Darknet: An Introduction

Piyush Bulchandani
Department of Computer Science and Engineering
JIET Group of Institutions
Jodhpur, India
piyushbulchandani320@gmail.com

Kavita Choudhary
Department of Computer Science and Engineering
JIET Group of Institutions
Jodhpur,India

Abstract—Darknet is an anonymous internet where one can browse the internet without any fear of being traced. It is a portion of deep web in which clusters of computers are meshed together to form a network. Unlike other kinds of private peer to peer network connections involved in Darknet are made between trusted peers and due to this, IP addresses are also not publically shared. Darknet is not a separate physical network but an application and a protocol layer riding on existing networks and to connect to that network one has to install special software on the system by which data traffic can be routed through hundreds of nodes inside the network. Today there are many different products by which Darknets can be created; TOR is the most popular product which is used by many people to improve their security and privacy on the internet. Although TOR provides privacy to a large extent but still there are some by which user can be tracked and to prevent this user has to take some precautions to maintain anonymity.

Keywords—Darknet;Tor;anonymous internet

I. INTRODUCTION

Beyond the approach of the goolge and yahoo there exists a dark hidden web called “Darknet”. Users of Darknet try to maintain their anonymity through various ways for good or bad reasons. Darknetis like an ordinary network but to access this network one has to install some software into his/her system. This software/services and the network encompass so called Darknet. The main concept behind Darknet is that identity of the user is kept anonymous, which means that one can freely surf the network without any fear of getting tracked although user has to take some measures to protect his anonymity but still one has to bypass many layers of encryption to track any user who is using Darknet.

As we all know TCP/IP packets, headers contain a lot of identifiable information, so if anyone gets a hold on that packet he may gather information about the user. There are multiple different products available by which one can create darknet’s .The most popular one is Tor which stands for the onion router some people also use Freenet as an alternative of tor.
Today Darknet is a becoming a major concern for many organizations and individuals as the illegal activities on Darknet are increasing tremendously and as it is very difficult to find who is on Darknet and what for is looking for because of layers of encryption.

II. Darknet

Darknet is a small part of ‘Deep Web’ which means normal search engine cannot simply index the website because the spiders of the search engines cannot find the path of website. In Darknet connections are made between the trusted nodes to form a network and in order to connect to that network one has to install some kind of software to his / her computer. The main concept behind using Darknet is that it maintains your anonymity and due to this dark net is often associated with illegal activities. The most commonly used software is TOR (the onion router) and the other one is Freenet, which many people use as an alternate. Most of the people use the word TOR and Darknet interchangeably but they both are different, Darknet is a specific concept while TOR or Freenet are specific products or services and these services encompass what this Darknet is considered and it is important to note that anything that comprises Darknet has to use TCP/IP protocol. It has to be internet accessible and more importantly it has to prevent your anonymity. Darknet is sometimes rumored as “commercial underworld” because it is the place where weapons, drugs, pirated DVD’s are traded without any fear of police and DRM (Digital rights management).

III. Tor (The Onion Router)

TOR is a free software which was developed by U.S. Navy in mind, for the purpose of protecting government communications.It allows groups and individuals to communicate and share information without any fear of losing anonymity. The main idea behind using TOR was that user can route his data through 3 different nodes (entry node, exit node and middle node) so that he can bypass security filters which are restricting him to access that website. (see fig 1)

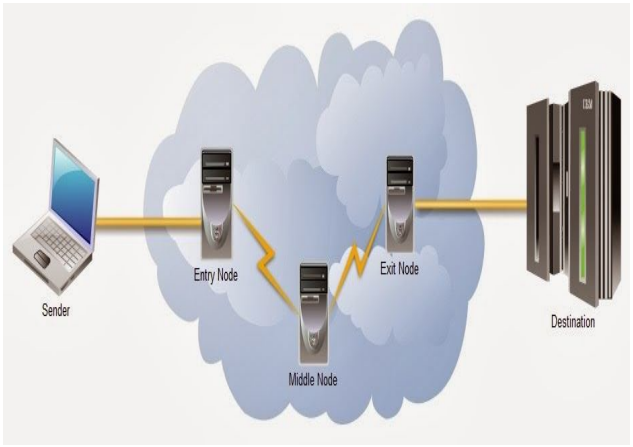

Fig 1:- TOR nodes

So if he is in a autocratic country and he want to access a website which is banned in his country he can access that website by installing TOR in his computer and by this he will be able to connect to TOR network and it will then route data/communication through 3 nodes and by this he can access that website without being tracked easily. It is also important to note that, InsideDarknet links are encrypted which increases privacy to a higher level.

