Tor – the dark side of the internet essay

Contents

In the mid-1990s, the internet experienced a vast growth that transformed the society significantly on the global scale. Unexpected change that was not part of the initial intention of starting the internet came up where people could communicate instantly. The internet was not established with the aspects of privacy and anonymity in mind. As such, everything that people, as or post online can and in many cases, is traced, recorded and tracked back to the people who initially say it or post it. Due to a rising concern for the privacy and anonymity, a group of researchers developed a system of communication that could allow a bi-directional communication over the internet(MacLeod, 2016). In such a communication system, a mid source could not determine the source and the destination of the communication. This system creates an overlay network (a network that is built on top of another network; internet in this case).

Dark web versus Deep web

Darknet is, therefore, an overlay network that uses the onion router (TOR), meaning that it can only be accessed through particular software. TOR together with other darknets such as the I2P and Freenet forms the dark web. Dark web is a small portion of the deep web. The deep web can be identified as the all the things that are on the web but which cannot be indexed by normal search engines such as Google, Yahoo, and Bing. Deep web involves everything on the web that has paywall or password protection. Some examples of deep webs may include Netflix, dynamic pages, online

banking, and webmails (MacLeod, 2016). The deep web is said to contain the largest data content of which, the dark web is part of it.

TOR

Tor comprises of two aspects; software and a network that promotes the operation of the software. These two aspects of Tor work to ensure the privacy and anonymity of the internet users. TOR hides the IP address of a person using the internet in such a way that it appears to come from an address that is already in existence that is hard to locate. Most people prefer using TOR in order to have access to services or websites that are blocked in certain countries such as the Great Firewall of China, avoid websites that can tracks a person's activity online and maintain anonymity when sending sensitive information to social sites (What is a Tor Relay? | Tor Challenge, 2016).

Bitcoin

With the advancement in technology, a group of anonymous engineers came together and designed a virtual currency that is formally known as the Bitcoin. It is a form of online interaction protocols that allows people to use this virtual currency. The Bitcoin technology was introduced into the market in 2009 but since then, it has served more than 62. 5 million transactions globally(Böhme, Christin, Edelman, & Moore, 2015). In early 2005, it was estimated that more than 200, 000 ($50 million) bitcoins were transacted daily in the market exchange. Since it source is anonymous, the amount of bitcoins in the circulation is not known although it is estimated to be 14 million whose value is approximate $3. 5 billion (Böhme, Christin, Edelman, & Moore, 2015). The operation of bitcoin is somehow complicated because it

is built on transaction log that is distributed across the network of operating users rather than being stored on any single server or set of servers. Its mechanism is interesting as it protects against the concentration of power, can reward honest and can allow irreversible transactions.

Silk Road

Silk Road is an online platform (a darknet market) that was design for the black market activities dealing with selling and buying of drugs. It is the largest known black market in the dark web and is operated using TOR services. Having been developed in February 2011, Silk Road attracted many Tor users, and it attracted the public to an extent that I became the security's targets. The website was associated with the assassin for hire something that raised an alarm for the security of the society. By October 2013, the FBI managed to put down the website and convicted the alleged criminal behind its design and operation (Ross William Ulbricht). By the time it was shut down, Silk Road had earned William approximately $1. 2 billion (What is a Tor Relay? | Tor Challenge, 2016). One month later, Silk Road 2. 0 was launched by the alleged ex-administrators of Silk Road. In late 2014, Silk Road 2. 0 was captured and shut down. Two hours after the Silk Road 2. 0 was closed down, Silk Road 3. 0 was launched, and the FBI are still on the lookout for more affiliation of Silk Road websites.

Web Based Hidden Services

The web-based hidden services operate in TOR technology. All the hidden services operate in addresses that end in . onion, a pseudo domain that hardly exists on the surface web but which operates only on the TOR network (Constantin, 2016). The hidden services protect the anonymity of

the users as well as the servers. It, therefore, attracts many users as the surveillance on the internet is avoided thus law enforcements can hardly trace the sources and the destination. TOR hidden services operate on nodes that contain special Hidden Service Directory (HSDir) flag that they use to advertise their services on the TOR network for the users to identify them easily (Constantin, 2016). The hidden services select six hidden service directory nodes that operate as its rendezvous points. The selection of the nodes is done from the pool of 4000 nodes depending on a specified date-dependent formula.

The hidden wiki

The hidden wiki is a term that is given to various TOR operating hidden services. They allow a user to edit the links anonymously upon the registration. The hidden links are operated through the onion pseudo top-level domain that can only be accessed using TOR. The main page provides numerous links that claim to offer services in the black-market such as cyberattacks, money laundering, selling of drugs, adult content, contract killing and child pornography. The hidden links always appear on the main page of the Tor.

Sandbox

A sandbox can be identified as the environment that offers the appropriate settings for the testing of the programs that are usually from untrusted sources. Such programs usually are designed for destructive purposes. When the programs are run, they run freely in the sandbox. The sandbox tests them and once identified as malicious or malware, systems notes the malware sections and takes a rollback operation (Sanya, Hainan & Sheng,

2015). The sandbox protects the system from destruction by the malicious programs. Currently, sandbox technology as being used in common browsers such as Google Chrome browsers and the latest Microsoft Office suite (2013).

Online privacy

It is possible to track down people's identity and personal information while they are using the internet (moving from one site to another), with the help of very sophisticated technology. Web browsers, for example, use cookies to store files on a person's computer and which can disclose their personal information. Of the sophisticated technology that is currently being used to fish data from internet users is the flash cookies (Online Privacy: Using the Internet Safely | Privacy Rights Clearinghouse, 2016). These types of cookies also known as supercookies cannot be deleted during the process of clearing standard cookies and cache. In fact, they are hardly deleted by adware removal or anti-spyware program. Such technology is used to interfere with the privacy of the internet users.

References

Bohme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance †. *Journal Of Economic Perspectives* , *29* (2), 213-238. http://dx. doi. org/10. 1257/jep. 29. 2. 213

Sanya, Hainan & Sheng (2015). *Industrial Engineering, Machine Design and Automation (IEMDA 2014) et Computer Science and Application (CCSA 2014): Proceedings of the 2014 Congress on IEMDA 2014 et proceedings of the 2nd Congress on CCSA 2014 : Sanya, Hainan, China, 12-14 Dec 2014* . Singapore: World Scientific.

Constantin, L. (2016). *Tor connections to hidden services could be easy to de-anonymize* . *PCWorld* . Retrieved 9 August 2016, from http://www. pcworld. com/article/2928752/tor-connections-to-hidden-services-could-be-easy-to-deanonymize. html

MacLeod, K. (2016). *The Dark Side of the Web* . Retrieved from https://www. youtube. com/watch? v= mUP0tx7Ib2w

Online Privacy: Using the Internet Safely | Privacy Rights Clearinghouse . (2016). *Privacyrights. org* . Retrieved 9 August 2016, from https://www. privacyrights. org/online-privacy-using-internet-safely

What is a Tor Relay? | Tor Challenge . (2016). *Eff. org* . Retrieved 9 August 2016, from https://www. eff. org/torchallenge/what-is-tor. html