REVA UNIVERSITY
Bengaluru, India
REVA Academy for Corporate Excellence (RACE)

Name: Srinath R

SRN: R24MSC18

Date: 22/09/2025

Module Name: Incident Response Management

1) **Executive Summary:**
    - To contain the name of malware

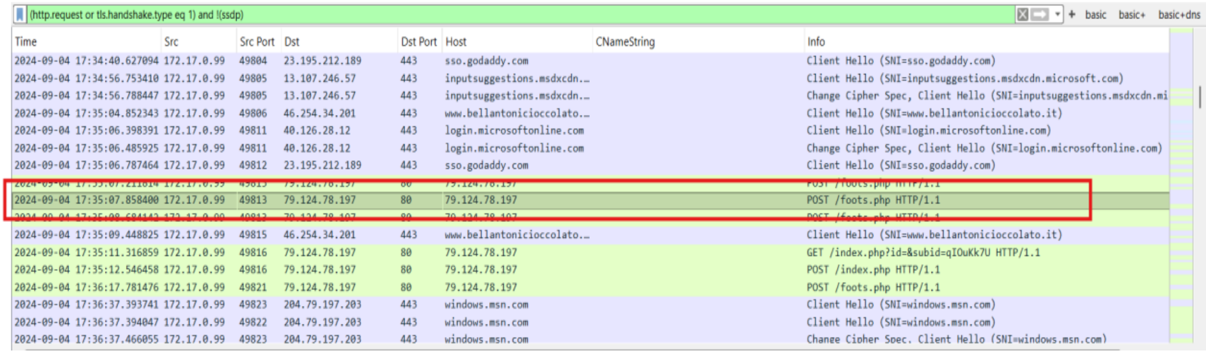
2) **Victim Details:**
    - Host name:
    - IP address:
    - MAC address:
    - Windows user account name:
    - Name of victim:

3) **Indicators of Compromise (IOCs):**
    - IP addresses, domains and URLs associated with the activity.

Determining Malware

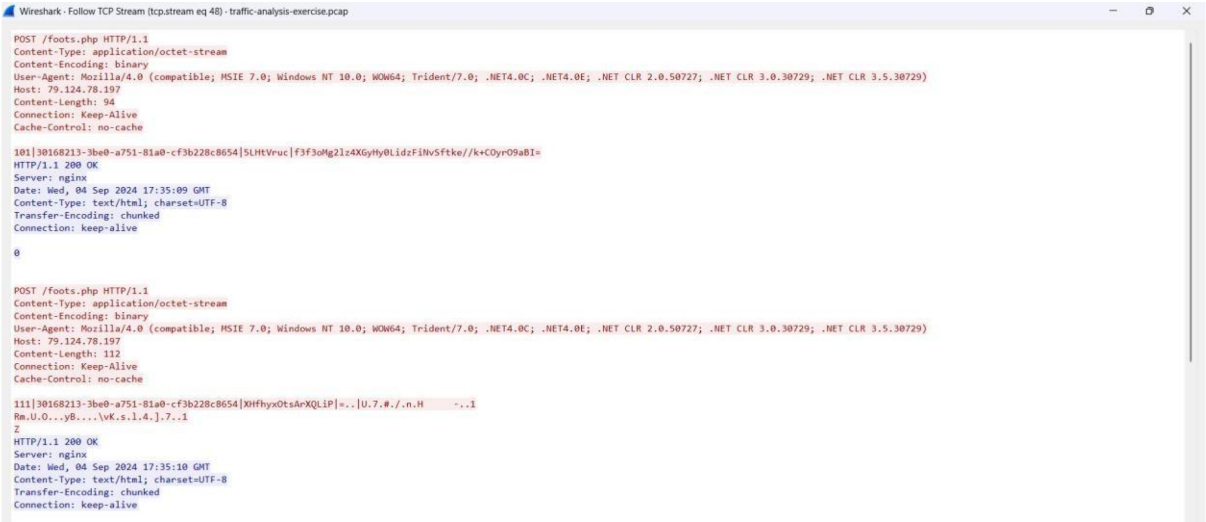
Applied the filter "(http.request or tls.handshake.type eq 1) and !(ssdp)" and the snippet is as shown below.

