowerfulNetworkPowerfulBrands®

I. Introduction

Media coverage in recent years of illicit websites such as the Silk Road and other online havens for cybercriminals, has shed light on the Dark Web. Despite this attention, many corporate executives and managers responsible for corporate security or for protecting their company's brand and content have little to no knowledge of the Dark Web.

To raise awareness and address the lack of knowledge concerning the Dark Web, this report provides a brief overview of the Dark Web. This overview also may serve as the first of a series of tutorial documents about the Dark Web and its implications for trademark and content owners.

II. What is the Dark Web?

The Dark Web is a collection of websites that are publicly visible but hide the Internet Protocol (IP) addresses of the servers that run these sites. Simply put, anyone can visit a Dark Web site, but very few can determine where these sites are hosted and by whom.

III. How does the Dark Web work?

The overwhelming majority of Dark Web sites use the anonymity software Tor. The name Tor is an acronym derived from the original software project name The Onion Router. Tor software encrypts web traffic in layers and redirects this traffic around the world through randomly-chosen computers, each of which removes a single layer of encryption before passing the data on to the next computer in the network. The goal of this process is to prevent anyone – even one who controls one of those computers in the encrypted chain – from matching the traffic's origin with its destination.

When web users run a Tor browser, the sites they visit cannot easily see the web user's IP address. Tor also provides anonymity to websites and other servers. Servers configured to receive inbound connections through Tor only are called "hidden services." Tor is necessary to access hidden services through their onion address, which hides the service's server IP address (and hence its network location). The Tor network recognizes these addresses and routes data to and from hidden services, including those hosted behind firewalls, while preserving the anonymity of both parties.

It is important to note that the IP addresses of hidden services are not hidden to all. Tor hidden services, including illegal marketplaces such as Silk Road, Silk Road 2.0, Agora and Evolution have had hundreds of thousands of regular users. Anyone who runs Tor will know the URL of a hidden service, which for Tor hidden services ends in ".onion," and can easily visit those illegal online marketplaces.

III. Distinctions between the Surface Web, Dark Web and Deep Web

Many in the media often confuse or misunderstand the difference between the Dark Web and the Deep Web, and do not understand how these terms relate to the worldwide web that most of us see and routinely use. To put things into perspective, this report provides the following descriptions of the three relevant portions of the web. First, the surface web is the part of the web most of us are familiar with as it comprises any webpages that typical search engines can access and index. Note that the webpages of the surface web contain links that help search engines find and identify content. Second, the Deep Web contains anything that a search engine cannot access. Third, the Dark Web is the small portion of the Deep Web that is intentionally hidden and inaccessible through standard web browsers.

IV. Recent Developments

Although the Dark Web is known as a safe haven for those who traffic in the sale of drugs, weapons, counterfeit documents and child pornography, not everything on the Dark Web is "illegal." There are some who use the Dark Web for legitimate purposes. For instance, many activists and political dissidents use the Dark Web to exercise their right to freely express their opinions, or as a way to exchange and receive information that is censored or controlled. The same protection Tor provides to cybercriminals can also be used to circumvent censors and nationally imposed restrictions on the web. The use of Tor hidden services has allowed journalists to accept leaks from anonymous sources. For example, the software tool SecureDrop, works with Tor hidden services to let any news organization receive anonymous submissions.

Further, Facebook has launched a Dark Web site designed to appeal to users who visit the site using Tor to evade surveillance and censorship. Given Facebook's use of SSL encryption, it is difficult for any surveillance system monitoring Facebook's connection or a web user's local traffic to match the user's identity with their Facebook activity. Facebook's use of SSL encryption in combination with Tor hidden services provides users high level of cybersecurity and privacy. This unconventional approach could be a model for sites that wish to provide a higher level of cybersecurity and privacy to their users.