Ministry/Organization Name/Student Innovation:
National Technical Research Organisation,(NTRO)

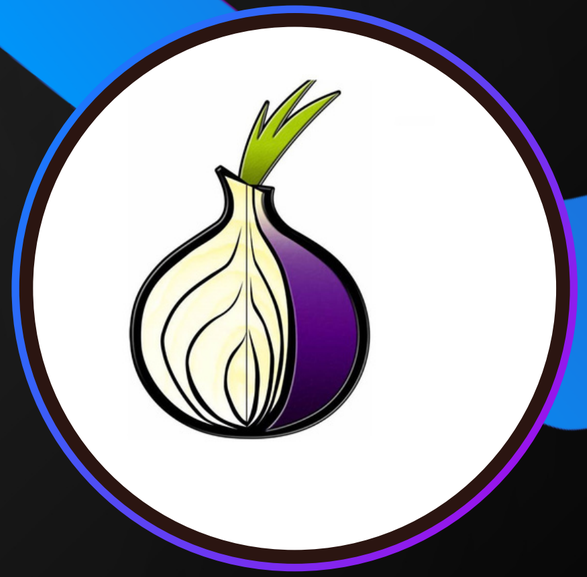
PS Code: SIH1455

Problem Statement Title: Efficient enumeration of URLs of active hidden servers over anonymous channel (TOR)

Team Name: Binary Brains

Theme Name: Blockchain and Cybersecurity

EFFICIENT ENUMERATION OF URLS OF ACTIVE HIDDEN SERVERS OVER ANONYMOUS CHANNEL (TOR)

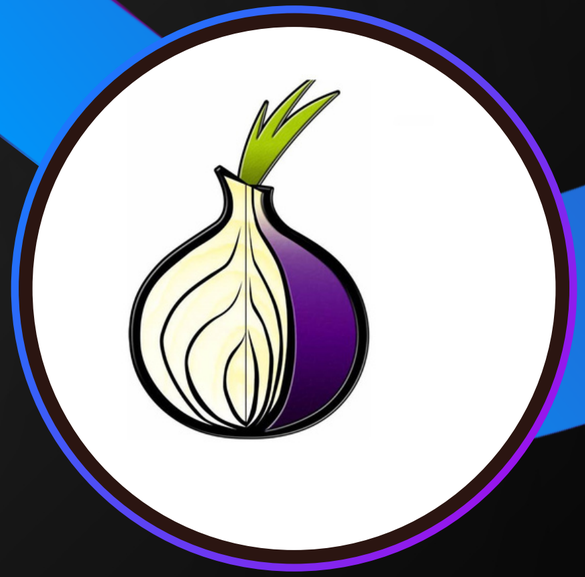


Basic references

Anomaly Detection - Employ anomaly detection mechanisms that can identify deviations from normal network behavior. This can help in identifying malicious activities that may not be immediately apparent.

Traffic Analysis - Analyze network traffic to identify patterns and anomalies. Tor traffic can often be identified through its distinctive characteristics. Tools like Bro/Zeek can be configured to detect Tor network traffic.

TOR
THE ONION ROUTING



Free and open-source software for enabling anonymous communication which directs Internet traffic via a free, worldwide, volunteer overlay network that consists of more than seven thousand relays

Our Goal

Moderation of .onion URLs in Tor using Parent-child bot instance.

Maintainance of Traffic regulation.

Restrictions on the illegal sites using anonymous Tor channels

Using modular bots that keeps up with Tor's promise on privacy and anonymity.