The highlighted log, foot.php file is suspected malware for command and control



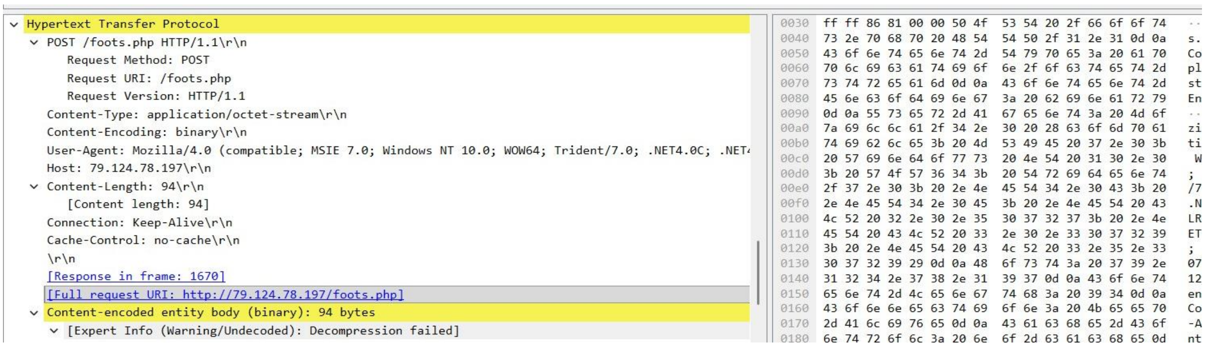
(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Src	Src Port	Dst	Dst Port	Host	CNameString	Info
2024-09-04 17:34:40.627094	172.17.0.99	49804	23.195.212.189	443	sso.godaddy.com		Client Hello (SNI=sso.godaddy.com)
2024-09-04 17:34:56.753410	172.17.0.99	49805	13.107.246.57	443	inputsuggestions.msdxcdn.…		Client Hello (SNI=inputsuggestions.msdxcdn.microsoft.com)
2024-09-04 17:34:56.788447	172.17.0.99	49805	13.107.246.57	443	inputsuggestions.msdxcdn.…		Change Cipher Spec, Client Hello (SNI=inputsuggestions.msdxcdn.mi
2024-09-04 17:35:04.852343	172.17.0.99	49806	46.254.34.201	443	www.bellantonicioccolato.…		Client Hello (SNI=www.bellantonicioccolato.it)
2024-09-04 17:35:06.398391	172.17.0.99	49811	40.126.28.12	443	login.microsoftonline.com		Client Hello (SNI=login.microsoftonline.com)
2024-09-04 17:35:06.485925	172.17.0.99	49811	40.126.28.12	443	login.microsoftonline.com		Change Cipher Spec, Client Hello (SNI=login.microsoftonline.com)
2024-09-04 17:35:06.787464	172.17.0.99	49812	23.195.212.189	443	sso.godaddy.com		Client Hello (SNI=sso.godaddy.com)
2024-09-04 17:35:07.211814	172.17.0.99	49813	79.124.78.197	80	79.124.78.197		POST /foots.php HTTP/1.1
2024-09-04 17:35:07.858400	172.17.0.99	49813	79.124.78.197	80	79.124.78.197		POST /foots.php HTTP/1.1
2024-09-04 17:35:08.684142	172.17.0.99	49813	79.124.78.197	80	79.124.78.197		POST /foots.php HTTP/1.1
2024-09-04 17:35:09.448825	172.17.0.99	49815	46.254.34.201	443	www.bellantonicioccolato.…		Client Hello (SNI=www.bellantonicioccolato.it)
2024-09-04 17:35:11.316859	172.17.0.99	49816	79.124.78.197	80	79.124.78.197		GET /index.php?id=&subid=qIOuKk7U HTTP/1.1
2024-09-04 17:35:12.546458	172.17.0.99	49816	79.124.78.197	80	79.124.78.197		POST /index.php HTTP/1.1
2024-09-04 17:36:17.781476	172.17.0.99	49821	79.124.78.197	80	79.124.78.197		POST /foots.php HTTP/1.1
2024-09-04 17:36:37.393741	172.17.0.99	49823	204.79.197.203	443	windows.msn.com		Client Hello (SNI=windows.msn.com)
2024-09-04 17:36:37.394047	172.17.0.99	49822	204.79.197.203	443	windows.msn.com		Client Hello (SNI=windows.msn.com)
2024-09-04 17:36:37.466055	172.17.0.99	49823	204.79.197.203	443	windows.msn.com		Change Cipher Spec, Client Hello (SNI=windows.msn.com)



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

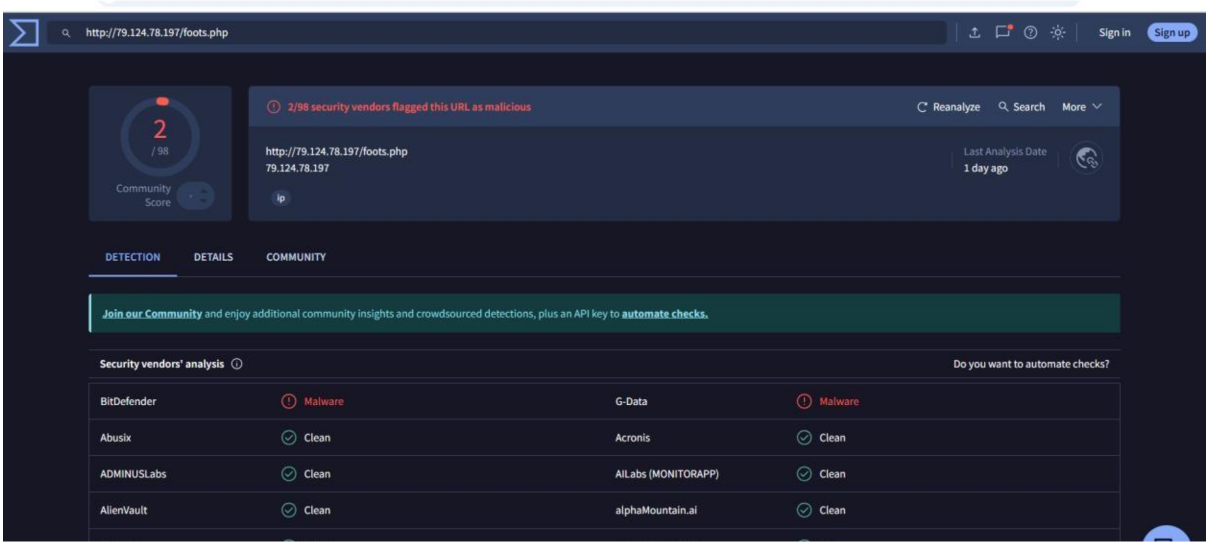
```
POST /foots.php HTTP/1.1
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 79.124.78.197
Content-Length: 94
Connection: Keep-Alive
Cache-Control: no-cache

101|30168213-3be0-a751-81a0-cf3b228c8654|5LHtVruc|f3f3oMg2lz4XGyHy0LidzFiNvSftke//k+COyrO9aBI=
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

0


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: 112
Connection: Keep-Alive
Cache-Control: no-cache

111|30168213-3be0-a751-81a0-cf3b228c8654|XHfhyxOtsArXQLiP|=..|U.7.#./.n.H     -..1
Rm.U.O...yB....\vK.s.l.4.].7..1
Z
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 04 Sep 2024 17:35:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
```



```
v Hypertext Transfer Protocol
  v POST /foots.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /foots.php
      Request Version: HTTP/1.1
    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
    Host: 79.124.78.197\r\n
  v Content-Length: 94\r\n
      [Content length: 94]
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Response in frame: 1670]
    [Full request URI: http://79.124.78.197/foots.php]
  v Content-encoded entity body (binary): 94 bytes
    v [Expert Info (Warning/Undecoded): Decompression failed]
```

```
0030  ff ff 86 81 00 00 50 4f  53 54 20 2f 66 6f 6f 74   ··
0040  73 2e 70 68 70 20 48 54  54 50 2f 31 2e 31 0d 0a   s.
0050  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 61 70   Co
0060  70 6c 69 63 61 74 69 6f  6e 2f 6f 63 74 65 74 2d   pl
0070  73 74 72 65 61 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   st
0080  45 6e 63 6f 64 69 6e 67  3a 20 62 69 6e 61 72 79   En
0090  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··
00a0  7a 69 6c 6c 61 2f 34 2e  30 20 28 63 6f 6d 70 61   zi
00b0  74 69 62 6c 65 3b 20 4d  53 49 45 20 37 2e 30 3b   ti
00c0  20 57 69 6e 64 6f 77 73  20 4e 54 20 31 30 2e 30    W
00d0  3b 20 57 4f 57 36 34 3b  20 54 72 69 64 65 6e 74   ;
00e0  2f 37 2e 30 3b 20 2e 4e  45 54 34 2e 30 43 3b 20   /7
00f0  2e 4e 45 54 34 2e 30 45  3b 20 2e 4e 45 54 20 43   .N
0100  4c 52 20 32 2e 30 2e 35  30 37 32 37 3b 20 2e 4e   LR
0110  45 54 20 43 4c 52 20 33  2e 30 2e 33 30 37 32 39   ET
0120  3b 20 2e 4e 45 54 20 43  4c 52 20 33 2e 35 2e 33   ;
0130  30 37 32 39 29 0d 0a 48  6f 73 74 3a 20 37 39 2e   07
0140  31 32 34 2e 37 38 2e 31  39 37 0d 0a 43 6f 6e 74   12
0150  65 6e 74 2d 4c 65 6e 67  74 68 3a 20 39 34 0d 0a   en
0160  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Co
0170  2d 41 6c 69 76 65 0d 0a  43 61 63 68 65 2d 43 6f   -A
0180  6e 74 72 6f 6c 3a 20 6e  6f 2d 63 61 63 68 65 0d   nt
```

The URL http://79.124.78.197/foots.php is tracked as Malware in the virus total.



http://79.124.78.197/foots.php

2/98 security vendors flagged this URL as malicious

http://79.124.78.197/foots.php
79.124.78.197

Last Analysis Date
1 day ago

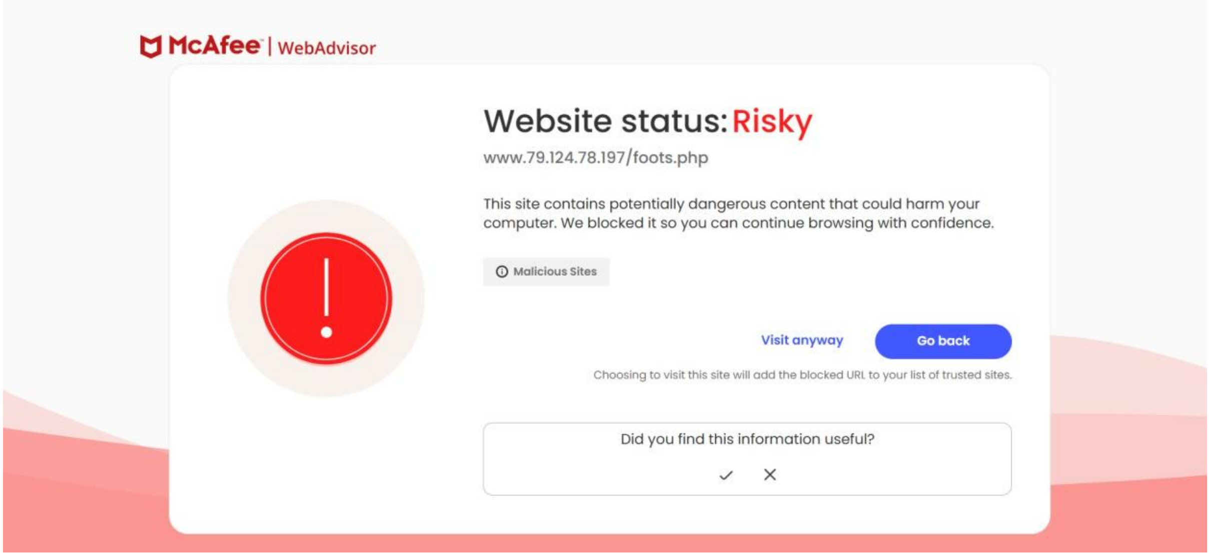
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

BitDefender	Malware	G-Data	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

Also, upon searching the URL on browser the McAfee detects it as the risky URL.



