Paul Badu Yakubu

Penetration Testing

Professor Anthony J. Candeias

April 14, 2024

NCL: Individual Game (OSINT)

Open-Source INTelligence gathering involves using publicly available tools to gather information and find solutions to a given challenge. One of the challenges required using publicly available resources to find information about an IP address (104.244.73.193) found on a network that was assumed to be performing malicious activities.

By performing a whois lookup, it was revealed that the given IP address was associated with a Tor Browser, which is a web browser that enables users to browse the internet anonymously and access websites with enhanced privacy and security. It achieves this through the use of the Tor network, a decentralized network of servers known as relays. Here's an explanation of the key components of the Tor Browser:

1. **Relays** are the backbone of the Tor network. They are volunteer-operated servers that pass traffic between users and destinations on the internet. The Tor network has three types of relays: entry relays, middle relays, and exit relays. Entry relays receive traffic from Tor users, middle relays pass traffic within the Tor network, and exit relays connect to destinations on the internet.

   Relays are operated by volunteers worldwide who donate bandwidth and resources to support the Tor network's mission of providing privacy and anonymity.

2. **Exit Nodes** are a type of Tor relay that connects to destinations on the internet outside of the Tor network. When a user sends a request through the Tor network, it passes through a series of relays, including one or more exit nodes, before reaching its destination. Exit nodes are responsible for decrypting and forwarding traffic from the Tor network to its final destination on the internet. It's important to note that exit nodes can see the unencrypted traffic leaving the Tor network, so they have the potential to monitor or intercept sensitive information if the destination website is not secured with HTTPS encryption.

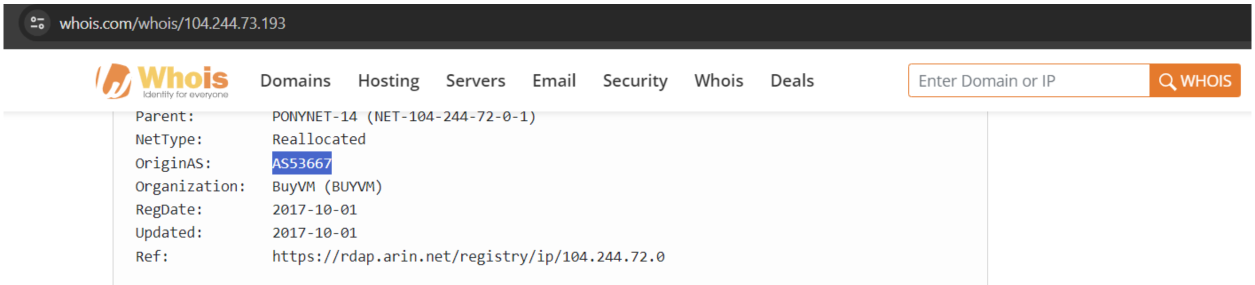
As a Security Analyst, my task was to investigate the IP address further to answer the following questions?

1. <u>What is the AS number of the relay?</u>

Performing a WHOIS lookup with the IP address provided, I found the AS number stands for Autonomous System Number under OriginAS. It uniquely identifies collections of IP networks and routers managed by network operators with shared routing policies. AS numbers are assigned by Regional Internet Registries (RIRs) and play a crucial role in the Border Gateway Protocol (BGP) for routing information exchange between different Autonomous Systems on the Internet. During a WHOIS lookup, encountering an AS number provides information about the organization or entity operating the network associated with the IP address or domain name, including details about network ownership, routing policies, and related IP address ranges.

AS numbers are integral to threat intelligence analysis. By monitoring AS numbers associated with known threat actors, malware campaigns, or malicious infrastructure, analysts can detect and respond to emerging cyber threats more effectively. It can be used in conjunction with geolocation data to map out the physical locations of networks and their associated infrastructure. This information can be valuable for geopolitical analysis, law enforcement investigations, and cybersecurity operations.

The whois results revealed that the AS number associated with the address 104.344.73.193 was ***AS53667***.



```
Parent:         PONYNET-14 (NET-104-244-72-0-1)
NetType:        Reallocated
OriginAS:       AS53667
Organization:   BuyVM (BUYVM)
RegDate:        2017-10-01
Updated:        2017-10-01
Ref:            https://rdap.arin.net/registry/ip/104.244.72.0
```

Fig 1: As highlighted above, the AS number of 104.244.73.193 on whois lookup.

