MALICIOUS DOMAIN DETECTION

23rd December 2021

Speaker: *Gopinath Palaniappan*

Outline

- Common uses of maliciously registered domains
- Approaches to detect malicious domains
- Datasets for research

Common uses of maliciously registered domains

1.

- Manipulate to webpage similar to a reputed website

2.

- Data Exfiltration

3.

- Download malware

4.

- Redirect to other malware hosts

5.

- Remote control your network resources

6.

- Crash infrastructures

Approaches to detect malicious domains

Blacklist

- Reputation based on history

Lexical Features

- Length
- Characters ratio, continuity rate
- Phrases

Global ranking

- Alexa
- DomCop
- Majestic
- Google Page-ranking

Registration data

- RDAP
- IPWhois
- DomainWhois

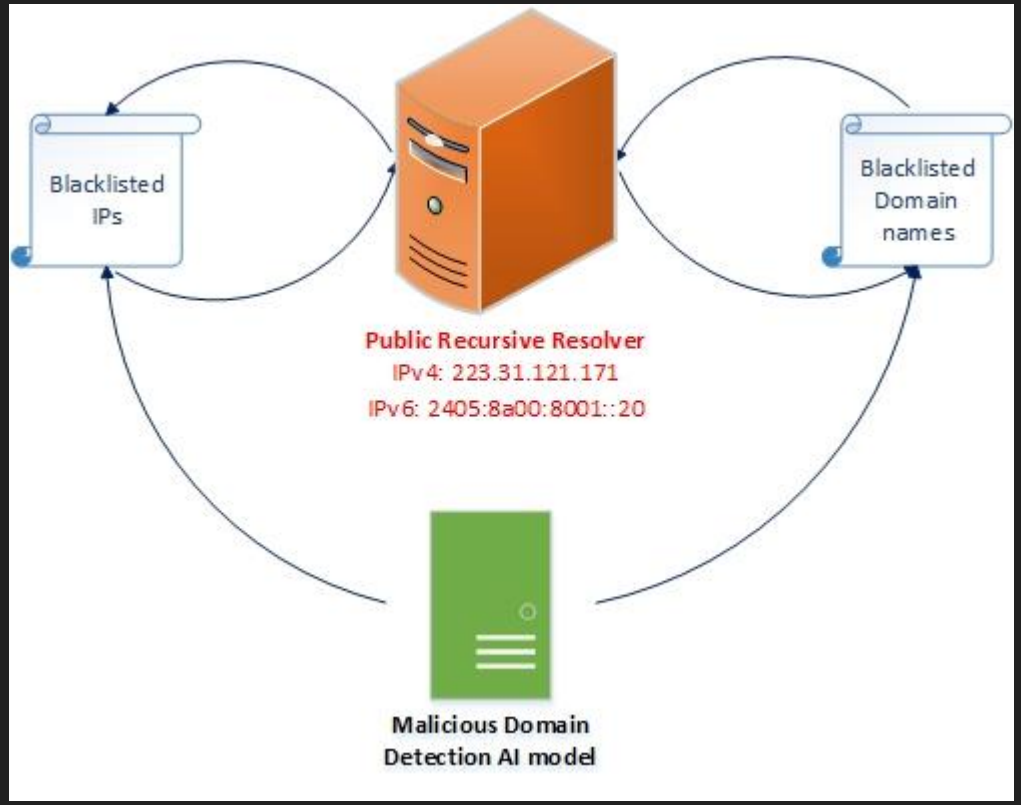
Web Traffic

- Visitors count
- Stay time
- Web referrals

Category & Content

- Type of website
- Number of pages
- Broken links

Deployment of the Malicious Domain Detection



Datasets for research

- Spamhaus DBL
- SURBL
- IANA
- ICANN
- Our own datasets

Thank You