

Athanasius Joseph Kojo Gadosey

Week 3

Practical Task: The Suspicious Downloaded PCAP Analysis

The following answers are the analysis of the incident reports:

1. The IP address of the infected Windows Client is **10.1.17.215**

Filter: (*ip.src == 10.1.17.0/24 && ip.dst != 10.1.17.0/24*) This command was used to analyse the host IP address communicating to any external networks, which helped us to spot the suspicious outbound connections.

2025-01-22-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 10.1.17.0/24 && ip.dst != 10.1.17.0/24

No.	Time	Source	Destination	Protocol	Length	Info
39355	3164.129029	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39357	3164.911783	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39360	3165.530786	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24346 Ack=1198542 Win=523264 Len=0
39368	3169.368989	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39370	3170.494838	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39373	3171.131741	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24395 Ack=1198817 Win=523008 Len=0
39375	3174.480627	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39377	3176.097646	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39380	3176.374717	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24444 Ack=1199092 Win=524032 Len=0
39384	3179.655781	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39386	3181.340731	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39389	3184.568944	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24493 Ack=1199367 Win=523776 Len=0
39395	3184.828551	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39397	3186.535218	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39400	3186.763186	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24542 Ack=1199642 Win=523520 Len=0
39402	3189.998919	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39404	3191.727993	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39406	3191.956177	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24591 Ack=1199917 Win=523264 Len=0
39411	3195.179051	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39413	3196.921867	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39418	3197.181811	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24640 Ack=1200192 Win=523008 Len=0
39422	3200.359362	10.1.17.215	45.125.66.252	TLSv1.2	81	Application Data
39424	3202.128240	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39427	3202.388113	10.1.17.215	5.252.153.241	TCP	60	49689 → 80 [ACK] Seq=24689 Ack=1200467 Win=524032 Len=0

Hardware address length: 6
Hops: 0
Transaction ID: 0xd1207c03
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
0... .. = Broadcast flag: Unicast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 10.1.17.215
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_26:4a:74 (00:d0:b7:26:4a:74)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (51) IP Address Lease Time
Option: (54) DHCP Server Identifier (10.1.17.2)
Option: (1) Subnet Mask (255.255.255.0)
Option: (81) Client Fully Qualified Domain Name
Option: (3) Router
Option: (6) Domain Name Server
Option: (15) Domain Name
Option: (30) End

0000 ff ff ff ff ff ff 00 24 e8 7f 09 5d 08 00 45 00\$...]:E
0010 01 59 33 ec 00 00 00 11 ea a5 0a 01 11 02 ff ff ..Y3.....
0020 ff ff 00 43 00 44 01 45 6a 5a 02 01 06 00 51 28 ...C O E m.....(
0030 7c 03 00 00 00 00 00 00 00 0a 01 11 47 00 00&Jt....
0040 00 00 00 00 00 00 00 00 b7 26 4a 74 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 63 82 53 63 35 01 05 3a 04 00
0120 05 46 00 3b 04 00 09 3a 80 33 04 00 0a 8c 00 36 ..F;...:3...
0130 04 0a 01 11 02 01 04 ff ff 00 51 03 00 ff ffQ...
0140 03 04 0a 01 11 01 06 08 0a 01 11 02 08 00 00
0150 0f 14 62 6c 75 65 6d 6f 6f 6e 74 75 65 73 64 61 ..bluemo ontuesda
0160 79 2e 63 6f 6d 00 ffy.com..

2. The MAC address of the infected Windows Client is **00:d0:b7:26:4a:74**
Filter: (`arp && arp.src.proto_ipv4 == 10.1.17.215`) This command was to help identify the MAC address of the IP address.

The screenshot shows a Wireshark packet capture of an ARP request. The filter is `arp && arp.src.proto_ipv4 == 10.1.17.215`. The packet list shows a single packet at time 169.7093907. The packet details pane shows the Ethernet II frame with source Intel_26:4a:74 and destination Broadcast. The ARP section shows the request for 10.1.17.215 from Intel_26:4a:74. The packet bytes pane shows the raw data of the ARP request.