WORKFLOW

01
Ideation

02
Planning

03
Development

04
Presentation

Ideation

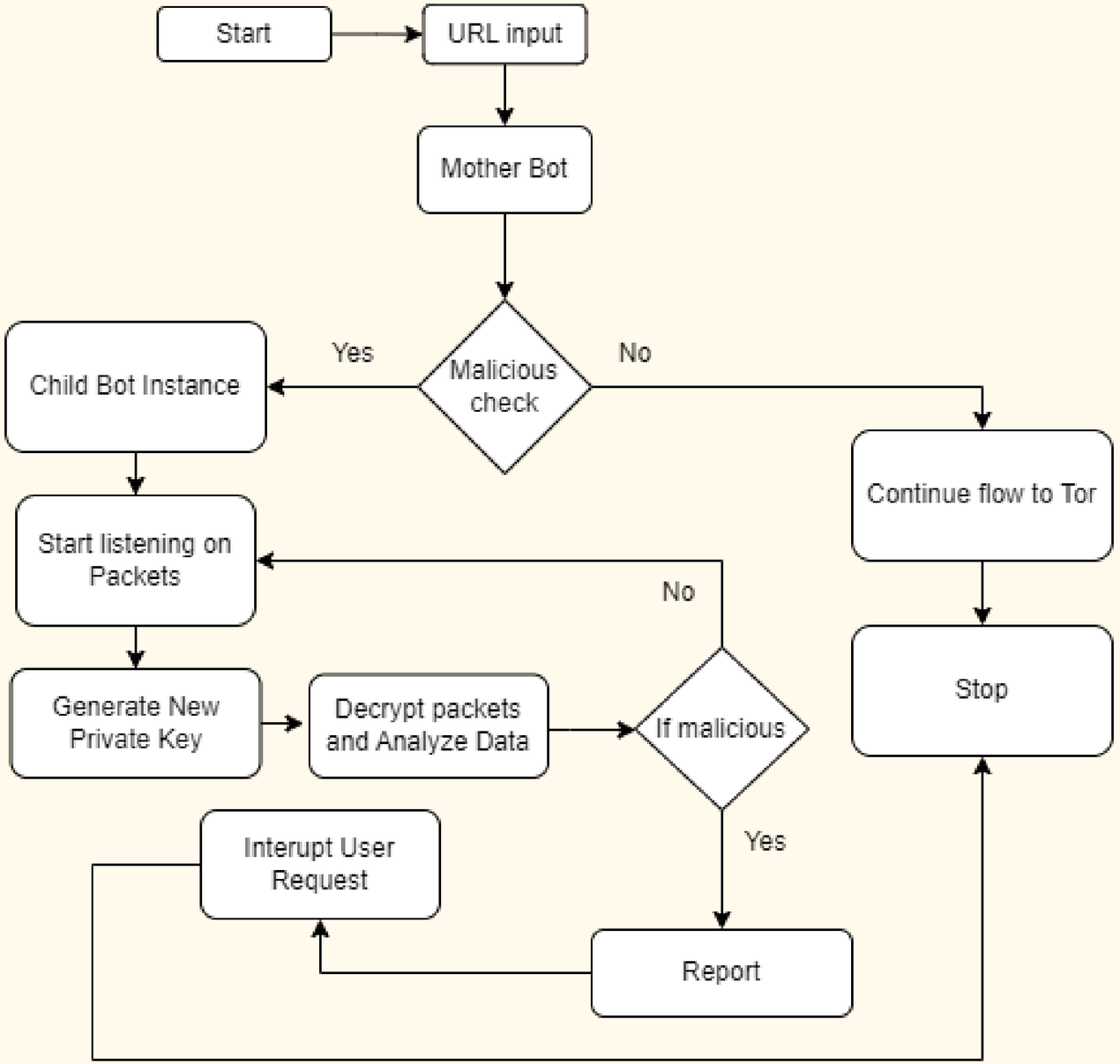
OUR BOT - EAGLE

The bot analyzes network traffic within the Tor network, examining data packets and connections to identify patterns, helping to trace the malicious activities by sending data from anonymous websites.

Why Eagle?

Bro/Zeek was a open-source network security analysis monitoring tool software vs Eagle can be highly customised to the user’s specific needs and deep contextual understanding of the users network and systems and response flexibility. Eagle can adapt quickly to changing situations and respond to incidents in real-time.