1. How TOR works..?

Let us take an example of a user who wants to access a website which is banned in his country but by using tor he wants to access that website for good or bad reasons. So by following steps he can do this:

Step 1: User's tor client obtains a list of Tor nodes for the directory server. In the given figure Tor nodes are represented as '+'. (Fig 2)

Fig 2: User's TOR client obtains a list of TOR nodes

Step 2: Now TOR client picks a random path to destination server of blocked website. In this process user's data will berouted through 3 different computers or nodes that are part of this tor network and are located at 3 different geographical locations.

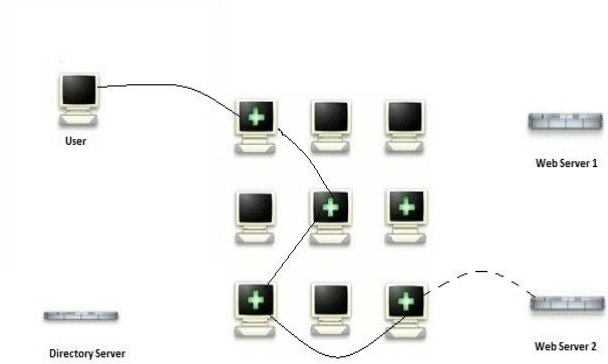

Fig 3: TOR client picks a random path to destination server

It is also important to note that, inside the TOR network links are encrypted. In the above given fig: 3 thin dashed lines are representing un-encrypted links and continuous thin lines are representing encrypted links.

2. TOR Hidden Services

Tor allows users to hide their locations while offering them various kinds of services such as web publishing or instant messaging and other users can connect to these hidden services without knowing each other's identity so users can set up a website and can publish data without taking care of censorship or being located.

3. TOR Security Concerns

Although TOR can protect anonymity of a user to a good extent but still there are ways by which user can be tracked. The main problem with TOR is that it only protects the transport of data but if the user's computer is infected with some virus, malware or any spyware then his anonymity can be cracked easily .There are many other ways by which user can be tracked, Some of threats about which user should be concerned are explained below:

A) Key loggers/spywares: These are the software's that has the capability to record every key stroke made by the user or can spy each activity done by the user depending upon without any permission of user. By these users, data can be retrieved directly from his computer and this can become a threat to user's anonymity.

B) JavaScripts:JavaScripts is one of the biggest threats that user should be concerned about. These scripts can leak a lot of information about the user and even the IP address of the user can be tracked by these java scripts without any permission and by this anonymity of user.

C) While using TOR user should be concerned about other Internet applications that are running in background should be turned off because these links are not encrypted and if someone is watching the data traffic he can locate the user.

D) As we know TOR network consist of 3 relays or nodes (namely entry node, middle or relay node and exit node) and if a person somehow monitors these 3 relays he can locate from where the traffic is coming from.

There are still many other ways by which user can be tracked and to maintain this anonymity user has to take a lot of precautions and also has to install much different software on his computer.

IV. Conclusion

Darknet hasbecame a big concern because of increase in illegal activities such as drug dealing, contract killing and Black-marketing .Today, millions of people use TOR to protect themselves from being tracked while surfing the web but intelligence agencies has discovered multiple ways by which they can retrieve the identity of user. Although user can still install some additional softwares to make sure his/her privacy is not compromised.

V. Acknowledgement

I want to acknowledge my tutor Dr. GarimaGoswami for encouraging me. I also want to thank my parents for supporting me and God for giving me courage

VI. References

[1] https://www.torproject.org

[2]http://www.elithecomputerguy.com/

[3]http://www.ubertechblog.com/2011/07/beginners-guide-to-deep-web-or-darknet.html

[4]http://en.wikipedia.org/wiki/Tor_(anonymity_network)

[5]http://www.pcworld.com/article/2052149/tor-stands-strong-against-the-nsa-but-your-browser-can-bring-you-down.html

[6]http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption