JOVITA
CYBER SECURITY

Cyber Security Incident Analysis Report

Presented for :
IDN Bootcamp Cyber

Author :
Jovita Kusuma

Date :
1 June 2025

Version:
3.0

Revisions

Version	Issue Date	Issued By	Comments
0.1	29 May 2025	Jovita Kusuma	Initial Draft
0.2	30 May 2025	Jovita Kusuma	Revised Draft
0.3	1 June 2025	Jovita Kusuma	Revised Content

Executive Summary

Field	Detail
Host Name	DESKTOP-RNV09AT
Client MAC Address	18:3d:a2:b6:8d:c4
User Name	afletcher
Date/Time Detected	2024-09-04 17:35 UTC
Internal IP Address	172.17.0.99
External IP Address	79.124.78.197
Malware	Win32/Koi Stealer

In the current state of our threat landscape, the following cyber threat has demonstrated a significant impact on our internal network security posture. This incident reflects risks originating from within our internal infrastructure and from interaction with an untrusted external entity.

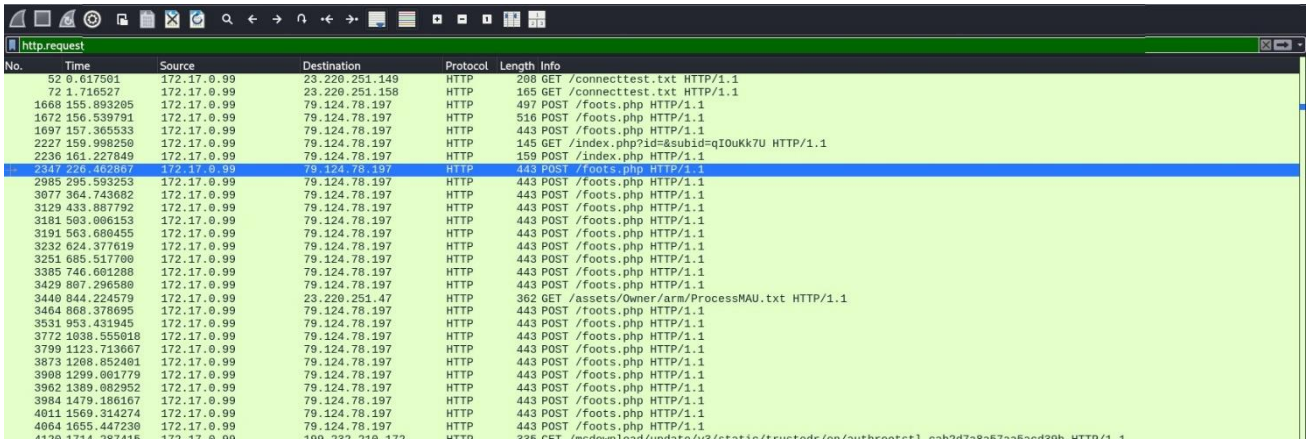
Our network monitoring tools identified persistent and anomalous communication between an internal host (IP: **172.17.0.99**) and a known malicious external server (IP: **79.124.78.197**). The external IP has been flagged as malicious by VirusTotal and associated with malware infrastructure.

Repeated HTTP POST requests to a suspicious PHP endpoint (**foots.php**) indicate a likely compromise of the internal host. This behavior is consistent with *Command-and-Control (C2)* operations or data exfiltration activities commonly used by *remote access trojans (RATs)* or information stealers.

To detect and analyze this threat, we use a combination of deep packet inspection, behavioral traffic analysis, and cyber threat intelligence tools (including VirusTotal). Our assessment underscores the need for immediate containment, forensic investigation, and proactive network hardening to prevent lateral movement or further compromise.