Website status: Risky

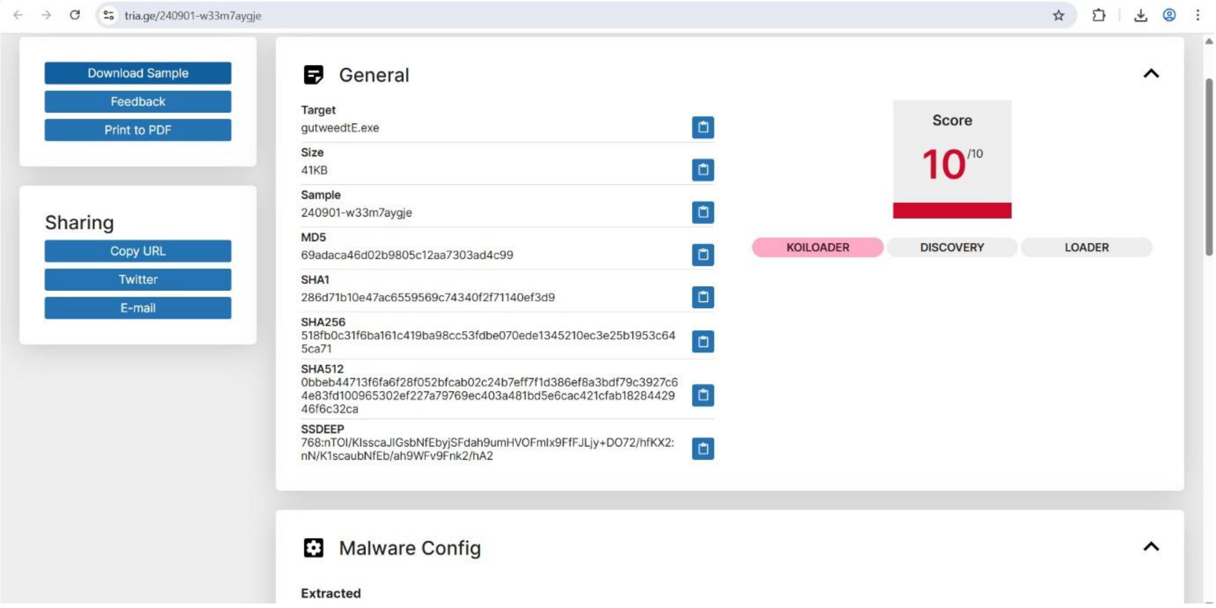
www.79.124.78.197/foots.php

This site contains potentially dangerous content that could harm your computer. We blocked it so you can continue browsing with confidence.

Choosing to visit this site will add the blocked URL to your list of trusted sites.

Did you find this information useful?

Upon further investigating on the foot.php, it is identified that it belongs to Koiloader Family and gutweedtE.exe seems to be the malware.



General

Target
gutweedtE.exe

Size
41KB

Sample
240901-w33m7aygje

MD5
69adaca46d02b9805c12aa7303ad4c99

SHA1
286d71b10e47ac6559569c74340f2f71140ef3d9

SHA256
518fb0c31f6ba161c419ba98cc53fdbe070ede1345210ec3e25b1953c645ca71

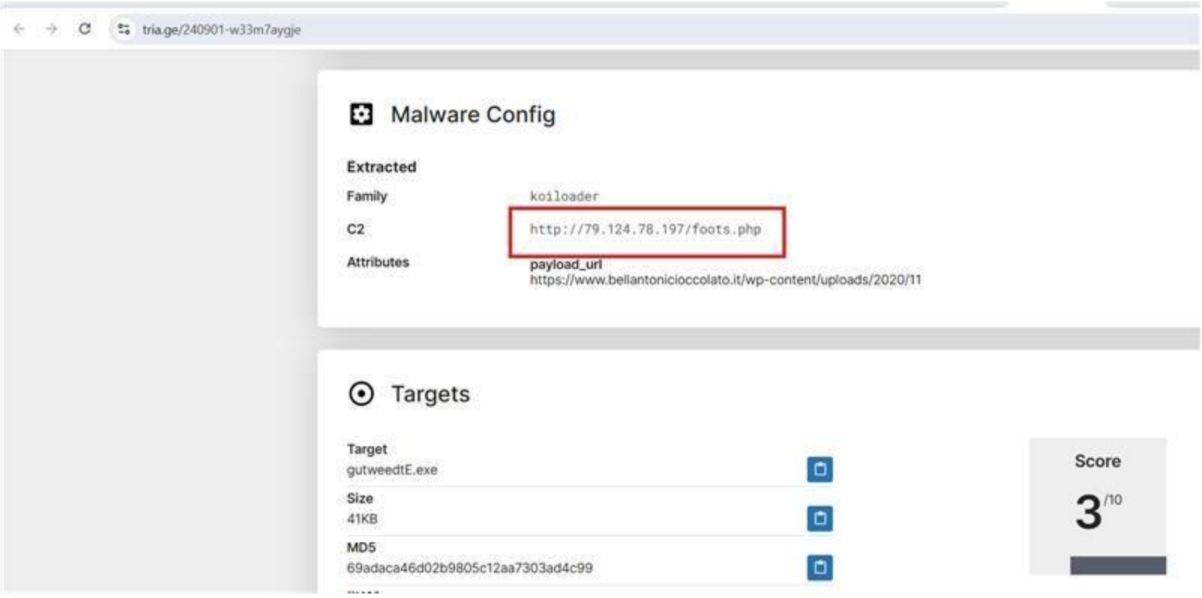
SHA512
0bbeb44713f6fa6f28f052bfcab02c24b7eff7f1d386ef8a3bdf79c3927c64e83fd100965302ef227a79769ec403a481bd5e6cac421cfab1828442946f6c32ca

