Navigating the Dark Web

Paulo Lima and Maria Silva

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89983,a83840}@alunos.uminho.pt

Abstract. The internet is the perfect way to share information, and with the proper tools such as The Onion Project it is possible to communicate having a small risk of detection, its services facilitate the creation of hidden sites and users. This paper objective is to enlarge the view of the reader about the internet and the uses of the Dark Web.

1 Introduction

The services Tor and others alike allow private and anonymous connections to the internet. Websites that use those same services are known as Hidden services. These sites and others that use protocols or tools like Tor form darknets, and all together the dark web. The dark web is just a small portion of the deep web, since a lot of content in it can't be accessed through normal search engines. The deep web is considered to be much larger than the surface web, but due to it being very hard to search its size is very hard to determine. Services like Tor allow criminals, people trying to escape censorship, and overall privacy searchers. . ...

2 Internet

2.1 Layers of the Internet

The internet is not the same as the World Wide Web (web), it's much bigger. There are a set of websites that can be accessed through a common search engine like Google and others, but that is just a little fraction of the internet known as "Surface Web". The other fraction, thought to be much bigger, is the Deep Web, unlike the web, it is not indexed by search engines, this fraction includes private intranets and commercial databases. The Dark Web is a part of the Deep Web that is hidden so that its users can be able to share information with more security and anonymously. This power is used both for legal and illegal activities.

3 TOR

3.1 History

Tor is based on the principle developed by Paul Syverson, Michael G. Reed and David Goldschlag, called "onion routing". It was developed in the U.S. Naval Research Laboratory in the 1990s, and funded by DARPA (Defense Advanced Research Projects Agency). Its initial purpose was anonymizing traffic so that, for example, undercover agents could communicate without being detected and officials were able to visit websites without a government IP address showing. However, if all users were law enforcement, it would lose it's purpose, as it would be easily identifiable that all Tor connections were from law enforcement. Therefore, the project had to be used by all - those enforcing the law, those breaking it, and those just looking for privacy. This allowed users to truly camouflage themselves because a Tor user could be anyone.

3.2 Purpose

Tor can be used for a myriad of reasons, being themselves legal or illegal. Tor provides an easily accessible tool to anonymize the user internet navigation.

3.3 How it works

Tor passes traffic through at least 3 different servers before sending it on to the destination. Because there's a separate layer of encryption for each of the three relays, somebody watching your Internet connection can't modify, or read, what you are sending into the Tor network.

Traffic is encrypted between the Tor client and where it pops out somewhere else in the world. Each relay only decrypts enough data in the packet to know he location of the previous and next relays. Since each path is randomly generated and none of the relays keep records, none of the nodes (relays) know both the user's ID nor the destination's ID, making it almost impossible for the activity to be traced back to the user. Tor relay nodes are simply connections through Tor users that have volunteered bandwidth to Tor for this purpose.

There is a possibility that the first server can see encrypted Tor traffic coming from the user's computer. It still doesn't know who the user is or its activity. It can only see "This IP address is using Tor". Tor is not illegal, so using Tor by itself is fine although it may raise suspicion.

There is also a possibility that the third server can see the traffic that was sent into Tor, but it doesn't know who sent it. If the user uses encryption (like HTTPS), it will only know the destination.

3.4 Silk Road arrests

It is interesting to understand what went wrong on the Silk Road case, so here are a few things that led to the arrest of Ross Ulbricht.

Ulbricht was first connected to "Dread Pirate Roberts" by linking the username "altoid", used during Silk Road's early days to announce the website, and a forum post in which Ulbricht, posting under the nickname "altoid", asking for programming advice, giving his email address and real name.

The FBI has claimed that the real IP address of the Silk Road server was found via data leak directly from the site's CAPTCHA and it was located in Reykjavík, Iceland.

Despite his apparent success building 'the eBay of hard drugs' through anonymous servers and a hidden identity, the man known as 'Dread Pirate Roberts' began to leave a trail of traceable activity social media:

- Even though he probably wasn't counting on working "traditionally" again, Ross Ulbricht maintained a profile on LinkedIn while he was allegedly running the Silk Road. His mother claimed that this profile referred to a MMORPG, not a darknet market, when it stated, "I am creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force." It was then suspected that this "economic simulation" referred to by Ulbricht was Silk Road. - A package was intercepted as part of a routine mail search, with his address on it, and found to contain nine fake IDs, each with a different name but all with a real photo of himself. Dread Pirate Roberts explained that he "needed a fake ID to rent servers". - Registered on Stack Overflow with his personal email address, and username 'Ross Ulbricht', he posted the question "How can I connect to a Tor hidden service using curl in php?", which later lead to suspicion as the code was very similar. Christopher Tarbell stated: "The computer code on the Silk Road web server includes a customized PHP script based on "curl" that is functionally very similar to the computer code described in Ulbricht's posting on Stack Overflow, and includes several lines of code that are identical to lines of code quoted in