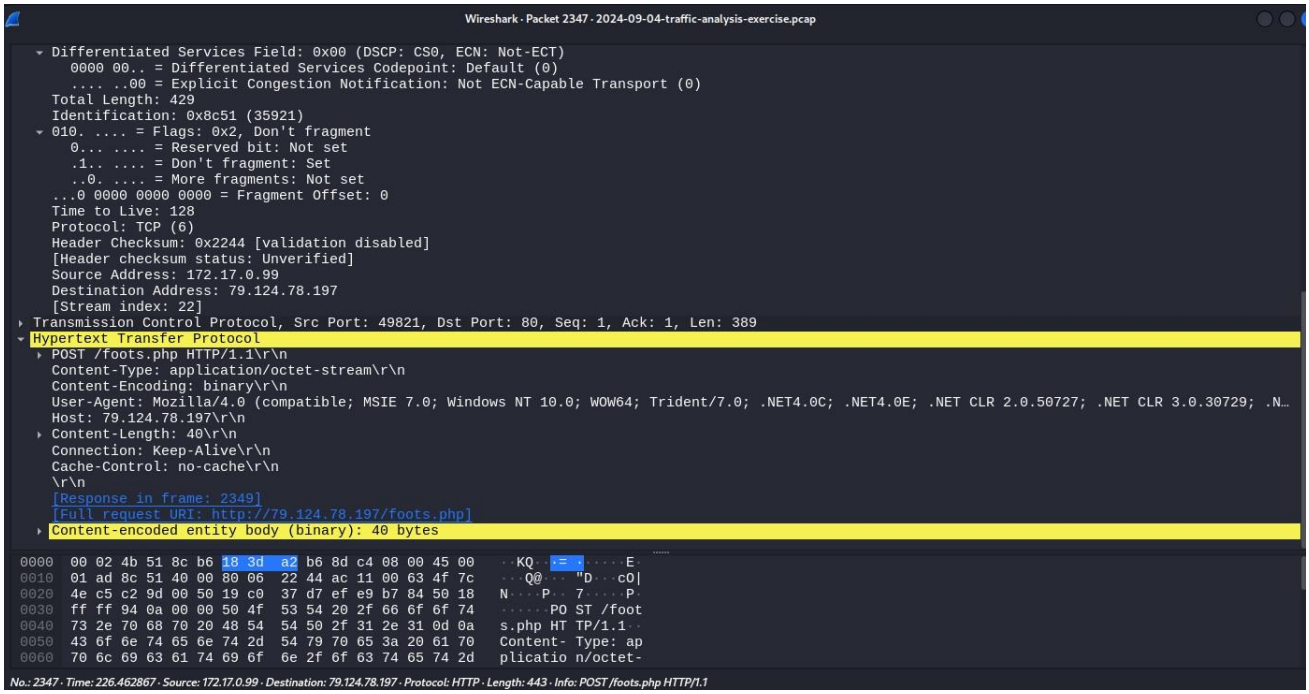
Findings

1. Suspicious HTTP POST Requests to a Malicious IP

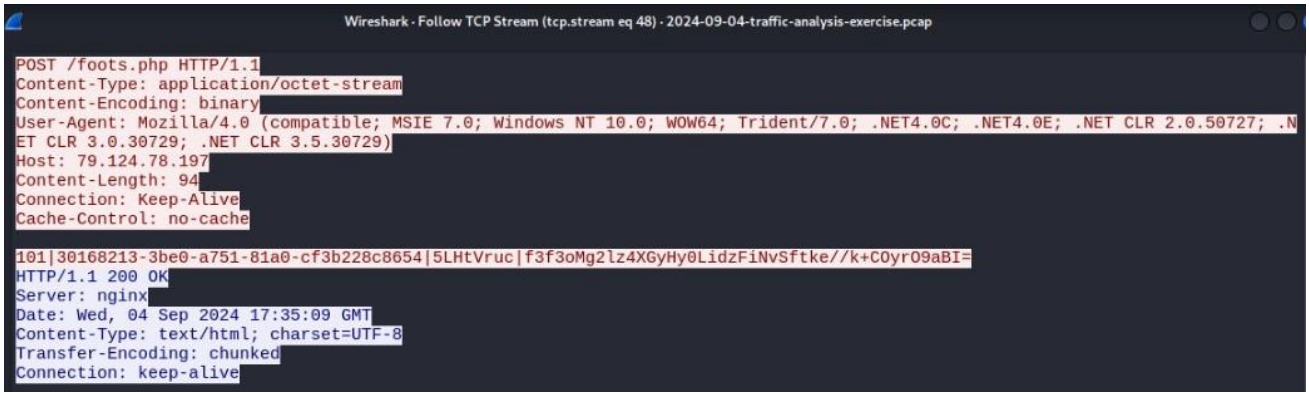


No.	Time	Source	Destination	Protocol	Length	Info
52	0.617501	172.17.0.99	23.220.251.149	HTTP	208	GET /connecttest.txt HTTP/1.1
72	1.716527	172.17.0.99	23.220.251.158	HTTP	165	GET /connecttest.txt HTTP/1.1
1668	155.893205	172.17.0.99	79.124.78.197	HTTP	497	POST /foots.php HTTP/1.1
1672	156.539791	172.17.0.99	79.124.78.197	HTTP	516	POST /foots.php HTTP/1.1
1697	157.365533	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
2227	159.998250	172.17.0.99	79.124.78.197	HTTP	145	GET /index.php?id=&subid=qIOuKk7U HTTP/1.1
2236	161.227849	172.17.0.99	79.124.78.197	HTTP	159	POST /index.php HTTP/1.1
2347	226.462867	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
2985	295.593253	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3077	364.743682	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3129	433.887792	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3181	503.006153	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3191	563.680455	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3232	624.377619	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3251	685.517700	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3385	746.601288	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3429	807.296580	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3440	844.224579	172.17.0.99	23.220.251.47	HTTP	362	GET /assets/Owner/arm/ProcessMAU.txt HTTP/1.1
