Detecting Phishing Links & Identifying Black Hats

VENGER

Team Zeta

Problem Statement

This world of highly interconnected people has exposed an increasing risk in terms of phishing attacks on the people as well as on the organization. Cyber attackers have also become very intelligent in composing their malevolent messages and tricks which incite the users to click on links of malware and reveal all their private details

The most of the solutions try to see which threats should be blocked or detected, whereas it forgets who these attackers are. That's why this creates a threat to its users and shows them vulnerability, and without any hint about what may be done against such an attack.

Solution :

Proposed Solution

- Our solution uses an isolated sandbox with VMs and monitoring tools like Wireshark and Zeek for phishing detection. Integrating threat intelligence sources (VirusTotal, AbuseIPDB) and visualizing data in ELK enables safe, automated analysis of malicious links and patterns.

- After the detection , we will Gather all the information about the Sender using the process called ReverseShell. And from the customer,end by themself they can send all the gathered information will be filed as a report to the Cyber Department So that they easily verify all scammers and Black hat hackers Protecting The Children In The Digital Space From Various Threats Such As Cyberbullying , Viruses ,Sexting, invasive Advertising, phising Attacks.

Tech Stack

DOCKER container → Scanning all the phishing links using the docker

→ **Live Boot** → Dark Network →

Zeek tool → **VENGER** → Wire Shark

→ Sand Box → Endpoint security

→ Reverse Shell (Payload)

Sandbox in our custom environment → Githubgit
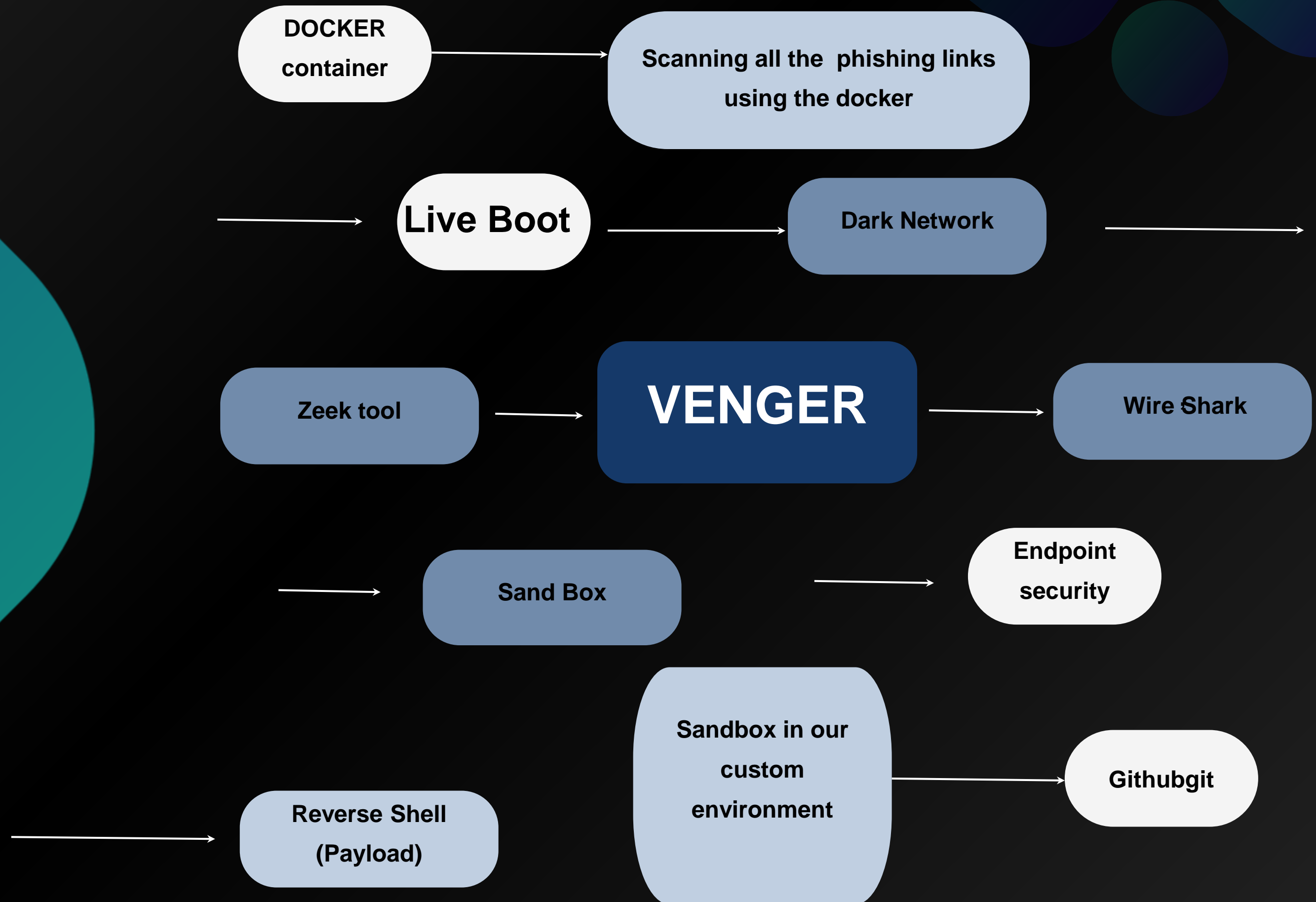
Dependencies

