https://doi.org/10.48009/4_iis_2016_36-41

Issues in Information Systems
Volume 17, Issue IV, pp. 36-41, 2016

DEEP WEB, DARK WEB, INVISIBLE WEB AND THE POST ISIS WORLD

Ryan Ehney, Texas A&M University – Kingsville, cehney@satx.rr.com
Jack D. Shorter, Texas A&M University – Kingsville, jack.shorter@tamuk.edu

ABSTRACT

Is there a difference between the invisible or deep web and Dark web? "New research from MIT (Massachusetts Institute of Technology) shows how malicious TOR entry guards can strip away the Dark Web's anonymity features, exposing users and the hidden websites they visit." Law enforcement and government agencies have made considerable headway by developing new and improved methods to deanonymize the TOR and track users using the Deep web for bad purposes. How can we fight terrorism and use the Deep/Dark web for good? The United States government has been trying to design certain programs that can take away some of the anonymity of the TOR and track users on the Dark web. They are trying to find ways to fight terrorist groups but still give people a certain level of privacy. The biggest design that has been created to aid in the tracking and monitoring of users on the Dark web (including terrorist groups) is a MEMEX project that has been developed by DARPA (Defense Advanced Research Projects Agency). If we can start to monitor certain users of the Dark web, then we can finally take a step to actively fight terrorism.

Keywords: Deep Web, Dark Web, Invisible Web, Terrorism

INTRODUCTION

Consider this thought. You are fishing on the ocean, which we all know is greatly immense, and are all trying to catch fish on the surface of the water right underneath the boat. There is a world out there that most people do not even know about. I am talking about a cyber world that is invisible to those who do not know how to access it. To the majority of the people on this earth that have access to the World Wide Web, what they see when they open up an Internet browser is all that they know. In reality, they have no idea just how much of the web they are not able to access. The typical search engines such as Google, Yahoo, and Bing are just the surface of the web that can be accessed from anywhere and by anybody, all one needs is a stable Internet source (Goodman, April 1, 2015). When performing a regular search on the Internet, what is returned really only makes up less than one percent of all the information that is actually out there for review? There is another dimension out there that can only be accessed by special software and is estimated to be about five hundred times larger than the surface of the web that we can see. I am talking about the invisible web, which to some is better known as the "Deep" web or "Dark" web. It is a place that is beyond our understanding. Places where people can do, say, or acquire anything that they want because there are advanced forms of privacy and anonymity. It is entirely a different world that few know much about, but it is time for us to start learning and realizing just how mysterious and dangerous these places really are. We all need to be educated and informed on the uses and abilities of the Deep web. Knowledge is the most vital key to the world as we now know it.

DEEP WEB VS DARK WEB

Is there a difference between the invisible or deep web and Dark web? Many people that know about the invisible web will give a different answer to this question because it is easy to consider them as being the same thing. Central to the Dark web discussion are key definitions to reduce the confusion concerning Deep web, Dark web and anonymous browsing. The Deep web is, in a sense, the content of databases and other services of the web that for one reason or another cannot be indexed by the typical search engines that everybody uses. The Deep web is not all bad (Lamo, 2015). The Dark web on the other hand is part of the Deep web, and requires a specially designed browser and encryption methods to access. Neither the Deep nor Dark web can be indexed when seeking information which leads people to believe that they are the same. But the two categories of web that cannot be indexed are synonymous. The Dark web is a massive cyber underground world where some of the worst kinds of

people like hackers, gangsters, terrorists, and pedophiles go to have fun or purchase anything. Some people might even consider the Dark web to be the black market where one can acquire things like drugs, counterfeit currency, forged documents, firearms and explosives, human organs, and even hitmen. One cannot expect to purchase these things by inputting a credit card number and providing an address to which to have it shipped. There are certain things that help Internet crime work. Forms of cryptocurrency, such as bitcoins, facilitate currency exchange for whatever the purchaser wishes. Many organized cybercrime syndicates even have the ability to outsource hackers for hire. There are sites on the invisible web where one can contract certain "entities" to hire a hacker to do the dirty work for a well-funded organization or person (On Line Universities.Com, 2015)

As explained, one can see there is a difference, whether it is slight or not, between the Deep and Dark web. Both require special access but one is far more dangerous than the other. The Dark web (or Dark Net) is a twisted and maniacal place where some of the world's most unsavory or dangerous people or groups centralize to stay "under the radar" of government agencies or others that may condemn their actions.