3464	868.378695	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3531	953.431945	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3772	1038.555018	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3799	1123.713667	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3873	1208.852401	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3908	1299.001779	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3962	1389.082952	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3984	1479.186167	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
4011	1569.314274	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
4064	1655.447230	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1

- Numerous and continuous HTTP POST requests were identified from internal host 172.17.0.99 to external IP 79.124.78.197, specifically targeting the /foots.php endpoint.

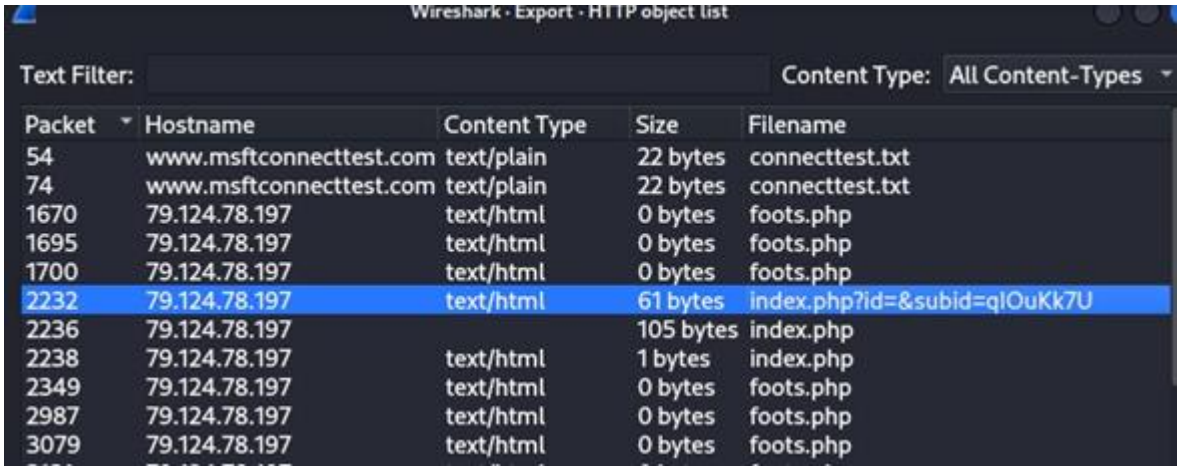


- Repeated POST requests to an unknown PHP file on an external server are a strong indicator of C2 activity or data exfiltration. The use of *application/octet-stream and Content-Encoding: binary* in the requests is especially concerning, as it implies the transmission of *arbitrary binary data*. This binary payload could include commands sent to the compromised host or sensitive data being stolen from 172.17.0.99.

