Measuring the Accessibility of Popular Websites while Using the I2P Anonymity Network


[2]

Introduction

- Having an anonymous identity online is desirable for various reasons (online privacy, whistleblowing, safely accessing medical information).
- Anonymity networks such as I2P (the Invisible Internet Project) enable users to browse the web anonymously by providing additional encryption through garlic routing.
- However, blocking behaviour might be encountered due to their association with criminal activity.

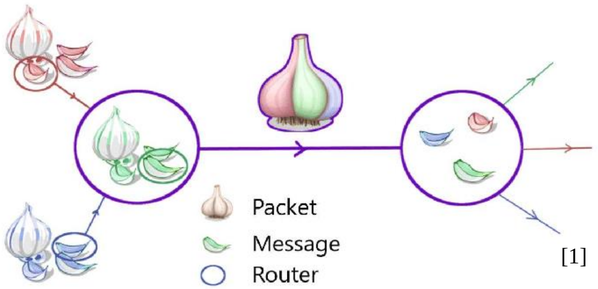

Figure 1: Garlic routing encryption method

Questions

- To what extent do websites block users accessing them using I2P?
- How frequent is blocking and which content does it affect?
- Are there specific website categories that are more prone to implement blocking mechanisms?

The Experiment

- Deploy a spider to crawl popular websites.
- To ensure that the experiment is conducted responsibly, the crawler will respect the Robot Exclusion Protocol and will quit requesting websites after three attempts that result in no response.

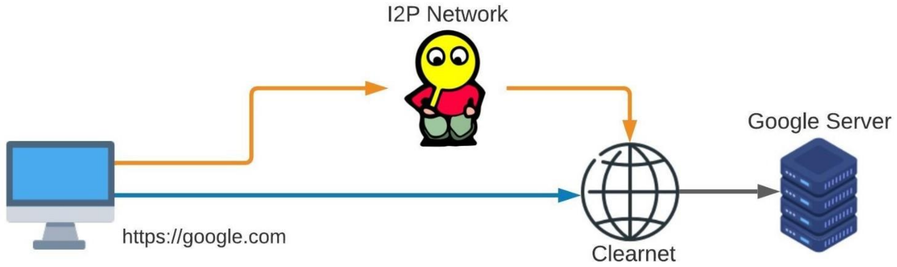

Figure 2: Experimental setup

Results

- The dataset consists of the top 500 websites from Moz [3].

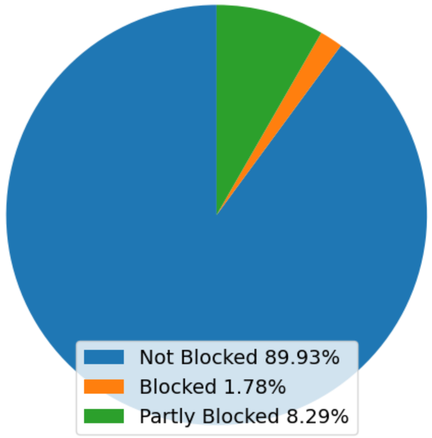

Figure 3: Proportion of successful, blocked, and partly blocked requests

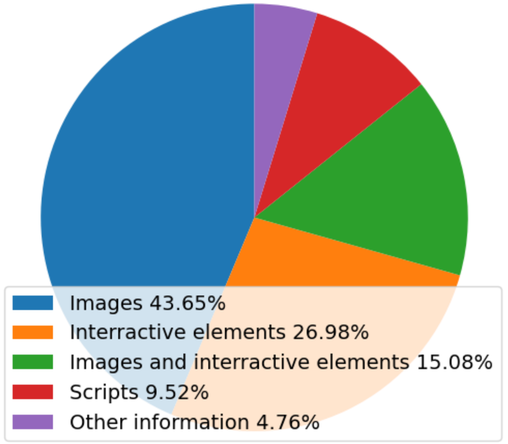

Figure 4: Content affected by partial blocking

- 89.28% of I2P requests were successful with respect to the control request, 9.14% were partly blocked and 1.58% were blocked.
- The content most affected by blocking are images, followed by interactive elements and scripts.
- The categories of websites that presented with blocking include news 23.3%, blogs/wiki 10.2%, business 8.7%, internet services 8%, and others.

Conclusions

- 10.7% of I2P requests show blocking behaviour when compared to the control requests.
- However, I2P has certain bandwidth limitations since it was designed for internal P2P use.
- On average 7.3 out of 15 I2P requests fail due to I2P network failures.
- Therefore, some negative results could be the result of I2P accessibility issues.

References

[1] Andrei Dakhnovich, D. Moskvin, and D. Zegzhda. “Approach for Securing Network Communications Modelling Based on Smart Multipath Routing”. In: *Nonlinear Phenomena in ComplexSystems* 23 (Dec. 2020), pp. 386–396.
[2] I2P's mascot, itoopie, who is looking through a magnifying glass, en.wikipedia.org/wiki/I2P
[3] moz.com/top500

Paula Iacoban
I.P.Iacoban-1@student.tudelft.nl
Supervisor: Stefanie Roos