Improving Intelligence Collection Efforts Targeting Dark Web Sources

Erin L. Dickerson

Northeastern University

360 Huntington Avenue

Boston, MA 02115

College of Professional Studies - Master of Arts in Strategic Intelligence and Analysis

Intelligence Collection - SIA6090

dickerson.e@husky.neu.edu

Improving Intelligence Collection Efforts Targeting Dark Web Sources

Abstract

OSINT and HUMINT can obtain and vet valuable information available in the deep/dark web that would otherwise be inaccessible by utilizing task forces and deanonymizing tools to target TOR browsers and users.

The Internet is an invaluable asset for multiple intelligence collection methods. Open Source (OSINT) and Human Intelligence (HUMINT) in particular benefit greatly from information gleaned from the Internet. The Internet is comprised of much more than what is readily available through simple web searches. If the Internet is an iceberg, everything readily accessible is the tip and the dark/deep web is everything below the surface. This paper will discuss methods to deanonymize and vet dark/deep web information sources efficiently, thereby solving a problem currently plaguing the Intelligence Community (IC).

Dark Web and Deep Web

The Dark Web and Deep Web are used by criminals and terrorists who rely on the anonymity to maintain secrecy.

All Internet users have access to a certain number of websites through commercial search engines (Google, for example). "The Deep Web is anything not accessible through the commercial search engines… the Darknet [is] a specific part of that hidden Web where you can operate in total anonymity." (*Going Dark* 2014)

The Dark Web is perhaps most famous for Silk Road and Silk Road 2.0 (now defunct due to the efforts of the Federal Bureau of Investigation), both of which allowed users to purchase

drugs, weapons, false government documents, and even allowed the hiring of assassins. (*Going Dark* 2014).

To access the Dark Web, a user must download a browser that allows the user to operate "anonymously". "Tor is the main browser people use to access the part of the Web where anonymity reigns." (*Going Dark* 2014) Tor anonymizing users identities by bouncing their Internet Protocol (IP) addresses to other domains, making it appear as though a user who is located in Germany is actually located in Sweden, then in Ireland, then in Cyprus. This information is of course then encrypted so that it is difficult to trace back the origin of the user's IP address.

In the past, the Federal Bureau of Investigation has used Malware and "exploited a known bug in Firefox to identify users connecting with the Tor Browser Bundle" (*The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers* 2016). The Federal Bureau of Investigation has used more sophisticated Network Investigative Techniques (NIT) to investigate Dark and Deep Web users as well. These tactics, however, can be expanded upon and improved as outlined below.

Issues

One issue, of course, is that Deep and Dark Web sites such as Silk Road and its replacements are resilient. There will always be new marketplaces for anonymous trading and trafficking.

Another issue is the use of Tor browsers and chats as a means for terrorists to communicate and plan attacks without the knowledge of the IC.

The main issue, however, is whether IC agencies are able to keep up with technology given the technological resources (both human and physical) provided to them.

Solutions

Creation of Task Forces

The first and most important step is to create departments or task forces in each of the IC agencies. These task forces would solely focus on deanonymizing targeted Tor users using the means outlined below, thus making it easier to vet the information provided by those users in their chats and transactions. The creation of task forces would allow for these groups to become well trained and focused on their work, and provide an attractive workplace setting for potential employees with experience in hacking who would be interested in becoming a White or Grey Hat[1] hacker for various IC agencies.

Exploiting Tor Browser Leaks

As each IC agency sets up their task force, each task force can in turn set up and host a "Tor exit node". Hosting a Tor exit node (or several) is essential to exploiting the weaknesses of the Tor browser, and is the first step to deanonymizing target users.

The Tor exit node makes it possible perform a series of hacks to "see" Tor users purchasing and selling cryptocurrency as well as conducting any other peer-to-peer (P2P) business, capture their IP addresses, and then later verify their IP addresses.