SSDEEP
768:nTOI/KIsscaJIGsbNfEbyjSFdah9umHVOFmIx9FfFJLjy+DO72/hfKX2:nN/K1scaubNfEb/ah9WFv9Fnk2/hA2

Score
10/10

Malware Config

Extracted



Malware Config

Extracted

Family koiloader

C2 http://79.124.78.197/foots.php

Attributes payload_url
https://www.bellantonicioccolato.it/wp-content/uploads/2020/11

Targets

Target
gutweedtE.exe

Size
41KB

MD5
69adaca46d02b9805c12aa7303ad4c99

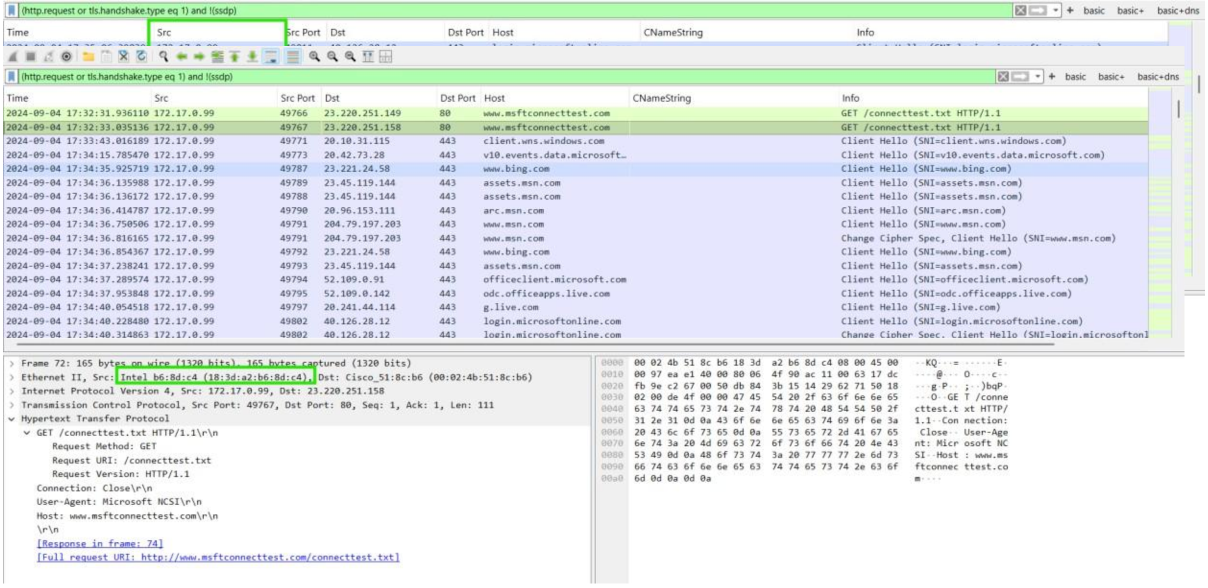
Score
3/10

Victim Details

Identified the victim IP address and the MAC address from the source tab on the filter “(http.request or tls.handshake.type eq 1) and !(ssdp)“

Victim **ip address**:172.17.0.99

MAC address: Ethernet II, Src: Intel_b6:8d:c4 (**18:3d:a2:b6:8d:c4)**



(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Src	Src Port	Dst	Dst Port	Host	CNameString	Info
2024-09-04 17:32:31.936110	172.17.0.99	49766	23.220.251.149	80	www.msftconnecttest.com		GET /connecttest.txt HTTP/1.1
2024-09-04 17:32:33.035136	172.17.0.99	49767	23.220.251.158	80	www.msftconnecttest.com		GET /connecttest.txt HTTP/1.1
2024-09-04 17:33:43.016189	172.17.0.99	49771	20.10.31.115	443	client.wns.windows.com		Client Hello (SNI=client.wns.windows.com)
2024-09-04 17:34:15.785470	172.17.0.99	49773	20.42.73.28	443	v10.events.data.microsoft…		Client Hello (SNI=v10.events.data.microsoft.com)
2024-09-04 17:34:35.925719	172.17.0.99	49787	23.221.24.58	443	www.bing.com		Client Hello (SNI=www.bing.com)
2024-09-04 17:34:36.135988	172.17.0.99	49789	23.45.119.144	443	assets.msn.com		Client Hello (SNI=assets.msn.com)
2024-09-04 17:34:36.136172	172.17.0.99	49788	23.45.119.144	443	assets.msn.com		Client Hello (SNI=assets.msn.com)
2024-09-04 17:34:36.414787	172.17.0.99	49790	20.96.153.111	443	arc.msn.com		Client Hello (SNI=arc.msn.com)
2024-09-04 17:34:36.750506	172.17.0.99	49791	204.79.197.203	443	www.msn.com		Client Hello (SNI=www.msn.com)
2024-09-04 17:34:36.816165	172.17.0.99	49791	204.79.197.203	443	www.msn.com		Change Cipher Spec, Client Hello (SNI=www.msn.com)
2024-09-04 17:34:36.854367	172.17.0.99	49792	23.221.24.58	443	www.bing.com		Client Hello (SNI=www.bing.com)
2024-09-04 17:34:37.238241	172.17.0.99	49793	23.45.119.144	443	assets.msn.com		Client Hello (SNI=assets.msn.com)
2024-09-04 17:34:37.289574	172.17.0.99	49794	52.109.0.91	443	officeclient.microsoft.com		Client Hello (SNI=officeclient.microsoft.com)
2024-09-04 17:34:37.953848	172.17.0.99	49795	52.109.0.142	443	odc.officeapps.live.com		Client Hello (SNI=odc.officeapps.live.com)
2024-09-04 17:34:40.054518	172.17.0.99	49797	20.241.44.114	443	g.live.com		Client Hello (SNI=g.live.com)
2024-09-04 17:34:40.228480	172.17.0.99	49802	40.126.28.12	443	login.microsoftonline.com		Client Hello (SNI=login.microsoftonline.com)
2024-09-04 17:34:40.314863	172.17.0.99	49802	40.126.28.12	443	login.microsoftonline.com		Change Cipher Spec, Client Hello (SNI=login.microsoftonl

