Chapter 17
A Framework for Dark Web Threat Intelligence Analysis

Xuan Zhang
Criminal Investigation Department of Shandong Police College, Jinan, China

KP Chow
Department of Computer Science University of Hong Kong, Hong Kong, China

ABSTRACT

This article describes how the Dark Web is usually considered the dark side of the World Wide Web. Cyber criminals usually use specialized tools, e.g. TOR, to access the hidden services inside the Dark Web anonymously. Law enforcement officers have difficulty tracing the identity of these cyber criminals using traditional network investigation techniques that are based on IP addresses. The information available in the Dark Web, which includes BitCoin wallets, email addresses, hyperlinks, images and user behavior profiles, can be used for further analysis, such as a correlation analysis. Present within this artcile is a threat intelligence analysis framework to help analyze the crimes and criminals in the Dark Web and the framework is realized by the implementation of the Dark Web Threat Intelligence Analysis (DWTIA) Platform.

INTRODUCTION

The World Wide Web (WWW) is much bigger than what people see today. Existing search engines, e.g. Google and Baidu, can only search approximately 5% of the whole WWW. Besides those searchable contents, there are a lot more resources and data that are available on the Internet and such places are usually known as Deep Web and Dark Web (Pagliery, 2014). Deep Web usually refers to resources and data that are available on the Internet, but are not accessible with normal web browsers and hyperlinks. According to some statistics, the part of WWW that are accessible by normal web browsers (also known as Surface Web) contain approximately 4 billion web sites, while the Deep Web contains several times more web sites than the Surface Web. A portion of Deep Web that is widely used for criminal activities, such as drugs dealing, child pornography, weapons selling, etc., is known as the Dark Web. Items for

DOI: 10.4018/978-1-7998-2466-4.ch017

sales in the Dark Web include stolen email accounts and credit card numbers, personal identity information and medical information, fake identities, design drawings, malware, systems vulnerabilities, child pornography, drugs, weapons, and hire to kill services. Most of the sales items are illegal (Vogt, 2017).

Cyber criminals usually use specialized tools, e.g. the TOR, to access the hidden services inside the Dark Web anonymously. Law enforcement officers have difficulty to trace the identity of these cyber criminals using traditional network investigation techniques that are based on IP addresses. Therefore, specialized intelligence analysis techniques are needed to trace cyber criminals in the Dark Web. Law enforcement agencies all over the world are trying to trace the identity of users that access the Dark Web using TOR and progress is very limited. Silk Road, an e-commerce platform in the Dark Web, was launched in February 2011 selling illegal items. Due to the support of the hidden services protocol and TOR, Silk Road was able to hide its identity from law enforcement agencies. Silk Road was taken down by FBI in October 2013 and Silk Road 2.0 was taken down later. In 2015, after the discovery of the child pornography website Playpen in the Dark Web, FBI used Network Investigative Technique (NIT) tools to trace hidden users behind the encrypted and anonymous TOR network (Condliffe, 2016). FBI eventually found more than 1,300 "real" IP addresses, of which 137 users were charged with crimes (Osborne, 2014). However, these two cases also caused a lot of controversy. Does the use of hacking techniques to trace network users that are using anonymous tools compliance with laws and regulations? In April of 2016, the Supreme Court of US approved a change to the existing Rule 41 that would allow US federal judges to issue search warrants to use NIT to hack computer anywhere (Moore et al., 2016).

As the increase in popularity of the Dark Web by normal web users, how to conduct cybercrime investigation in the Dark Web in a legal manner becomes a challenge to law enforcement officers. How to identify the anonymous web surfer in TOR? How to identify the e-commercial sites that are using hidden services in TOR? All these are new challenges to today's law enforcement agencies. With tools like FBI's NIT, it has to rely on system's vulnerabilities even it is allowed under the legal framework. By collecting and analyzing large volume of data and information from the Dark Web may be a possible alternative to assist law enforcement officers to combat cyber criminals. In this paper, we present a framework which investigators can analyze data and information from the Dark Web, which includes BitCoin wallets, email addresses, hyperlinks, images and user behavior profiles. This deep analysis can help investigators to have a better understanding of potential crimes and behavior of the criminals. The proposed framework is realized in the design of the Dark Web Threat Intelligence Analysis Platform.

THE DARK WEB

To access the Dark Web, specialized tools are needed, such as TOR (The Onion Router), I2P and Freenet. All these tools support anonymous web serving. The most popular one is TOR. The principle behind TOR is communication between a user and the server will go through many routers and all communications are encrypted. Moreover, communication between any 2 routers uses different encryption key. Therefore, no one is able to trace where the real user and the server are. In this manner, anonymous web serving can be guaranteed.