



+

•

○

# TN POLICE HACKATHON

Tracking Phishing Message

Team: Script Kiddies

A vertical bar on the left side of the slide with a gradient from orange at the top to purple at the bottom.

# MEET OUR TEAM

## KUMARAGURU COLLEGE OF TECHNOLOGY COIMBATORE

MENTOR

Dr. SUGANTHI N

TEAM MEMBERS

RAJHESHWAR V

MANAVALLAN S

VISHAL M L

DHANUSHKUMAR S G

# Introduction

*"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it."*

*– Stephane*

- <sup>Nappo</sup> Over 255m phishing attacks in 2022 so far.
- Estimated an 80% increase in threats from trusted services such as Microsoft, Amazon Web Services or Google, with nearly one-third (32%) of all threats now being hosted on trusted services.
- The top 3 attack sectors are Healthcare, Professional and Scientific Services, and Information Technology.

# Problem Statement

- It's required to trace the phishing messages to locate the cyber attacker on citizens, who fell into the trap of clicking the link shared or giving important login credentials.
- So, Police to get a handy interface with a solution that can fetch the details of servers or mobile numbers (dynamically changing in this case) and provide investigators sufficient information to trace and track the perpetrator.

# Solution

- Categorizes the message and validate the contents of the message by performing domain validation and malware analysis for email headers and malicious files respectively.
- We built our own scripts and user interfaces to gather information.
- Our tool will help the user to get an overview of security posture of an attacker such as location, public username, etc.
- We designed a tool that has a handy User Interface that retrieves information about the domain of originated Phishing Link.

# Functional Features

- Spam/Phishing Link Identification
- Email Header Analyzer
- URL examination and Data Gathering
- Location and mobile number tracker
- DNS and IP address lookup
- Network scanner
- Malware Analyzer

# Architecture

## Email Header Analyzer

- Extract IP Addresses
- Extract Domain Name
- Creation time
- Extract Username
- Extract File Path
- Extract Email Addresses
- #Mobile number lookup

## URL and Network Analyzer

- Network scanner
- Domain details fetcher
- SSL Certificate Details
- OS Detection
- Subdomain Enumeration
- DNS, IP lookup
- Geolocation of IP

## Malware Analyzer

- File type identifier
- Target OS
- File Format
- Malware Hash examine
- Malware metadata extraction
- Strings analyzer
- #Packing and Obfuscation
- #PE Header Analyzer

# Final Output

- Information gathering about the attacker as close as possible
- Our dashboard will display the IP address, usernames, emails, domain and server details, mobile number lookup in order attain his public identity
- Provided geolocation, identifying and bypassing CDN networks will help to detect the public IP of the attacker
- With this information, we can lend a supporting hand from the ISP and the cloud vendors to retrieve further information about the attacker
- Generating an overall report with the information gathered



# Innovation

- Providing an open-source framework and generating an API for fetching the attacker's details specifically
- Scripting the module architectures and interactive user interfaces
- Integrating tools in a strategical manner which works in a well-structured flow in information gathering and attacker tracking
- Performing malware analysis may provide us with additional information about the attacker such as backdoor information which can be used to trace the foot-prints of the attacker
- Predicting the attacker's public identity such as username, location, IP, reverse number lookup, and email using social platforms

# TECHNOLOGY STACK

- Automated framework - Stacks used:

## LANGUAGES

- Python
- HTML
- CSS
- Bash

## API

- IP API
- Wappalyzer
- DNS For Family

## FRAMEWORK

- Django

## Python Packages

- Py-Nmap
- DNS Resolver
- Pycrtsh

# Demonstration

The screenshot displays the Spoor web application interface. The browser address bar shows the URL `localhost:8000/spoor/2222`. The application has a blue sidebar on the left with the title "SPOOR" and navigation options: "Scan", "Email Header Analyse", and "Malware Analysis". A back button is also present in the sidebar.