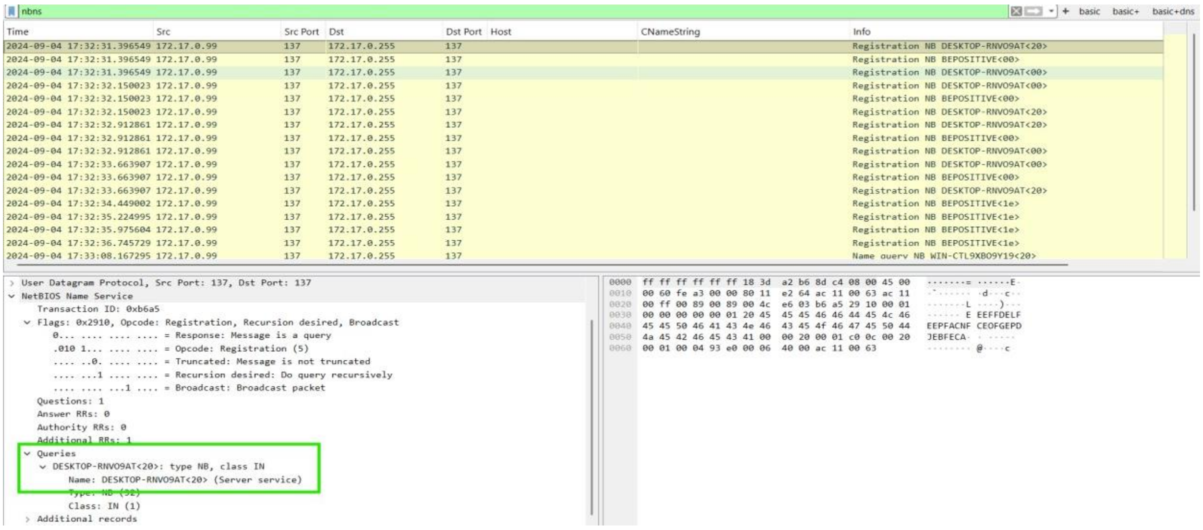
```
> Frame 72: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
> Ethernet II, Src: Intel_b6:8d:c4 (18:3d:a2:b6:8d:c4), Dst: Cisco_51:8c:b6 (00:02:4b:51:8c:b6)
> Internet Protocol Version 4, Src: 172.17.0.99, Dst: 23.220.251.158
> Transmission Control Protocol, Src Port: 49767, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
v Hypertext Transfer Protocol
  v GET /connecttest.txt HTTP/1.1\r\n
      Request Method: GET
      Request URI: /connecttest.txt
      Request Version: HTTP/1.1
    Connection: Close\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: www.msftconnecttest.com\r\n
    \r\n
    [Response in frame: 74]
    [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
```

```
0000  00 02 4b 51 8c b6 18 3d  a2 b6 8d c4 08 00 45 00   ··KQ···= ······E·
0010  00 97 ea e1 40 00 80 06  4f 90 ac 11 00 63 17 dc   ····@··· O····c··
0020  fb 9e c2 67 00 50 db 84  3b 15 14 29 62 71 50 18   ···g·P·· ;··)bqP·
0030  02 00 de 4f 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ···O··GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   1.1··Con nection:
0060  20 43 6c 6f 73 65 0d 0a  55 73 65 72 2d 41 67 65    Close·· User-Age
0070  6e 74 3a 20 4d 69 63 72  6f 73 6f 66 74 20 4e 43   nt: Micr osoft NC
0080  53 49 0d 0a 48 6f 73 74  3a 20 77 77 77 2e 6d 73   SI··Host : www.ms
0090  66 74 63 6f 6e 6e 65 63  74 74 65 73 74 2e 63 6f   ftconnec ttest.co
00a0  6d 0d 0a 0d 0a                                     m····
```

Used the filter “nbns” and determined the hostname as below.