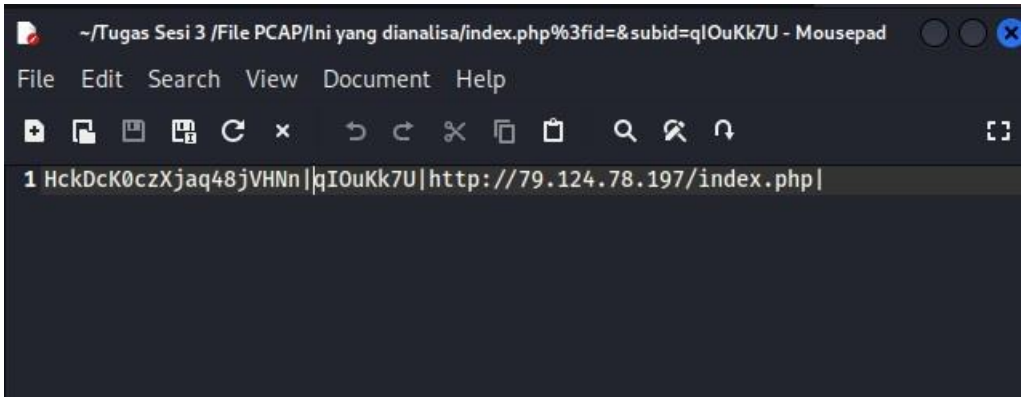


- *Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729)* is outdated and likely spoofed — a common characteristic of malware attempting to blend in with older traffic or target vulnerabilities in outdated systems.

2. Win32/Koi Stealer Indicators



- **Target URL**: http://79.124.78.197/index.php — this domain has been used by multiple malware campaigns.
- **Spoofed User-Agent string** mimicking .NET CLR and MSIE 7.0 to pose as legitimate user traffic.



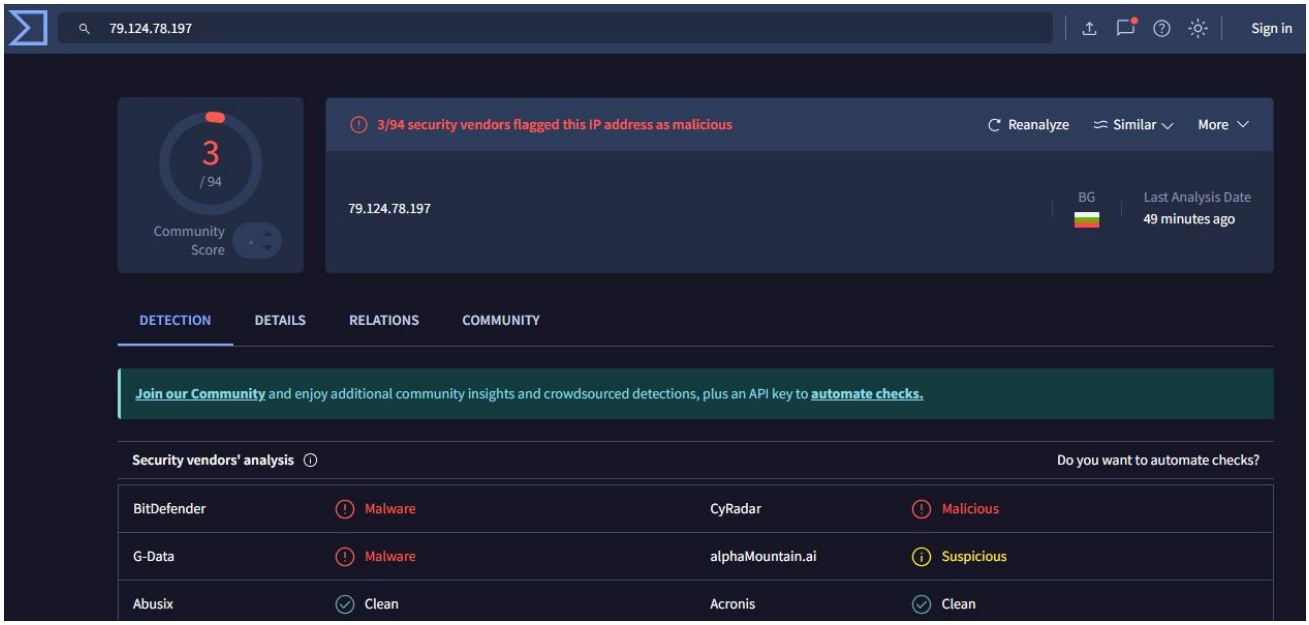
- **File token** found in index.php:

  HckDcK0czXjqa48jVHNm|qIOuKk7U|http://79.124.78.197/index.php

  This token pattern closely resembles a known C2 beacon from **Koi Stealer**.

