Concordia Institute of Information System Engineering (CIISE)
Concordia University

ENGR 6991 Project and Report III

Research Project Progress Report : Tor/Onion Hidden Service Deanonymization Techniques

Submitted to :
Prof. Ivan Pustagarov

Submitted by :

Student Name	Student ID
Riya Vinodbhai Patel	40224858
Hulli Rahul Ravi	40234542
Jubin Raj Nirmal	40235087

Current Milestone

The current milestone within the project is to select .onion sites for investigation to deanonymize Tor server users. Our specific criteria revolve around .onion sites that have "server-status" page enabled on the local host. We are specifically interested in websites that are relatively new, typically having been established within a few hours or days. The justification behind this choice is the assumption that owners of such recently created sites might lack the technical knowledge necessary to disable the server status option.

We have approached this objective using two different strategies. The first method includes using Tor on Whonix, which entails installing Whonix within a virtual machine (in our case, VirtualBox), and then using Whonix to run Tor. The second method would be Tor on Host, where Tor would be installed directly on the host system while utilizing a different network connection.

Progress

By far, to give an estimate, we have traversed up to 200-250 .onion websites in total, out of which we were able to find one confirmed .onion site with server-status enabled and 4 potential .onion sites. The reason why those are potential sites is because /server-status against these sites do not return a landing page. They will be inspected under a tool called Onion Scan, which will scan all the links to reveal potential IP address / link of the .onion website. The search for the .onion sites is done through the Ahmia search engine, the Torch search engine and Not Evil search engine. These .onion links will be scanned under onion scan and the results will be analyzed for deanonymization. Installation of whonix on virtual box, onion scan service, Tor browser was completed much earlier.

Challenges Faced

1. Time constraints: Time has been a major issue, as my team has not been able to dedicate enough time to this project due to other commitments. Though, the team is slowly back on track and the project is in a smooth flow.
2. Bugs related to Whonix: Whonix needs a special kind of system configuration to work on. Particularly, I spent about 30% of the available time to fix any issues I faced running Whonix on my system, then just reverted back to installing tor on host and resume with an alternate network connection.
3. Bugs related to onion scan: Onion scan is a very unstable tool if it's installed on a ubuntu based system. It stops functioning after a few scans. As of the moment, we have just one system that's able to run onion scan effectively.
4. Getting a .onion site that can be used for the research: It's observed that most of the Tor sites that we have traversed by far cannot be used for the research to be deanonymized. At the same time, Tor does not show Tor sites that have been just created and running.
5. Not Evil search engine is not always up: Not Evil search engine returns a lot of popular and unpopular websites that can have potential to be used for the project. But the times it would be up, and running is not predictable, its mostly inactive.
6. Ahmia Blacklist: Ahmia has blacklisted a lot of websites already (which is generally a good thing, but it doesn't help the project), hence, this makes it all the more difficult to get a website which can be deanonymized.

References

[1] DEFCON30 Ionut Cernica: Deanonymization of TOR HTTP Hidden Services https://youtu.be/v45_tkKCJ54?si=1Y2Hsm_aRY_Bz507

[2] LayerOne 2018 - Leeky Onions (Zorro): https://youtu.be/LN4mfmfZ69s?si=n2Ogo1NIXW3sl5W8

[3] Onion Scan KitPlot: https://www.kitploit.com/2016/04/onionscan-onion-services-security-scan.html?m=0 , https://github.com/s-rah/onionscan

[4] Setting up Whonix: https://www.youtube.com/watch?v=rUzeuYTYucw

[5] Best Darknet Search Engines: https://www.avast.com/c-best-dark-web-search-engines

[6] Ahmia Blacklist: https://ahmia.fi/blacklist/