How does one simply access the invisible web? One cannot access the invisible web but just going to Google and typing in "Invisible Web". It does not work like that. All one will find is articles and instructions on how to possibly gain access to the invisible web. In order to effectively access the Deep web, a particular set of software packages and routers are required which are capable of finding multitudes of hidden information and in a sense "illuminate the Dark" (OWEDB.org, 2013). There are a few different browsers people use to gain access to the invisible web, the original TOR browser, which is what a majority of people used, and the more recently created Hornet TOR browser, which was designed to be a more secure option to the TOR. TOR (The Onion Router) routers came into existence in the mid-nineties as a result of US Naval Research Lab project aimed at providing covert communication channels for military and government employees (TORproject.org, 2015). Eventually the technology was released into the Open Source community (undoubtedly because something more effective was developed by the government) where it has since been improved. TOR browsers use random entry points in the Onion network based on information provided by a TOR directory server which lists random entry points. Data request are encrypted and forwarded along with the final destination address. Each subsequent relay point in the path unencrypts the address, re-encrypts the request and forwards along. It only knows where the data came from last and where it goes next. At each point along the path data is encrypted between nodes (TORproject.org, 2015). No one relay can determine the entire path the data took. Finally the data reaches an exit point where it is then directed to its final destination. Additionally, further requests for the TOR network get new paths approximately every 10 minutes to provide further privacy in case someone is performing traffic analysis at a singular node. Hornet, (Osborne, 2015) is a high-speed onion routing network which leverages next-generation architecture to make user tracking more difficult. Hornet was developed by Chen Chen of Carnegie Mellon University together with Daniele Enrico Asoni, David Barrera, George Danezis and Adrian Perrig -- hailing from Zurich's Federal Institute of Technology and University College London. The way it works is the network goes through servers and creates virtual passageways which make the IP tracking a strenuous process. The primary item that makes Hornet more secure than the initial TOR browser is when Hornet is in use the system it will not keep track of the per session states, instead, Hornet offloads session states to end hosts by default, encrypting each packet to reduce the risk of data leaks (Osborne, 2015).

The anonymity of the TOR browser has recently been discovered to not be as anonymous and secure as it may lead people to believe. We live in a world now where there is always going to be at least one person who is so computationally savvy that they can crack into any network on almost every system, all they need is a device capable of accessing the network and a reliable Internet source. It is also very difficult for someone to even simply download a TOR without the government knowing that you actually did download it (Tucker, 2015). "Any user simply attempting to download TOR was automatically fingerprinted, essentially enabling the NSA (National Security Agency) to know the identity of millions of TOR users." The entry guards that the TOR requires are one of the biggest reasons why it is not as anonymous as it should be (Stockley, 2015). "New research from MIT (Massachusetts Institute of Technology) shows how malicious TOR entry guards can strip away the Dark Web's anonymity features, exposing users and the hidden websites they visit." (Stockley, 2015) The way they are able to track TOR users is through a process called website fingerprinting. When users attempt to do a website fingerprint attack one needs to (According to the MIT research team) "start by studying the behavior of TOR circuits on the live TOR network when a client connects to a TOR hidden service (Kwon, 2015). Our key insight is that during the circuit construction and communication phase between a client and a hidden service, TOR exhibits finger printable