Libpcap / tcpdump

Essential for capturing network packets.

Glib and GTK

Required for Wireshark's graphical interface on some

Linux systems.

SSL Libraries (e.g., OpenSSL)
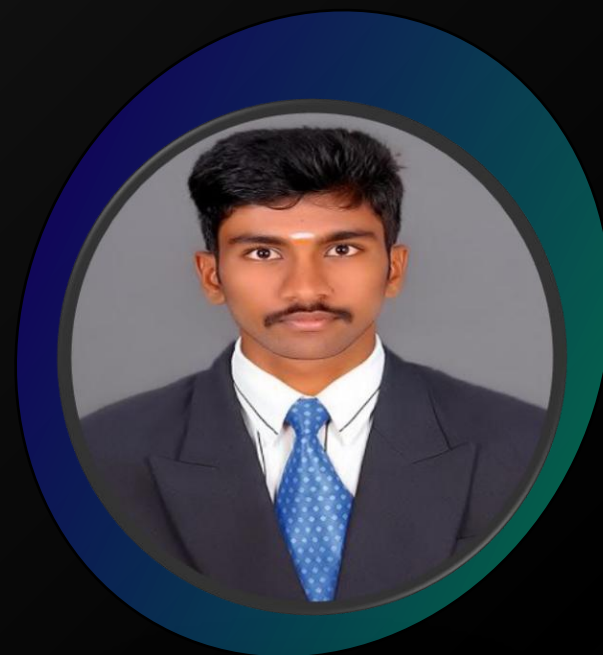
Necessary for HTTPS decryption.

Lua (Optional)

Enables custom scripting within Wireshark.

+ New analysis

Public reports
History
Threat Intelligence *new*

Windows 11 64 bit
Windows 11 64 bit
Windows 11 64 bit
Windows 7 64 bit
Windows 7 32 bit
Windows 7 64 bit

Profile
Pricing
Contacts
FAQ
Log Out

Start your analysis
Interact with the OS directly from the browser window, and immediately see the feedback from your actions.