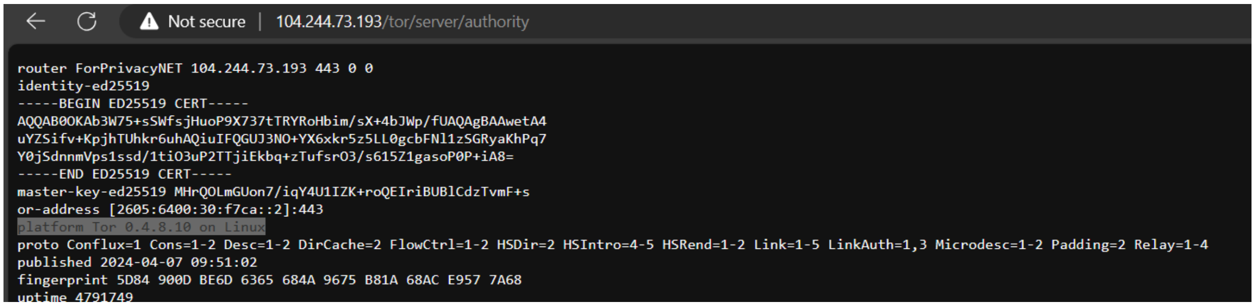
2. <u>What version of Tor is running on this IP address: 104.244.73.193?</u>

From google search, it was known that I could connect to the exit node to get information about the node on 104.244.73.193/tor/server. The information provided on this page typically pertains to the list of directory authorities in the Tor network.

In the Tor network, directory authorities are trusted entities responsible for generating and signing these consensus documents, which Tor clients use to determine the routes (circuits) through which their traffic will be routed. The information provided on the "authority" page includes details about the directory authorities themselves, such as their

IP addresses, cryptographic keys used for signing consensus documents, uptime statistics, and other relevant metadata. This information helps ensure the integrity and reliability of the Tor network by providing transparency and accountability regarding the directory authority infrastructure.

Going through the information under the authority directory of the target IP, the version of Tor browser was found to be ***Tor 0.4.8.10*** which was running on a Linux operating system.



```
router ForPrivacyNET 104.244.73.193 443 0 0
identity-ed25519
-----BEGIN ED25519 CERT-----
AQQAB0OKAb3W75+sSWfsjHuoP9X737tTRYRoHbim/sX+4bJWp/fUAQAgBAAwetA4
uYZSifv+KpjhTUhkr6uhAQiuIFQGUJ3NO+YX6xkr5z5LL0gcbFNl1zSGRyaKhPq7
Y0jSdnnmVps1ssd/1tiO3uP2TTjiEkbq+zTufsrO3/s615Z1gasoP0P+iA8=
-----END ED25519 CERT-----
master-key-ed25519 MHrQOLmGUon7/iqY4U1IZK+roQEIriBUBlCdzTvmF+s
or-address [2605:6400:30:f7ca::2]:443
platform Tor 0.4.8.10 on Linux
proto Conflux=1 Cons=1-2 Desc=1-2 DirCache=2 FlowCtrl=1-2 HSDir=2 HSIntro=4-5 HSRend=1-2 Link=1-5 LinkAuth=1,3 Microdesc=1-2 Padding=2 Relay=1-4
published 2024-04-07 09:51:02
fingerprint 5D84 900D BE6D 6365 684A 9675 B81A 68AC E957 7A68
uptime 4791749
```

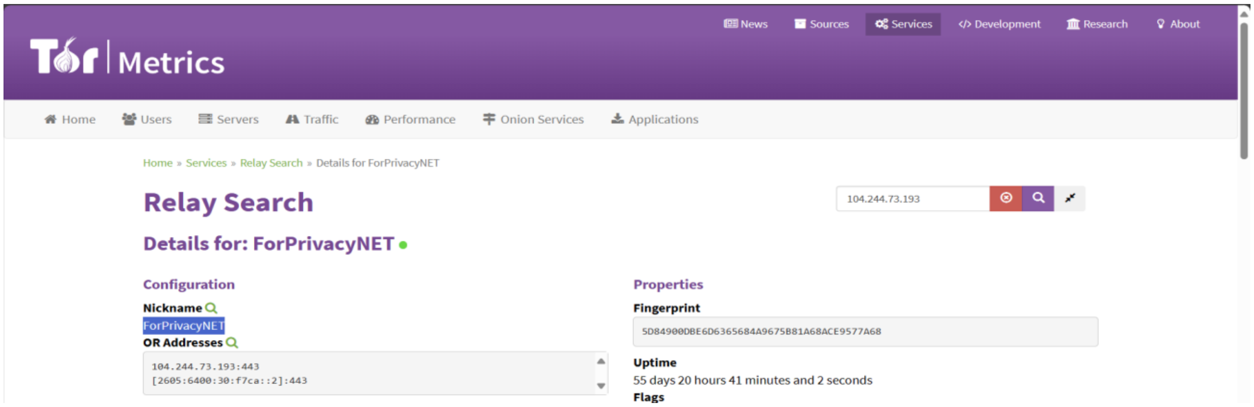
Fig 2 dipicts the platform version associated with the ip address.