traffic patterns that allow an adversary to efficiently and accurately identify, and correlate circuits involved in the communication with hidden services. Therefore, instead of monitoring every circuit, which may be costly, the first step in the attacker's strategy is to identify suspicious circuits with high confidence to reduce the problem space to just hidden services. Next, the attacker applies the WF attack to identify the clients' hidden service activity or deanonymize the hidden service server." (Kwon, 2015) The TOR is a very useful piece of software, it is quite unique and interesting in what all it is capable of doing. For just as many reasons as somebody would want to use a TOR to access deeper web browsing, there are equally as many reasons as to why one would want to stop somebody from being hidden while they access websites that a typical search engine could not even attempt to find. There are a number of people out there that are trying to find different ways to be able to track and identify who is accessing what on the invisible web (Keller, 2015). There are MIT researchers who have been able to identify sites with about an 88 percent rate of accuracy. It is extremely difficult but not impossible. The best way to try and track somebody using a TOR is to track their keystrokes. Just like how someone will have the same handwriting tendencies over and over again, when people use a computer they tend to create a pattern with their keystrokes. A keystroke is "the detailed timing information that describes exactly when each key was pressed and when it was released as a person is typing at a computer keyboard." The best way to prevent somebody from tracking your activities is to not do anything to draw attention to yourself and stay away from illegal activity. Being able to track somebody using a TOR browser should make one assume that nothing truly is anonymous.

THE DARK WEB AND TERRORISM

How has recent activity on the Dark web proved to be negative and dangerous? As I stated previously, there are a lot of malicious and conniving characters that like to use the Dark part of the invisible web. They could be individuals looking to satisfy their own guilty pleasures, or as research will show, could be terrorist organizations, such as ISIS and al Qaeda, looking to recruit and gain funding from those who are willing to help their cause. They are able to post many propaganda videos and images in certain places within the Dark web that can generate a lot of traffic. This is a great way to recruit solders and aid them by funding these terrorist groups. They also use the Dark web to communicate with one another because the invisible web helps them stay out of the watchful eye of government authorities. Terrorist groups, namely the two listed above; (Glasser, 2015) use what is called mujahedeen secrets, which is an encryption tool. Also (Paganini, 2015) there are even "hidden services in the Deep Web that offer downloads of mobile apps used by the jihadists to communicate securely and to transfer Bitcoins to terrorist cells located anywhere in the world." These bitcoins, as I mentioned earlier, are the main way that these groups get funded through the web because, even though it is online, cryptocurrency is still currency that is accepted anywhere on the Internet so the possibilities are endless of what all can be purchased. With this form of digital currency, people from all over the world can aid terrorists, even American citizens (Glasser, 2015). It is tremendously difficult to read or trace most messages between terrorists because most of them get destroyed right after they have been received and read only by the recipient the message was intended to reach. Only those who are sending the messages are able to see the entire message using special logarithmic keys. There are even applications that one can download on their smart phone that can allow anonymity when communicating with others.

Governments have definite reasons to keep tabs on certain individuals now because they feel that there is too much that can happen and has happened with groups correlating attacks by utilizing apps such as Whatsapp, Kik, Wickr and Surespot. There are always going to be people out there that believe that encrypted services should stay the way they are and not have too many people trying to spy because it is a violation of our freedoms. We need to have a certain level of privacy within our lives. It seems terrorists groups have a much deeper understanding of the Deep web than initially thought and are able to navigate through various "holes" in the system to remain undetected. Law enforcement and government agencies have made considerable headway by developing new and improved methods to deanonymize the TOR and track users using the Deep web for bad purposes (Kwon, 2015). Recent terrorist's attacks in Paris and Brussels have caught the attention of world media because of the global impact terrorists attacks create. A lot of the crimes that take place on the Dark web go unnoticed and undocumented because we have no idea that they are happening. These are tragic events, yes, but unless we do something about it, the events will continue to escalate and progressively get worse. The next event being planned over the Dark web could be one to cause even more mayhem and chaos. This is exactly what terrorist groups want, everyone becoming afraid to live their lives. Terrorist groups thrive off of the fear of others and use it to their advantage. It will not be an easy task to try and

stop these groups, but it is something that needs to be done and quickly before too many more innocent people get hurt.