Also, this filter command (`eth.addr == 00:d0:b7:26:4a:74`) was used to confirm the MAC address of the infected Windows client gotten earlier

The screenshot shows a Wireshark packet capture of an ARP reply. The filter is `eth.addr == 00:d0:b7:26:4a:74`. The packet list shows a single packet at time 7.014846. The packet details pane shows the Ethernet II frame with source Dell_7f:09:5d and destination Intel_26:4a:74. The ARP section shows the reply for 10.1.17.215 from Dell_7f:09:5d. The packet bytes pane shows the raw data of the ARP reply.

3. The hostname of the infected Windows client is www.msftconnecttest.com OR **DESKTOP-L8C5GSJ**

The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a GET request to /connecttest.txt from 10.1.17.215 to 239.255.255.250. The packet details pane on the right shows the request structure, including the Host header: `Host: www.msftconnecttest.com\r\n`, which is highlighted with a red box. The packet bytes pane on the right shows the raw data of the request.

The filter command used is [*bootp.option.hostname*](#)

The screenshot shows a Wireshark packet capture of a DHCP Discover packet. The packet list on the left shows a DHCP Discover packet from 0.0.0.0 to 255.255.255.255. The packet details pane on the right shows the packet structure, including the Host Name option: `Host Name: DESKTOP-L8C5GSJ`, which is highlighted with a red box.

The screenshot shows a Wireshark packet capture of a DHCP Request packet. The packet list on the left shows a DHCP Request packet from 0.0.0.0 to 255.255.255.255. The packet details pane on the right shows the packet structure, including the Host Name option: `Host Name: DESKTOP-L8C5GSJ`, which is highlighted with a red box.

4. The user account name from the infected Windows Client is

BLUEMOONTUESDAY/shutchenson

Filter: (**kerberos.CNameString**) This command is used because most user accounts can be found or appear in them, and is also known for its reliability.

2025-01-22-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

kerberos.CNameString

No.	Time	Source	Destination	Protocol	Length	Info
250	14.368083	10.1.17.215	10.1.17.2	KRB5	288	AS-REQ
258	14.374722	10.1.17.215	10.1.17.2	KRB5	368	AS-REQ
260	14.376723	10.1.17.2	10.1.17.215	KRB5	399	AS-REP
272	14.380720	10.1.17.2	10.1.17.215	KRB5	329	TGS-REP
296	14.529454	10.1.17.2	10.1.17.215	KRB5	461	TGS-REP
14710	316.418853	10.1.17.2	10.1.17.215	KRB5	435	TGS-REP
15464	522.604316	10.1.17.2	10.1.17.215	KRB5	435	TGS-REP
15476	522.606534	10.1.17.2	10.1.17.215	KRB5	285	TGS-REP
15709	606.272125	10.1.17.215	10.1.17.2	KRB5	301	AS-REQ
15717	606.281407	10.1.17.215	10.1.17.2	KRB5	381	AS-REQ
15719	606.283454	10.1.17.2	10.1.17.215	KRB5	445	AS-REP
15731	606.289671	10.1.17.2	10.1.17.215	KRB5	479	TGS-REP
16075	614.114385	10.1.17.215	10.1.17.2	KRB5	301	AS-REQ
16087	614.123815	10.1.17.215	10.1.17.2	KRB5	381	AS-REQ
16089	614.125892	10.1.17.2	10.1.17.215	KRB5	445	AS-REP

padata: 1 item

req-body

Padding: 0

kdc-options: 40810010

cname

name-type: kRB5-NT-PRINCIPAL (1)

CNameString: 1 item

CNameString: shutchenson

realm: BLUEMOONTUESDAY

sname

till: Sep 13, 2100 02:48:05.000000000 Coordinated Universal Time

rtime: Sep 13, 2100 02:48:05.000000000 Coordinated Universal Time

nonce: 859884582

etype: 4 items

addresses: 1 item DESKTOP-L8C5G5J<20>

[Response in: 251]

5. The likely domain name for the fake Google Authenticator page is

authenticatoor.org

Filter: (**dns.qry.name contains auth**) This command was used to query dns of the infected Windows client.