3. <u>What is the nickname of the exit node?</u>

Nicknames are custom names assigned to relays by their operators for organizational or identification purposes within the Tor network. Each relay in the Tor network has a unique fingerprint, which is a cryptographic identifier derived from its public key. This fingerprint is used to identify relays and verify their authenticity within the Tor network. While nicknames are not widely used or exposed outside of the Tor network's administrative interfaces, they can help relay operators manage and distinguish their relays within the network.

Knowing the nickname of a Tor exit node is valuable for SOC analysts as it aids in tracking malicious activity, attribution, and investigation. It allows analysts to monitor node behavior, correlate activities, and respond effectively to incidents. Additionally, sharing information about malicious exit nodes enhances threat intelligence efforts and promotes collaboration in detecting and mitigating cyber threats.

By performing a tor relay search on the target IP address, I discovered that the nickname associated with exit node(104.244.73.193) was ***ForPrivacyNET*** as shown in the figure below.



Home » Services » Relay Search » Details for ForPrivacyNET

Relay Search

104.244.73.193

Details for: ForPrivacyNET ●

Configuration

Nickname

ForPrivacyNET

OR Addresses

```
104.244.73.193:443
[2605:6400:30:f7ca::2]:443
```

Properties

Fingerprint

5D84900DBE6D6365684A9675B81A68ACE9577A68

Uptime

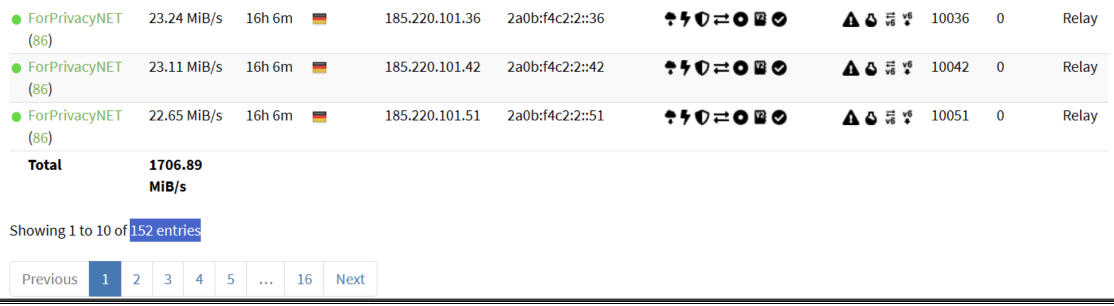
55 days 20 hours 41 minutes and 2 seconds

Flags

Fig 3: Depicts the Nickname and Fingerprint of the exit node.

4. <u>How many other relays were associated with the exit node?</u>

To answer the above question, I performed a reverse relay search with the nickname of the exit node, and it showed ***152*** entries/relays were associated with the exit node. These entries can be further investigated to determine whether there are known threats associated with the exit node.



● ForPrivacyNET (86)	23.24 MiB/s	16h 6m		185.220.101.36	2a0b:f4c2:2::36			10036	0	Relay
● ForPrivacyNET (86)	23.11 MiB/s	16h 6m		185.220.101.42	2a0b:f4c2:2::42			10042	0	Relay
● ForPrivacyNET (86)	22.65 MiB/s	16h 6m		185.220.101.51	2a0b:f4c2:2::51			10051	0	Relay
Total	**1706.89 MiB/s**									

Showing 1 to 10 of 152 entries

Fig 4 shows the number of entries/relays associated with ForPrivacyNET

References:

- [104.244.73.193/tor/server/authority]
- [check.torproject.org/torbulkexitlist]
- [What the heck is a TOR Exit Node? • Skeptical Science (skeptical-science.com)]
- [Tor Exit Nodes Mapped and Located | HackerTarget.com]