CONFRONTING TERRORISM

How can we fight terrorism and use the Deep/Dark web for good? The United States government has been trying to design certain programs that can take away some of the anonymity of the TOR and track users on the Dark web. They are trying to find ways to fight these terrorist groups but still give people a certain level of privacy. There have been a few different publications written by people with a lot of experience and expertise in this field and who have an active involvement in trying to fight the bad people who use the Dark web (Stockley, 2015). "Recently, the Chertoff Group put out a new paper detailing some of the methodologies that they advise law enforcement to use to monitor TOR users and sites. Since it was co-written by former DHS Director and Jeb Bush national security team member Michael Chertoff, it's safe to say it provides a good indication of current law enforcement thinking. The name of the paper is the Impact of the Dark Web on Internet Governance and Cyber Security, co-written with Toby Smith." This is just one example of a piece of work that somebody has written to try and help with the defense of the Dark web. Some of the different practices that can be taken to help track users could include mapping the hidden service directory, customer data monitoring, social site monitoring, hidden service monitoring and marketplace profiling (Chertoff, 2015).

The biggest design that has been created to aid in the tracking and monitoring of users on the Dark web is a MEMEX project that has been developed by DARPA (Defense Advanced Research Projects Agency). DARPA is a Department of Defense agency responsible for the development of emerging technologies used to aid the US military. Project MEMEX is a technical nod to American engineer Vannevar Bush's 1945 article, As We May Think (Bush, 2015). In it, he discusses his visionary memex (memory index) device which would be used to index knowledge in order to supplement human memory. "Project MEMEX has been in the works since 2014 and is being developed by seventeen different contractor teams who are working with the military's DARPA division (Zetter, 2015). Google and Bing are only able to capture approximately five percent of the Internet (Goodman, 2015). The goal of MEMEX is to build a better map of the Internet content in order to stop human trafficking". However, criminal activities of many types will most certainly be targeted, to include terrorist activity. "We need a technology to discover where that content is and make it available for analysis," said Chris White of the DARPA. "MEMEX allows you to characterize how many websites there are and what kind of content is on them," (Zetter, 2015) White said. "It was actually first developed to track down human trafficking on the web — it's an idea that works for an illicit activity users try to keep hidden." If we can start to monitor certain users of the Dark web, then we can finally take a step to actively fight terrorism and prevent a lot of future attacks. This is the technology age, and even though actual attacks are physical, all of the initial planning and coordination is done through some sort of digital equipment. Terrorist's groups use computers or mobile device that are able to hide from even the most qualified tracking systems (Beyond Google, 2014). We can use the invisible web for good by countering propaganda videos and images posted by terrorists groups. The forces fighting terrorism can utilize their own videos and images to educate the world with the truth about ISIS and other terrorist groups (OEDB.org, 2013). Not everyone on the invisible web is using it for bad purposes (Freenet, 2016). There can be a whistleblowing system in place. If someone is on the Dark web they can attempt intercept and let the proper authorities know about the unusual behavior. But we need to first establish a way to view others using the invisible web. Projects like MEMEX are only the beginning of what can be accomplished with the positive use of technology (O'Neill, 2013). It is inevitable that groups fighting terrorism will use their own Invisible Web experts to counter terrorist's usage of the deep web, and even use it to eradicate those that would destroy civilized groups who do not prescribe to a particular manifesto.

GLOBAL COOPERATION

A final topic to mention is global cooperation. Each country involved in cyber warfare defense and intelligence gathering must work together to fight the criminals and terrorists using the Deep web for ill-gotten gains and destruction. Every allied country against terrorism has varying laws governing Internet monitoring. Political cooperation is crucial to success. Organizations such as the United Nations Counter-Terrorism Implementation Task

Force reach across dozens of global entities in order to find and stop terrorist activities. The cooperative efforts of these organizations are critical to eliminate terrorist groups and ideals (Entities, 2015).

SUMMARY

As previously stated, there is a whole other world (and portion of the Internet) that most of us do not know about. It is frightening to contemplate the unknown plots and plans being hatched on the Deep/Dark/Invisible Web. Because that is exactly what is it, unknown. The search engines that we all use every day only scratch the surface of what is actually out there for us to access (Bruce, 2013). Civilized people throughout the world, need to educate themselves and do more to help expose terrorists who are utilizing the deep web to harm innocents (O'Neill, 2013). Most non-radicalized rational people want terrorist acts to stop. Everyone must start to actively think about how they can help stop the terror. The authors of this paper are citizens of the United States of America. Many of the worst attacks have not happened on our soil. But they will if we idly sit by and believe others will solve this problem for us. John F. Kennedy once said "Do not ask what your country can do for you, but what you can do for your country". The best thing we can do for our country is to gain knowledge and insight into this other cyber world. Knowledge has, and always will be, the most effective weapon against the heinous use of the Internet for gain or to reap terror.

