



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	23.226.251.149	HTTP	208	GET /connecttest.txt HTTP/1.1
72	1.716527	172.17.0.99	23.226.251.158	HTTP	165	GET /connecttest.txt HTTP/1.1
1668	155.893285	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	224.402367	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	563.066153	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
3191	563.698455	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	23.226.251.47	HTTP	362	GET /assets/Owner/arm/ProcessMAU.txt HTTP/1.1
3464	860.378695	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	1208.852481	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.

```

Wireshark - Packet 2347 - 2024-09-04-traffic-analysis-exercise.pcap
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 429
  Identification: 0x8c51 (35921)
- 010. .... = Flags: 0x2, Don't fragment
  0... .... = Reserved bit: Not set
  .1... .... = Don't fragment: Set
  ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x2244 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.17.0.99
  Destination Address: 79.124.78.197
  [Stream index: 22]
- Transmission Control Protocol, Src Port: 49821, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
- Hypertext Transfer Protocol
  POST /foots.php HTTP/1.1\r\n
  Content-Type: application/octet-stream\r\n
  Content-Encoding: binary\r\n
  User-Agent: 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; .N...
  Host: 79.124.78.197\r\n
  Content-Length: 40\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  \r\n
  [Response in frame: 2349]
  [Full request URI: http://79.124.78.197/foots.php]
  Content-encoded entity body (binary): 40 bytes

0000 00 02 4b 51 8c b6 18 3d a2 b6 8d c4 08 00 45 00  ..KQ..=.....E
0010 01 ad 8c 51 40 00 80 06 22 44 ac 11 00 63 4f 7c  ..Q@... "D...c0|
0020 4e c5 c2 9d 00 50 19 c0 37 d7 ef e9 b7 84 50 18  N...P... 7 ....P
0030 ff ff 94 0a 00 00 50 4f 53 54 20 2f 66 6f 6f 74  .... PO ST /foot
0040 73 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a  s.php HT TP/1.1..
0050 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70  Content- Type: ap
0060 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74 65 74 2d  plicatio n/octet-
  
```

- 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.

```

Wireshark · Follow TCP Stream (tcp.stream eq 48) · 2024-09-04-traffic-analysis-exercise.pcap

POST /foots.php HTTP/1.1
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: 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; .NET CLR 3.5.30729)
Host: 79.124.78.197
Content-Length: 94
Connection: Keep-Alive
Cache-Control: no-cache

101|30168213-3be0-a751-81a0-cf3b228c8654|5LHtVruc|f3f3oMg2lz4XGyHy0LidzFiNvSftke//k+C0yr09aBI=
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 04 Sep 2024 17:35:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

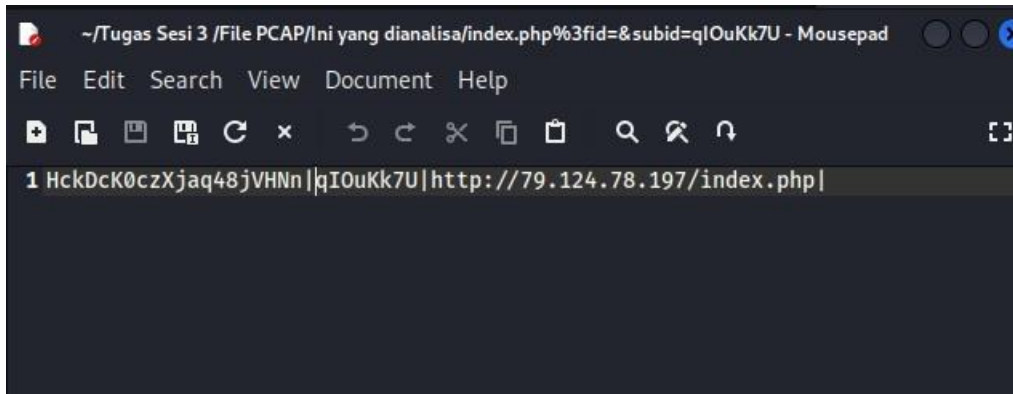
```

- *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

Packet	Hostname	Content Type	Size	Filename
54	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
74	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
1670	79.124.78.197	text/html	0 bytes	foots.php
1695	79.124.78.197	text/html	0 bytes	foots.php
1700	79.124.78.197	text/html	0 bytes	foots.php
2232	79.124.78.197	text/html	61 bytes	index.php?id=&subid=qlOuKk7U
2236	79.124.78.197		105 bytes	index.php
2238	79.124.78.197	text/html	1 bytes	index.php
2349	79.124.78.197	text/html	0 bytes	foots.php
2987	79.124.78.197	text/html	0 bytes	foots.php
3079	79.124.78.197	text/html	0 bytes	foots.php

- **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:

HckDcK0czXjqa48jVHNn|qlOuKk7U|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)

 A screenshot of the VirusTotal web interface showing the analysis of IP address 79.124.78.197. The interface includes a community score of 3/94, a warning that 3/94 security vendors flagged the IP as malicious, and a table of security vendor analyses.