The purpose of this is to deanonymize the user. Most users operate under the assumption that while they utilize the Tor browser and the Dark Web they are completely anonymous. Information provided there via chat rooms and transactions is highly, highly valuable. The hacks

[1] A "White Hat" or "Grey Hat" hacker is an ethical computer hacker. (Palmer, 2001)

done to deanonymize these users are largely undetectable, giving those collecting this intelligence an unprecedented opportunity to glean intelligence of great importance.

P2P Attacks

Peer-to-peer (P2P) transactions occur regularly on the Dark Web. While Silk Road and Silk Road 2.0 may not exist any longer, there is most certainly another iteration of those marketplaces on the Dark Web. In order to conduct business on the Dark Web, user rely heavily on Bitcoin (or another cryptocurrency, though Bitcoin has been popular). Ironically, Bitcoin is "a serious threat to the anonymity of Tor hidden services and their users." (Jawaheri, 2018).

"Using Bitcoin as a payment method for Tor hidden services leaks information that can be used to deanonymize their users. This represents a serious threat to these users, because they actively seek to maintain their anonymity by using Tor. The deanonymization is mainly due to the lack of retroactive operational security present in Bitcoin's pseudonymity model. In particular, by inspecting historical transactions in the blockchain, an adversary can link users, who publicly share their Bitcoin addresses on online social networks, within hidden services, which publicly share their Bitcoin addresses on their onion landing pages". (Jawaheri, 2018).

Distributed Hash Table Attacks

Tor browsers do not allow Distributed Hash Table (DHT) connections. This can also be exploited to gain information about a Tor browser user. By forcing a Tor browser to attempt to connect to a DHT, the Tor browser fails into "using the public network interface and publishes its public IP and listening port into the DHT". (Manils et al., 2010)

This is another instance where the preexisting Tor exit nodes and readily available computers and ports will be useful.

DDOS Attacks on Host Servers

This particular attack is not useful on a single user, however it can be useful when targeting a specific Dark Web site or server. These can be useful to disrupt communication once parties have been identified, or when a website has been deemed a target.

A Distributed Denial of Service attack "refers to malicious attempts to prevent users from accessing requested resources by depleting bandwidth or depleting the resource itself" (Soltanian, Amiri, & Neely, 2016). "DDoS can take … major websites down for several hours at a time… The attackers are able to break into hundreds or thousands of computers or machines and install their own tools to abuse them. Then they utilize these 'zombie' machines to launch the DDoS attack…" (Soltanian, Amiri, & Neely, 2016).

While this is typically a "Black Hat" hacker maneuver, DoS or DDoS attacks can be used ethically to gain intelligence as well.

Gaining Sources to Break Codes

It is exceedingly important to keep up and utilize all available resources. "Although a seemingly obscure source, reddit has been used to identify networks in illegal wildlife trafficking on the Dark Web. A 2016 study on Dark Web markets specifically listed sources in subreddit … as the basis for identifying code words used by networks in illegal wildlife trafficking. These code words were then run through many of the underground online marketplaces to identify offerings of illicit wildlife." (Paul, K. A. 2018)

These sources are invaluable and hidden in plain sight. Additionally, there are HUMINT opportunities lurking on the Dark Web, once the opportunity to vet them becomes available.

Keeping up with Technology

Anyone who has worked in the government understand the technological issues currently facing those in Intelligence Collection and Analysis. Procurement and hiring are often the most difficult roadblocks to any analysts' job.

In order to "keep up" with cyber criminals, it is important that agencies and agents receive equipment and training that coincides with the latest technology available. It is near impossible to identify, decrypt and utilize information and intelligence available on the Dark Web on computers that are ten years old. It is near impossible for an agent to run a Distributed Hash Table attack if that agent does not have a basic understand and basic training on what that attacks purpose and goal is. It is near impossible to mine cryptocurrency (a key component to catching cyber criminals) on a processing unit that struggles to come up with the computing power to run Microsoft Word.