If a worldwide conscious effort is made to eradicate groups who want to control others by the use of terror, it will be done. What a human is able to accomplish when they actually put their minds to it is astonishing. The authors hope, that after reading this paper one may have better insights into what actually goes on in the Dark/Deep/Invisible Web. If the invisible web can be used for horrible acts, it can also be used to eventually stop those who would suppress and terrorize innocent people in our world. We know that there are countless individuals working tirelessly to combat the negative use of the internet and its use for bad purposes.

REFERENCES

Beyond Google: The Invisible Web. (2014, December). Available: http://library.laguardia.edu/invisibleweb/characteristics

Bruce, J. (2013, April 17). How Do Search Engines Work? Available: http://www.makeuseof.com/tag/how-do-search-engines-work-makeuseof-explains/

Bush, V., (2015). As we may think. Available: http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/

Chertoff, M., & Simon, T., (2015). The impact of the Dark Web on Internet governance and cyber security. Available : https://www.cigionline.org/sites

Entities. (2015). Available: https://www.un.org/counterterrorism/ctitf/en/entities_CTITF

Freenet. (2016, March 20). Available: https://en.wikipedia.org/wiki/Freenet

Glasser, E. (2015, November 16). Paris attackers used 'Dark web' to coordinate. What is it? Available: http://www.wtsp.com/news/Dark-web-Internet-access-terrorists-recruit-communicate-encrypted-logarithm-usf-cybersecurity-macdill/47820003

Goodman, M. (2015, April 1). Most of the Web Is Invisible To Google. Here's What It Contains. Available: http://www.popsci.com/Dark-web-revealed

Keller, A. (2015, August 19). Just How Anonymous Is The TOR Browser? Retrieved from http://www.inquisitr.com/2350699/just-how-anonymous-is-the-TOR-browser/

Kwon, A., AlSabah, M., Lazar, D., Dacier, M., & Devadas, S. (2015). Circuit Fingerprinting Attacks: Passive Deanonymization of TOR Hidden Services. Available: https://people.csail.mit.edu/devadas/pubs/circuit_finger.pdf

Lamo, A. (2015). What is the Deep web and how do you access it? Available: https://www.quora.com/What-is-the-Deep-web-and-how-do-you-access-it

OEDB.org (2013, November 11) The Ultimate Guide to the Invisible Web. Available: http://oedb.org/ilibrarian/invisible-web/

O'Neill, P. H. (2013, October 14). How to Search the Deep Web. Available: http://www.dailydot.com/technology/how-to-search-the-Deep-web/

On-line Universities Com. (2015) How to Search the Invisible Web. Available: http://www.onlineuniversities.com/articles/students/how-to-search-invisible-web/

Osborne, C. (2015, July 24). Hornet TOR alternative for high-speed anonymous browsing revealed. Available: http://www.zdnet.com/article/hornet-TOR-alternative-for-high-speed-anonymous-browsing-revealed/

Paganini, P. (2015, May 22). The ISIS advances in the Deep Web among Bitcoin and Dark nets. Available: http://securityaffairs.co/wordpress/36961/intelligence/isis-in-the-Deepweb.html

Stockley, M. (2015, August 3). Can you trust TOR's entry guards? Available: https://nakedsecurity.sophos.com/2015/08/03/can-you-trust-TORs-entry-guards/

TORproject.org. (2015) What is the TOR Browser? Available: https://www.TORproject.org/projects/TORbrowser.html.en

Tucker, P. (2015, February 24). How the Military Will Fight ISIS on the Dark Web. Available: http://www.defenseone.com/technology/2015/02/how-military-will-fight-isis-Dark-web/105948/

Zetter, K. (2015, October 2). Darpa Is Developing a Search Engine for the Dark Web. Available: http://www.wired.com/2015/02/darpa-memex-Dark-web/