Analyze URL
Investigate phishing activity

Analyze Files / Emails
Investigate malicious activity and collect IOCs

Wireshark · Endpoints · longtrace.pcapng

Endpoint Settings

☐ Name resolution
☑ Limit to display filter

	Ethernet · 16	IPv4 · 48	IPv6 · 17	TCP · 205	UDP · 408			
Address	Packets	Bytes	Total Packets	Percent filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:05:cd:9a:b9:8e	363 bytes	182,747 KiB	363	100.00%	356 bytes	182,058 KiB	7 bytes	706 Bytes
00:11:32:60:78:9f	916 bytes	120,658 KiB	916	100.00%	611 bytes	71,444 KiB	305 bytes	49,214 KiB
01:00:5e:00:00:fb	1,885 KiB	357,859 KiB	1,930	100.00%	0 bytes	0 bytes	1,885 KiB	357,859 KiB
01:00:5e:7f:ff:fa	514 bytes	207,238 KiB	514	100.00%	0 bytes	0 bytes	514 bytes	207,238 KiB
14:10:9f:cf:da:cf	134 bytes	21,075 KiB	134	100.00%	105 bytes	15,662 KiB	29 bytes	5,413 KiB
33:33:00:00:00:01	15 bytes	1,291 KiB	15	100.00%	0 bytes	0 bytes	15 bytes	1,291 KiB
33:33:00:00:00:fb	1,540 KiB	329,924 KiB	1,577	100.00%	0 bytes	0 bytes	1,540 KiB	329,924 KiB
33:33:ff:00:05:30	1 bytes	86 bytes	1	100.00%	0 bytes	0 bytes	1 bytes	86 bytes
3c:2a:f4:eb:19:ed	12 bytes	10,020 KiB	12	100.00%	12 bytes	10,020 KiB	0 bytes	0 bytes
96:44:f7:51:49:78	61 bytes	18,538 KiB	61	100.00%	48 bytes	11,839 KiB	13 bytes	6,699 KiB
b8:27:eb:71:a0:e1	176 bytes	17,129 KiB	176	100.00%	88 bytes	10,223 KiB	88 bytes	6,906 KiB
dc:a6:32:06:88:d7	337 bytes	53,035 KiB	337	100.00%	337 bytes	53,035 KiB	0 bytes	0 bytes
e2:63:da:8c:6f:7f	9,877 KiB	4,379 MiB	10,696	94.56%	6,050 KiB	1,208 MiB	3,827 KiB	3,171 MiB
e2:b7:4a:7e:3c:ad	3,008 bytes	555,714 KiB	3,080	100.00%	1,539 KiB	296,973 KiB	1,469 KiB	258,741 KiB
f0:2f:4b:00:3c:57	10,746 KiB	4,477 MiB	11,586	94.98%	5,852 KiB	3,516 MiB	4,895 KiB	984,227 KiB
ff:ff:ff:ff:ff:ff	406 bytes	32,737 KiB	406	100.00%	0 bytes	0 bytes	406 bytes	32,737 KiB

Copy

Map

Protocol
☐ Bluetooth
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☐ IPX
☑ IPv4
☑ IPv6
☐ JXTA
☐ MPTCP
☐ NCP

Help   Close

Activities   Terminal   Jul 14 14:53

vboxuser@ub3: ~

vboxuser@ub3:~$ sudo docker run docker/whalesay cowsay boo

```
< boo >
 -----
    \
     \
      \
                    ##        .
              ## ## ##       ==
           ## ## ## ##      ===
       /""""""""""""""""___/ ===
  ~~~ {~~ ~~~~ ~~~ ~~~~ ~~ ~ /  ===- ~~~
       _____ o          __/
        \    \        __/
          _____/
```

vboxuser@ub3:~$

MOST-TARGETED INDUSTRIES, 4Q 2023

- SAAS / Webmail 15%
- Financial Institution 14%
- eCommerce / Retail 6%
- Logistics / Shipping 5%
- Payment 4%
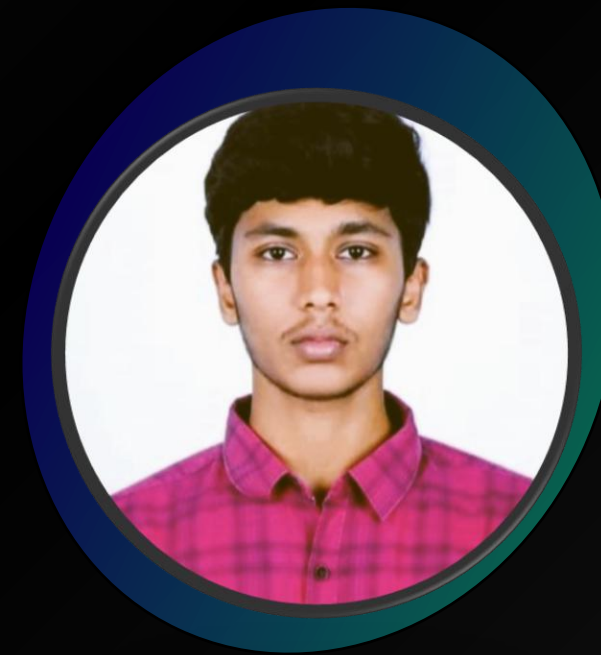- Telecom 3%
- Crypto 1%
- Other 9%
- Social Media 43%

Our Team

Praveen Kumar M
3rd -B.Tech-IT
Nandha College of
Technology,Erode

Hariharan S
3rd -B.Tech-IT
Nandha College of
Technology,Erode

Janeesh P
3rd -B.Tech - CSBS
RMK ENGINEERING
COLLEGE

Christopher A
3rd - B.E CSE
RMD ENGINEERING
COLLEGE

-    CSE