Approach


Start
URL input
Mother Bot
Malicious check
Yes
No
Child Bot Instance
Continue flow to Tor
Start listening on Packets
No
Generate New Private Key
Decrypt packets and Analyze Data
If malicious
Stop
Yes
Interupt User Request
Report

Development

STAGE 1: CREATION OF A BOT

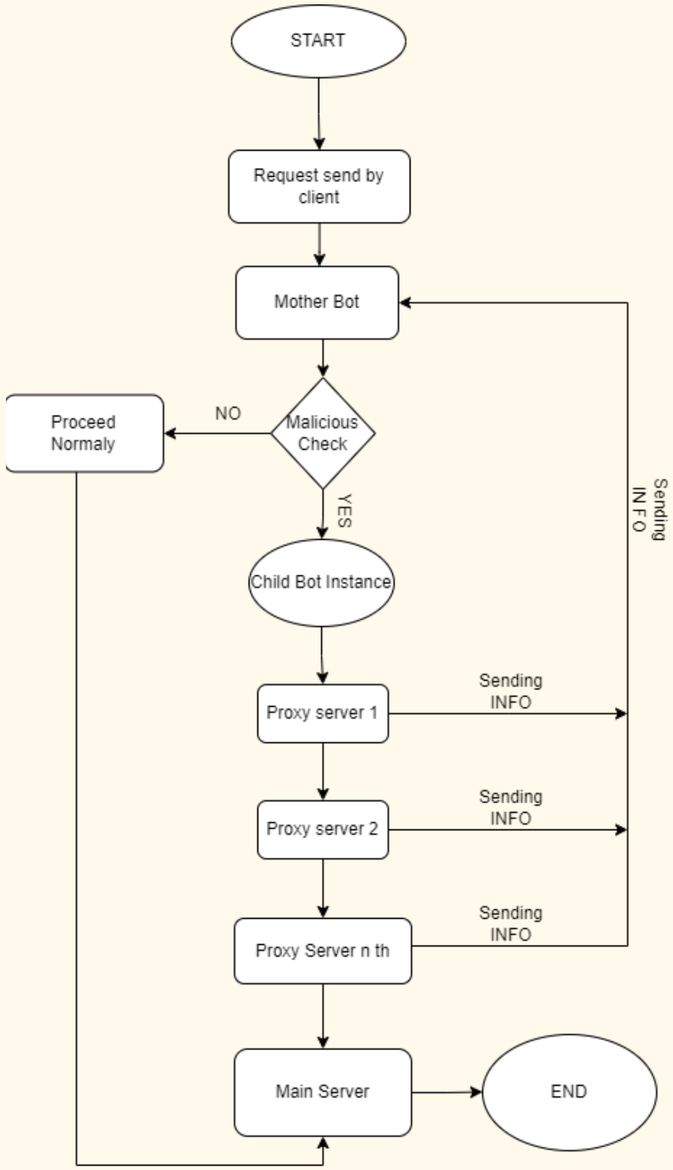
We tried to create a basic bot that fetches information from the server by directly communicating with the server.

Development

STAGE 2: CREATION OF A TOR LIKE NETWORK

We tried to create a network which acts as a clone to a TOR network to implement our idea of node hopping on a small level.

Working of Eagle



Conclusion

We performed many test cases that consisted of creating a bot with Postman API, but we couldn't execute that properly because we lacked information about API. We also checked the path of the packet over IP on Surface Web and tested the same for the Onion website, but it didn't work with the dig command. We visited one of the onion sites and checked its source code. We found one server trace with the name "Infocon.org", We fetched and succeeded in finding the server IP, which was 50.230.231.89

Conclusion

We tested the server IP with n-map and found the following open port: nmap 50.230.231.89 Starting Nmap 7.93 (https://nmap.org) at 2023-09-27 13:36 UTC Nmap scan report for 50-230-231-89-static.hfc.comcastbusiness.net (50.230.231.89) Host is up (0.017s latency). Not shown: 990 filtered tcp ports (no-response) PORT STATE SERVICE 21/tcp open ftp 25/tcp open smtp 80/tcp open http 110/tcp open pop3 143/tcp open imap 443/tcp open https 465/tcp closed smtps 993/tcp open imaps 995/tcp open pop3s 6346/tcp closed gnutella.

Conclusion

In summary, the efficient enumeration of URLs of active hidden servers over the anonymous channel Tor presents a multifaceted challenge that encompasses understanding the Tor network, monitoring for malicious bots, countering the creation of such bots, and addressing the emergence of Tor-like networks.

References

- *Bro/Zeek - open-source network security analysis monitoring tool*
- *Research paper from GoogleScholar*
- *Geeksforgeeks*
- *ChatGPT*
- *Github repo*
- *Youtube*