- **Binary HTTP POST traffic** to PHP scripts is a common method of exfiltrating stolen data.

3. Analysis of Destination IP (79.124.78.197)



- VirusTotal flagged the IP 79.124.78.197 as **malicious**, 94 out of 104 security vendors confirmed this.

- Specific detections include:
  - "Malware" by **BitDefender**, **G-Data**
  - "Malicious" by **CyRadar**

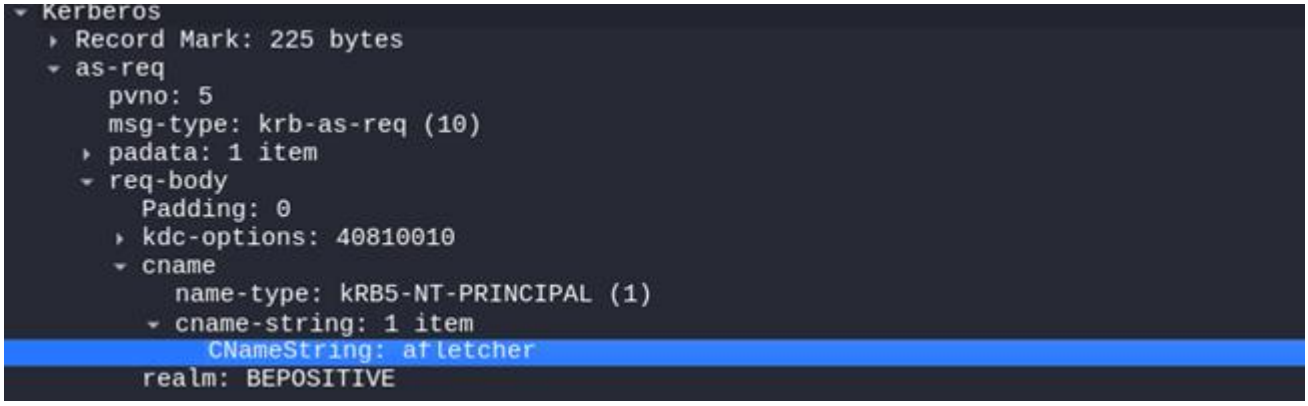
This classification indicates the IP is known to facilitate malware operations, act as a C2 server, or participate in phishing/fraud campaigns.

Based on current data, this IP is likely functioning as:

- **C2 Server**: Communicating commands and receiving data from infected systems such as 172.17.0.99.
- **Malware Distribution Point**: Hosting malicious payloads (not directly seen in this capture).
- **Data Exfiltration Endpoint**: The use of binary application/octet-stream POSTs strongly supports this role.

The ongoing communication between the infected host and this IP indicates an **active compromise**, not a one-time event.