Hostname:

DESKTOP-RNVO9AT<20>



nbns

Time	Src	Src Port	Dst	Dst Port	Host	CNameString	Info
2024-09-04 17:32:31.396549	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<20>
2024-09-04 17:32:31.396549	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<00>
2024-09-04 17:32:31.396549	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<00>
2024-09-04 17:32:32.150023	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<00>
2024-09-04 17:32:32.150023	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<00>
2024-09-04 17:32:32.150023	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<20>
2024-09-04 17:32:32.912861	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<20>
2024-09-04 17:32:32.912861	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<00>
2024-09-04 17:32:32.912861	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<00>
2024-09-04 17:32:33.663907	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<00>
2024-09-04 17:32:33.663907	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<00>
2024-09-04 17:32:33.663907	172.17.0.99	137	172.17.0.255	137			Registration NB DESKTOP-RNVO9AT<20>
2024-09-04 17:32:34.449002	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<1e>
2024-09-04 17:32:35.224995	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<1e>
2024-09-04 17:32:35.975604	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<1e>
2024-09-04 17:32:36.745729	172.17.0.99	137	172.17.0.255	137			Registration NB BEPOSITIVE<1e>
2024-09-04 17:33:08.167295	172.17.0.99	137	172.17.0.255	137			Name query NB WIN-CTL9XBO9Y19<20>

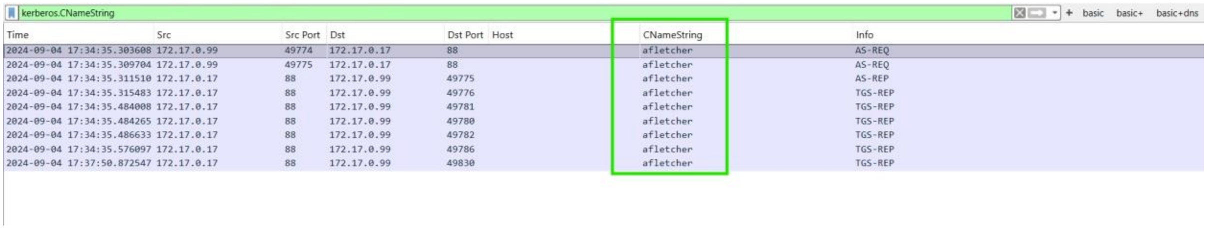
```
> User Datagram Protocol, Src Port: 137, Dst Port: 137
v NetBIOS Name Service
    Transaction ID: 0xb6a5
  v Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
      0... .... .... .... = Response: Message is a query
      .010 1... .... .... = Opcode: Registration (5)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... ...1 .... = Broadcast: Broadcast packet
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  v Queries
    v DESKTOP-RNVO9AT<20>: type NB, class IN
        Name: DESKTOP-RNVO9AT<20> (Server service)
        Type: NB (32)
        Class: IN (1)
  > Additional records
```

```
0000  ff ff ff ff ff ff 18 3d  a2 b6 8d c4 08 00 45 00   ·······= ······E·
0010  00 60 fe a3 00 00 80 11  e2 64 ac 11 00 63 ac 11   ·`······ ·d···c··
0020  00 ff 00 89 00 89 00 4c  e6 03 b6 a5 29 10 00 01   ·······L ····)···
0030  00 00 00 00 00 01 20 45  45 45 46 46 44 45 4c 46   ······ E EEFFDELF
0040  45 45 50 46 41 43 4e 46  43 45 4f 46 47 45 50 44   EEPFACNF CEOFGEPD
0050  4a 45 42 46 45 43 41 00  00 20 00 01 c0 0c 00 20   JEBFECA· · ······
0060  00 01 00 04 93 e0 00 06  40 00 ac 11 00 63         ········ @····c
```

Windows user account name:

Using the Kerberos.CNameString filter, identified the username.(afletcher)

Name of the Victim:



kerberos.CNameString

Time	Src	Src Port	Dst	Dst Port	Host	CNameString	Info
2024-09-04 17:34:35.303608	172.17.0.99	49774	172.17.0.17	88		afletcher	AS-REQ
2024-09-04 17:34:35.309704	172.17.0.99	49775	172.17.0.17	88		afletcher	AS-REQ
2024-09-04 17:34:35.311510	172.17.0.17	88	172.17.0.99	49775		afletcher	AS-REP
2024-09-04 17:34:35.315483	172.17.0.17	88	172.17.0.99	49776		afletcher	TGS-REP
2024-09-04 17:34:35.484008	172.17.0.17	88	172.17.0.99	49781		afletcher	TGS-REP
2024-09-04 17:34:35.484265	172.17.0.17	88	172.17.0.99	49780		afletcher	TGS-REP
2024-09-04 17:34:35.486633	172.17.0.17	88	172.17.0.99	49782		afletcher	TGS-REP
2024-09-04 17:34:35.576097	172.17.0.17	88	172.17.0.99	49786		afletcher	TGS-REP
2024-09-04 17:37:50.872547	172.17.0.17	88	172.17.0.99	49830		afletcher	TGS-REP

Name of the victim was identified using the filter “ldap contains "CN=Users"”(Andrew Fletcher)

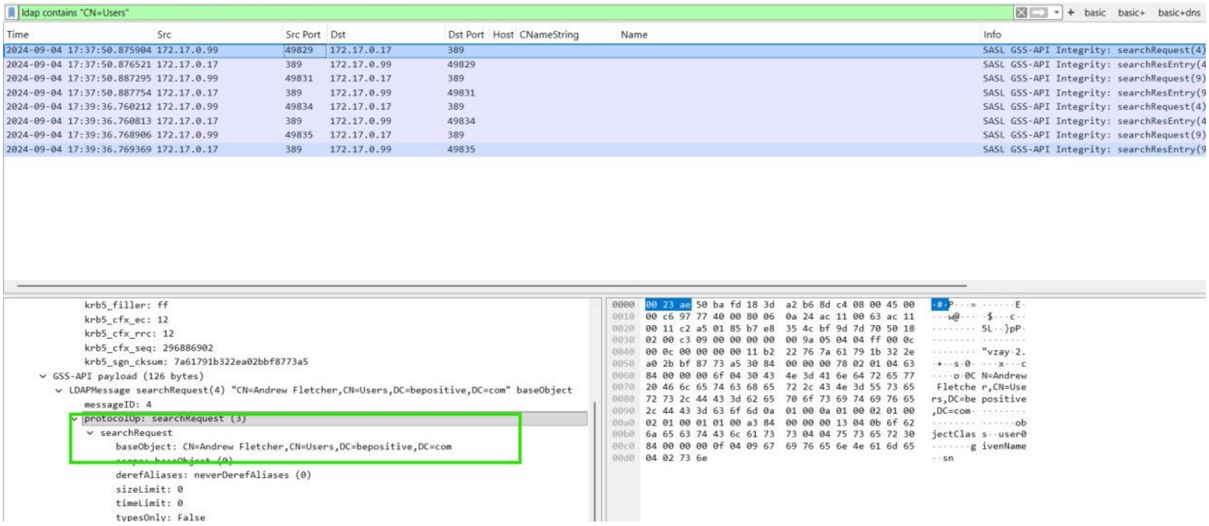
REVA UNIVERSITY
Bengaluru, India
REVA Academy for Corporate Excellence (RACE)