Ideally, start-up funding would need to be diverted to the task forces in order to hire pre-trained White/Grey Hat hackers and purchase adequate equipment. Further annual funding would be required for ongoing training in areas such as Tor browser weaknesses, P2P weaknesses, cryptocurrency use by cyber criminals, and working with informants on the Dark Web.

Final Thoughts

There are many opportunities to exploit the Dark Web for information regarding cyber criminals. Terrorists, human traffickers, sex traffickers, drug traffickers, and all kinds of other illegal black-market dealers exist in the Dark Web sphere. These users believe they are anonymous. They believe they are untraceable and cannot be caught. This belief is false. These users can be deanonymized and brought to justice.

References

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy, 35*. doi:10.1016/j.drugpo.2016.04.020

As the FBI Cleans the Dark Net, Sites Far More Evil Than Silk Road Live On. (2014, November 11). Retrieved from https://web.archive.org/web/20150726082027/http://motherboard.vice.com/read/as-the-fbi-cleans-the-dark-net-sites-far-more-evil-than-silk-road-live-on

Bradbury, D. (2014). Unveiling the Dark Web. Network Security, 2014(4), 14-17. doi:10.1016/s1353-4858(14)70042-x

Cubrilovic, N. (2014, November 17). FBI seizes fake Tor hosted Jihad funding website as part of Operation Onymous, leaves up real site. Retrieved from https://web.archive.org/web/20160220124858/https://www.nikcub.com/posts/fbi-seizes-fake-tor-hosted-jihad-funding-website-as-part-of-operation-onymous-leaves-up-real-site/

Farivar, C., Gallagher, S., & UTC. (2015, July 16). Feds bust through huge Tor-hidden child porn site using questionable malware. Retrieved from https://web.archive.org/web/20150809031658/http://arstechnica.com/tech-policy/2015/07/feds-bust-through-huge-tor-hidden-child-porn-site-using-questionable-malware/

Going Dark: The Internet Behind The Internet. (2014, May 25). Retrieved from https://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet

Jawaheri, H. A., Sabah, M. A., Bosmaf, Y., & Erbad, A. (2018). When a small leak sinks a great ship: Deanonymizing TOR hidden service users through Bitcoin transaction analysis.

Manils, P., Abdelberri, C., Blond, S. L., Kaafar, M. A., Castelluccia, C., Legout, A., & Dabbous, W. (2010). Compromising Tor Anonymity Exploiting P2P Information Leakage.

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal, 40*(3), 769-780. doi:10.1147/sj.403.0769

Paul, K. A. (2018). Ancient artifacts vs. digital artifacts: New tools for unmasking the sale of illicit antiquities on the dark web. Arts, 7(2), 12. doi:10.3390/arts7020012

Phelps, A., & Watt, A. (2014). I shop online recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digital Investigation, 11(4), 261-272. doi:10.1016/j.diin.2014.08.001

Silk Road 2.0 Was Just Shut Down by the FBI. (2014, November 06). Retrieved from https://web.archive.org/web/20150627203614/http://motherboard.vice.com/read/silk-road-2-has-been-seized-by-the-fbi

Soltanian, M. R., Amiri, I. S., & Neely, M. (2016). *Theoretical and experimental methods for defending against DDOS attacks*. Amsterdam: Elsevier.

The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers. (2016, January 05). Retrieved from https://web.archive.org/web/20160108050547/http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers

Wimmer, A. (2015). Darknet, Social Media and Extremism: Addressing Indonesian Counterterrorism on the Internet. Retrieved from

https://www.academia.edu/20813843/Darknet_Social_Media_nad_Extremism_Addressing_Indonesian_Counterterrorism_on_the_Internet

Zimmer, A. (2018, April). Arkansas Agency Catches Criminals with Cryptocurrency. Law Enforcement Technology. Retrieved from https://www.officer.com/investigations/article/20996785/alabama-agency-catches-criminals-with-cryptocurrency