4. Identity Attribution from Kerberos Activity

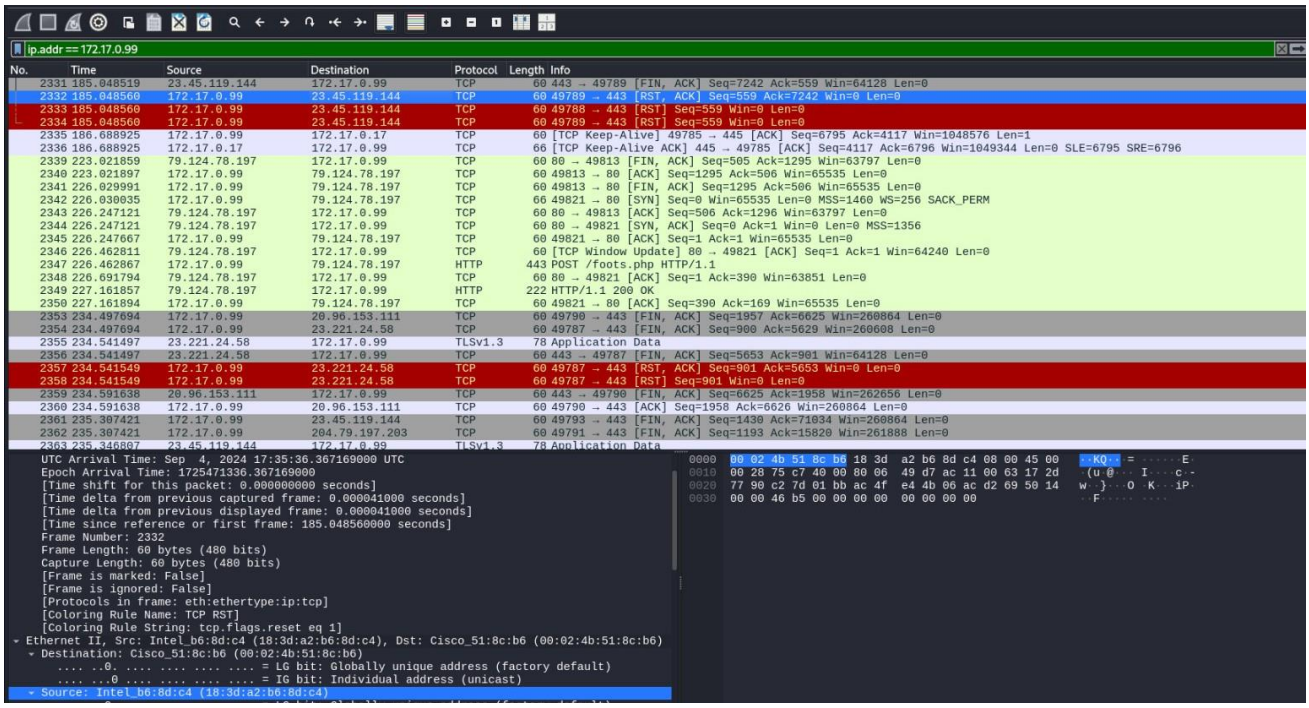


Kerberos traffic analysis revealed an AS-REQ authentication request originating from the compromised host (172.17.0.99) with the CNameString value **afletcher** and realm **BEPOSITIVE**. This provides direct user attribution and confirms that user **afletcher** initiated or was associated with the suspicious activity.

The presence of this Kerberos exchange further validates that this host is a domain-joined device, and the account afletcher@BEPOSITIVE was actively in use during the compromise timeframe.

This evidence strengthens the case for an internal compromise with authenticated user context and highlights the urgency for forensic investigation and account containment.

Technical Analysis



1. Affected Host

- **IP Address**: 172.17.0.99
- **MAC Address**: 18:3d:a2:b6:8d:c4
- **User** : afletcher

2. Indicators of Compromise (IoCs)

Type	Value
IP Address	79.124.78.197
URL/Path	/index.php
User-Agent	Mozilla/4.0 (MSIE 7.0)
Protocol	HTTP POST (TCP 80)
Payload Type	Trojan

Behavior Pattern

- The infected host initiates binary HTTP POST requests to the suspicious external server.
- Binary payloads are often used for C2 communications or data exfiltration.
- The paths /foots.php and /index.php match known backdoor or Trojan behavior.

Risk Assesment

Category	Assesment	Description
Infection Likelihood	Confirmed	POST requests sent from internal host
Potential Impact	High	C2 activity may lead to data theft or takeover
Spread Potential	Medium	Depends on afletcher's privileges and lateral movement opportunities
Stealth Level	Medium	Uses HTTP (unencrypted) but small, hidden payloads

External Host Check

- **IP**: 79.124.78.197
- **Geolocation**: Bulgaria (based on IP intelligence services)
- **Reputation**: Labeled as **malicious** by multiple threat intel feeds (VirusTotal, AbuseIPDB)

Mitigation and Recommendations

For Infected Host (172.17.0.99)

- Immediately isolate from the network to prevent lateral movement.
- Conduct a full malware scan using tools such as Windows Defender, Malwarebytes, or forensic toolkits.
- If infection cannot be safely removed, consider a clean reinstallation (re-image).

Network Security

- Block all traffic to/from IP 79.124.78.197.
- Search internal logs for other machines that communicated with the malicious IP.
- Implement *egress filtering* to block unauthorized outbound HTTP connections.
- Deploy intrusion detection/prevention rules (Snort, Suricata, etc.) for C2 behavior patterns.

Forensic Colection

- Export the full HTTP stream and binary payloads for offline analysis.
- Save the .pcap file and compute its SHA-256 hash for documentation purposes.