the posting. - Ulbricht asked on Google+, where anyone can see both his real name and real face, "Anybody know someone that works for UPS, FedEx, or DHL?". On his Youtube profile, linked to from that page, one of the videos he saved was "How to Get Away with Stealing". - Later it was found that Ulbricht kept a journal, leading to the discovery that he didn't run the site alone. "He was the biggest and strongest willed character I had met through the site thus far," Ulbricht wrote in a 2011 journal entry, talking about a user best known by Variety Jones. "He has helped me see a larger vision, a brand that people can come to trust and rally behind. Silk Road chat, Silk Road exchange, Silk We think this is an interesting topic, and learned Road credit union, Silk Road market, Silk Road everything!"

3.5 Anonimity

The main concern for users of Tor is to keep an anonymized internet experience with maximum privacy. It is very hard to achieve a malicious attack unveiling a Tor user identity without the said user has made some flawed actions. Discovering a user IP or MAC address can lead to much more information being given to the attacker, such as the user location. Tor has multiple security measures but it is still possible to access the originating and destination IP, for example two malicious nodes serving as entry and exit node can be very dangerous although such occurrence is very unlikely. The anonymity of the user in the internet is also dependent of which sites they visit since it's also possible to have malicious scripts that would identify the user, even on hidden services. Currently it is possible to get a warrant just based on internet traffic of a certain person that uses Tor.

3.6 NSA Tracking

It was found that through NSA's XKeyscore, anyone who downloads Tor is automatically fingerprinted electronically, which makes it possible to identify users who think are untraceable. Even just investigating privacy-enhancing methods from outside of the United States is an act worthy of scrutiny and surveillance according to rules that make XKeyscore. Searching for the Tails operating system, will also land you on the deep-packet list. Even though your ISP (Internet service provider) can't see what you're doing, it can see that you're connected to Tor. So, even if you're only using Tor to legally browse anonymously, just being connected to Tor can raise suspicion from the government surveillance. One way to avoid this may be connecting to a VPN before using Tor. This hides your activity from your ISP and prevents it from knowing you're using Tor.

3.7 Vulnerabilities

Users are still targets to malicious attacks since hidden service, a public website or even the Tor network can't ever completely eliminate these threats. Malicious scripts and cross-scripting are some of the ways clients can still be infected. Tor is also not danger free since a malicious exit node has access to the data flow and can inject malware in a connection that is not encrypted. Some malicious nodes perform sslstrip which can convert HTTPS request to the HTTP equivalent, this allows a breach in security that may lead to a leak of sensitive data such as usernames and passwords. SSH connections can also be interfered, although is harder since due to the nature of SSH the attacker would need to interfere the first time the client used the connection. Tor system to prevent this situations is to give a flag representing a status on each node, bad nodes would be classified as a BadExitNode which would stop them from being exit nodes again, but not from being used as relay nodes. Relay nodes are much weaker since data flowing is encrypted, but if relays are being used for malicious intents Tor will ban them which would classify them as unusable, but nodes are not the only way attacks are made, traffic patterns together with Tor network monitoring can help identify the types of some nodes and the users connected to their request, although

this method requires large amounts of resources. We can assume from all of this that Tor is a good tool to anonymize your internet traffic but it doesn't protect you from the same exploits you would find in the surface web.

3.8 Censorship

For most people reading this article, Tor Browser is completely legal to use. In some countries, however, Tor is either illegal or blocked by national authorities.

- China has outlawed the anonymity service and blocks Tor traffic from crossing the Great Firewall.

- Countries such as Russia, Saudi Arabia and Iran, are working hard to prevent citizens from using Tor.

- Most recently, Venezuela has blocked all Tor traffic. "Restricting access to information, and the tools necessary to access that information safely, is a flagrant violation of human rights by the Venezuelan government," said Javier Pallero, Latin America Policy Lead at Access Now.

4 Conclusions

Privacy is a right, not a priviledge, and it shouldn't be denied to anyone. Unfortunately, that is not the case, but we hope that some of the insights in this paper may help the reader to be better protected and informed. Working on this subject has made us learn even more about privacy, and the pros and cons of using Tor, so we think it was really helpful to have chosen this theme.

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." - Edward Snowden

5 References

https://2019.www.torproject.org/docs/faq.html.en

https://www.theguardian.com/technology/2013/oct/03/five-stupid-things-dread-pirate-roberts-did-to-get-arrested

http://www.wired.com/2015/02/ross-ulbricht-didnt-create-silk-roads-dread-pirate-roberts-guy/

https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/

https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn

"The Onion Router and the Darkweb", Corianna Jacoby

"Dark Web", Kristin Finklea