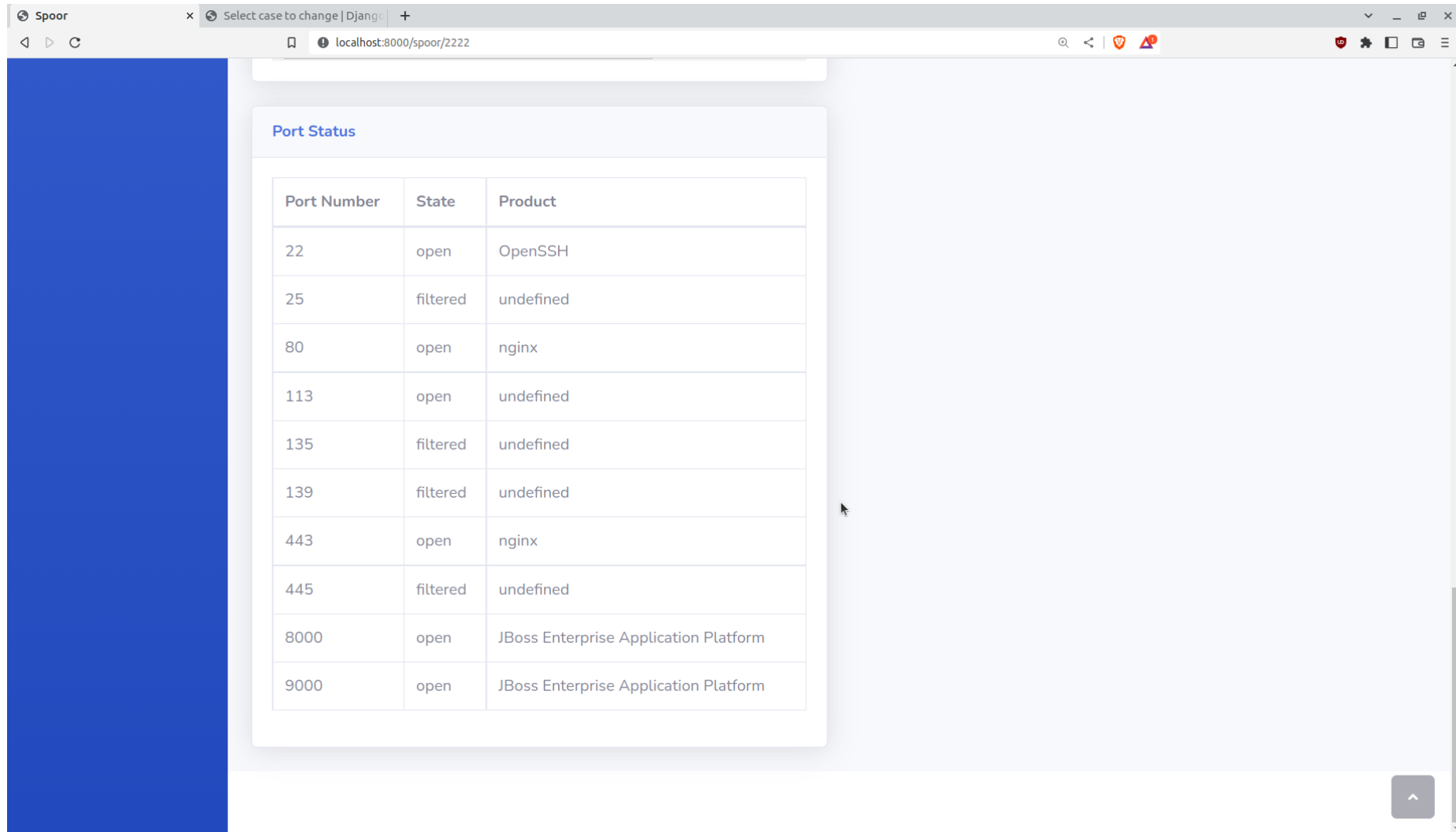
The main content area is divided into several sections:

- Is it Adult content webpage:** Displays the text "undefined".
- IP Address:** Displays the IP address "192.46.209.55".
- Domain Details:** A table showing various domain attributes.
- Map:** A Google Map showing the location of the IP address, with markers for "R.P. Electrical", "BMC Garden", "Aziz Enterprises", "Makdhum Mobile Shop", "Pandit Kailas Maharaj Damudre", and "A1 Honda Service Point".

The Domain Details table contains the following data:

Name	Value
ip	192.46.209.55
network	192.46.208.0/21
version	IPv4
city	Mumbai
region	Maharashtra
region_code	MH
country	IN
country_name	India
country_code	IN

# Demonstration



Port Status

Port Number	State	Product
22	open	OpenSSH
25	filtered	undefined
80	open	nginx
113	open	undefined
135	filtered	undefined
139	filtered	undefined
443	open	nginx
445	filtered	undefined
8000	open	JBoss Enterprise Application Platform
9000	open	JBoss Enterprise Application Platform

# Demonstration Video link

**Youtube:** <https://youtu.be/0OmTgwTaBW4>

# ADVANTAGES:

- Feasible
- Time efficient
- Low-cost maintenance
- Less resource consumption
- Performs malware analysis
- Works in a very strategical manner
- Collects precise information about the attacker



**THANK YOU**