Name: Srinath R

SRN: R24MSC18

Date: 22/09/2025

Module Name: Incident Response Management



ldap contains "CN=Users"

```
Time                       Src          Src Port Dst          Dst Port Host CNameString Name  Info
2024-09-04 17:37:50.875904 172.17.0.99  49829    172.17.0.17  389                             SASL GSS-API Integrity: searchRequest(4)
2024-09-04 17:37:50.876521 172.17.0.17  389      172.17.0.99  49829                           SASL GSS-API Integrity: searchResEntry(4
2024-09-04 17:37:50.887295 172.17.0.99  49831    172.17.0.17  389                             SASL GSS-API Integrity: searchRequest(9)
2024-09-04 17:37:50.887754 172.17.0.17  389      172.17.0.99  49831                           SASL GSS-API Integrity: searchResEntry(9
2024-09-04 17:39:36.760212 172.17.0.99  49834    172.17.0.17  389                             SASL GSS-API Integrity: searchRequest(4)
2024-09-04 17:39:36.760813 172.17.0.17  389      172.17.0.99  49834                           SASL GSS-API Integrity: searchResEntry(4
2024-09-04 17:39:36.768906 172.17.0.99  49835    172.17.0.17  389                             SASL GSS-API Integrity: searchRequest(9)
2024-09-04 17:39:36.769369 172.17.0.17  389      172.17.0.99  49835                           SASL GSS-API Integrity: searchResEntry(9
```

```
          krb5_filler: ff
          krb5_cfx_ec: 12
          krb5_cfx_rrc: 12
          krb5_cfx_seq: 296886902
          krb5_sgn_cksum: 7a61791b322ea02bbf8773a5
    ˅ GSS-API payload (126 bytes)
      ˅ LDAPMessage searchRequest(4) "CN=Andrew Fletcher,CN=Users,DC=bepositive,DC=com" baseObject
          messageID: 4
        ˅ protocolOp: searchRequest (3)
          ˅ searchRequest
              baseObject: CN=Andrew Fletcher,CN=Users,DC=bepositive,DC=com
              scope: baseObject (0)
              derefAliases: neverDerefAliases (0)
              sizeLimit: 0
              timeLimit: 0
              typesOnly: False
```

```
0000  00 23 ae 50 ba fd 18 3d  a2 b6 8d c4 08 00 45 00   ·#·P···=  ······E·
0010  00 c6 97 77 40 00 80 06  0a 24 ac 11 00 63 ac 11   ···w@···  ·$···c··
0020  00 11 c2 a5 01 85 b7 e8  35 4c bf 9d 7d 70 50 18   ········  5L··}pP·
0030  02 00 c3 09 00 00 00 00  00 9a 05 04 04 ff 00 0c   ········  ········
0040  00 0c 00 00 00 00 11 b2  22 76 7a 61 79 1b 32 2e   ········  "vzay·2.
0050  a0 2b bf 87 73 a5 30 84  00 00 00 78 02 01 04 63   ·+··s·0·  ···x···c
0060  84 00 00 00 6f 04 30 43  4e 3d 41 6e 64 72 65 77   ····o·0C  N=Andrew
0070  20 46 6c 65 74 63 68 65  72 2c 43 4e 3d 55 73 65    Fletche  r,CN=Use
0080  72 73 2c 44 43 3d 62 65  70 6f 73 69 74 69 76 65   rs,DC=be  positive
0090  2c 44 43 3d 63 6f 6d 0a  01 00 0a 01 00 02 01 00   ,DC=com·  ········
00a0  02 01 00 01 01 00 a3 84  00 00 00 13 04 0b 6f 62   ········  ······ob
00b0  6a 65 63 74 43 6c 61 73  73 04 04 75 73 65 72 30   jectClas  s··user0
00c0  84 00 00 00 0f 04 09 67  69 76 65 6e 4e 61 6d 65   ·······g  ivenName
00d0  04 02 73 6e                                        ··sn
```

Indicators of compromise

There is multiple network traffic that was captured from the source to the malicious IP 79.124.78.197.

The URL **http://79.124.78.197/foots.php** is malicious and belong to Koiloader family.

The POST uuids found from the TCP stream also are the

IOCs 101|30168213-3be0-a751-81a0-cf3b228c8654|5LHtVruc|f3f3oMg2lz4XGyHy0LidzFiNvSftke//k+COyrO9aBI=

111|30168213-3be0-a751-81a0-cf3b228c8654|XHfhyxOtsArXQLiP|=..|U.7.#./.n.H -..1

102|30168213-3be0-a751-81a0-cf3b228c8654