Security vendors' analysis		Do you want to automate checks?	
BitDefender	Malware	CyRadar	Malicious
G-Data	Malware	alphaMountain.ai	Suspicious
Abusix	Clean	Acronis	Clean

- 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
  ▶ Record Mark: 225 bytes
  ▼ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▶ padata: 1 item
    ▼ req-body
      Padding: 0
      ▶ kdc-options: 40810010
      ▼ cname
        name-type: KRB5-NT-PRINCIPAL (1)
        ▼ cname-string: 1 item
          CNameString: afletcher
        realm: BEPOSITIVE
```

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

ip.addr == 172.17.0.99

No.	Time	Source	Destination	Protocol	Length	Info
2331	185.048519	23.45.119.144	172.17.0.99	TCP	60	443 → 49789 [FIN, ACK] Seq=7242 Ack=559 Win=64128 Len=0
2332	185.048560	172.17.0.99	23.45.119.144	TCP	60	49789 → 443 [RST, ACK] Seq=559 Ack=7242 Win=0 Len=0
2333	185.048560	172.17.0.99	23.45.119.144	TCP	60	49789 → 443 [RST] Seq=559 Win=0 Len=0
2334	185.048560	172.17.0.99	23.45.119.144	TCP	60	49789 → 443 [RST] Seq=559 Win=0 Len=0
2335	186.688925	172.17.0.99	172.17.0.17	TCP	60	[TCP Keep-Alive] 49785 → 445 [ACK] Seq=6795 Ack=4117 Win=1048576 Len=1
2336	186.688925	172.17.0.17	172.17.0.99	TCP	60	[TCP Keep-Alive ACK] 445 → 49785 [ACK] Seq=4117 Ack=6796 Win=1049344 Len=0 SLE=6795 SRE=6796
2339	223.021809	79.124.78.197	172.17.0.99	TCP	60	80 → 49813 [FIN, ACK] Seq=505 Ack=1295 Win=63797 Len=0
2340	223.021897	172.17.0.99	79.124.78.197	TCP	60	49813 → 80 [ACK] Seq=1295 Ack=506 Win=65535 Len=0
2341	226.029991	172.17.0.99	79.124.78.197	TCP	60	49813 → 80 [FIN, ACK] Seq=1295 Ack=506 Win=65535 Len=0
2342	226.030035	172.17.0.99	79.124.78.197	TCP	60	49821 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2343	226.247121	79.124.78.197	172.17.0.99	TCP	60	80 → 49813 [ACK] Seq=506 Ack=1296 Win=63797 Len=0
2344	226.247121	79.124.78.197	172.17.0.99	TCP	60	80 → 49821 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1356
2345	226.247667	172.17.0.99	79.124.78.197	TCP	60	49821 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
2346	226.462811	79.124.78.197	172.17.0.99	TCP	60	[TCP Window Update] 80 → 49821 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2347	226.462867	172.17.0.99	79.124.78.197	HTTP	443	POST /foots.php HTTP/1.1
2348	226.691794	79.124.78.197	172.17.0.99	TCP	60	80 → 49821 [ACK] Seq=1 Ack=390 Win=63851 Len=0
2349	227.161867	79.124.78.197	172.17.0.99	HTTP	222	HTTP/1.1 200 OK
2350	227.161894	172.17.0.99	79.124.78.197	TCP	60	49821 → 80 [ACK] Seq=390 Ack=169 Win=65535 Len=0
2353	234.497694	172.17.0.99	20.96.153.111	TCP	60	49790 → 443 [FIN, ACK] Seq=1957 Ack=6625 Win=260864 Len=0
2354	234.497694	172.17.0.99	23.221.24.58	TCP	60	49787 → 443 [FIN, ACK] Seq=900 Ack=5620 Win=260608 Len=0
2355	234.541497	23.221.24.58	172.17.0.99	TLSv1.3	78	Application Data
2356	234.541497	23.221.24.58	172.17.0.99	TCP	60	443 → 49787 [FIN, ACK] Seq=5653 Ack=901 Win=64128 Len=0
2357	234.541549	172.17.0.99	23.221.24.58	TCP	60	49787 → 443 [RST, ACK] Seq=901 Ack=5653 Win=0 Len=0
2358	234.541549	172.17.0.99	23.221.24.58	TCP	60	49787 → 443 [RST] Seq=901 Win=0 Len=0
2359	234.591638	20.96.153.111	172.17.0.99	TCP	60	443 → 49790 [FIN, ACK] Seq=6625 Ack=1958 Win=262656 Len=0
2360	234.591638	172.17.0.99	20.96.153.111	TCP	60	49790 → 443 [ACK] Seq=1958 Ack=6626 Win=260864 Len=0
2361	235.307421	172.17.0.99	23.45.119.144	TCP	60	49793 → 443 [FIN, ACK] Seq=1430 Ack=71034 Win=260864 Len=0
2362	235.307421	172.17.0.99	204.79.197.203	TCP	60	49791 → 443 [FIN, ACK] Seq=1193 Ack=15820 Win=261888 Len=0
2363	235.346807	23.45.119.144	172.17.0.99	TLSv1.3	78	Application Data

UTC Arrival Time: Sep 4, 2024 17:35:36.367169000 UTC
 Epoch Arrival Time: 1725471336.367169000
 [Time shift for this packet: 0.000000000 seconds]
 [Time delta from previous captured frame: 0.000041000 seconds]
 [Time delta from previous displayed frame: 0.000041000 seconds]
 [Time since reference or first frame: 185.048560000 seconds]
 Frame Number: 2332
 Frame Length: 60 bytes (480 bits)
 Capture Length: 60 bytes (480 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp]
 [Coloring Rule Name: TCP RST]
 [Coloring Rule String: tcp.flags.reset eq 1]
 - Ethernet II, Src: Intel_b6:8d:c4 (18:3d:a2:b6:8d:c4), Dst: Cisco_51:8c:b6 (00:02:4b:51:8c:b6)
 - Destination: Cisco_51:8c:b6 (00:02:4b:51:8c:b6)
 = LG bit: Globally unique address (factory default)
 = IG bit: Individual address (unicast)
 - Source: Intel_b6:8d:c4 (18:3d:a2:b6:8d:c4)

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 Assessment

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.