2025-01-22-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains auth

No.	Time	Source	Destination	Protocol	Length	Info
2364	38.863141	10.1.17.215	10.1.17.2	DNS	78	Standard query 0xbcc7 A authenticatoor.org
2321	38.196580	10.1.17.215	10.1.17.2	DNS	103	Standard query 0xcc42 A google-authenticator.burleson-appliance.net
2322	38.196686	10.1.17.215	10.1.17.2	DNS	103	Standard query 0xe4c2 HTTPS google-authenticator.burleson-appliance.net
2365	38.863149	10.1.17.215	10.1.17.2	DNS	78	Standard query 0xe6f7 HTTPS authenticatoor.org
2376	39.387854	10.1.17.2	10.1.17.215	DNS	94	Standard query response 0xbcc7 A authenticatoor.org A 82.221.136.26
2329	38.256143	10.1.17.2	10.1.17.215	DNS	215	Standard query response 0xcc42 A google-authenticator.burleson-appliance.net A 104.21.64.1 A 104.21.48.1 A 104.21.48.1
2330	38.269839	10.1.17.2	10.1.17.215	DNS	351	Standard query response 0xe4c2 HTTPS google-authenticator.burleson-appliance.net HTTPS
2375	39.097981	10.1.17.2	10.1.17.215	DNS	147	Standard query response 0xe6f7 HTTPS authenticatoor.org SOA siti.ns.orangewebsite.com

UDP payload (36 bytes)

Domain Name System (query)

Transaction ID: 0xbcc7

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

authenticatoor.org: type A, class IN

Name: authenticatoor.org

[Name Length: 18]

[Label Count: 2]

Type: A (1) (Host Address)

Class: IN (0x0001)

[Response To: 2376]

6. The IP addresses used for C2 servers for this infection are **5.252.153.241**, **45.125.66.252** and **45.125.66.32**

Filter for **outbound traffic to external IP ranges** after the infection.

Wireshark - Conversations - 2025-01-22-traffic-analysis-exercise.pcap

Conversation Settings

☐ Name resolution

☐ Absolute start time

☒ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ BPV7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ LTP

Filter list for specific type

Ethernet · 4

IPv4 · 138

IPv6

TCP · 268

UDP · 33

Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A
10.1.17.215	20.189.173.8	53	29 kB	94	92	57.61%	53	29 kB	0	0 bytes	747.977598	1.5132	153 k
10.1.17.215	23.205.110.137	53	13 kB	13	97	54.64%	53	13 kB	0	0 bytes	17.087558	506.1210	208 b
10.1.17.215	23.45.119.143	54	5 kB	15	109	49.54%	54	5 kB	0	0 bytes	17.507462	109.1090	354 b
10.1.17.215	23.212.73.35	57	5 kB	79	143	39.86%	57	5 kB	0	0 bytes	607.498809	2353.7510	18 b
10.1.17.215	23.205.110.145	63	10 kB	92	167	37.72%	63	10 kB	0	0 bytes	727.638101	1704.5055	44 b
10.1.17.215	52.175.242.182	64	10 kB	71	115	55.65%	64	10 kB	0	0 bytes	512.146242	2499.6673	32 b
10.1.17.215	204.79.197.239	68	16 kB	19	143	47.55%	68	16 kB	0	0 bytes	26.421907	2568.9896	51 b
10.1.17.215	23.205.110.134	69	8 kB	29	172	40.12%	69	8 kB	0	0 bytes	31.505376	120.8557	528 b
10.1.17.215	185.188.32.26	72	10 kB	80	122	59.02%	72	10 kB	0	0 bytes	611.086898	4.9264	16 k
10.1.17.215	23.205.110.136	80	11 kB	25	171	46.78%	80	11 kB	0	0 bytes	27.933360	489.6253	178 b
10.1.17.215	52.152.180.158	82	54 kB	113	163	50.31%	82	54 kB	0	0 bytes	1150.916887	16.1100	26 k
10.1.17.215	13.107.42.16	86	23 kB	104	190	45.26%	86	23 kB	0	0 bytes	901.204887	1695.0831	108 b
10.1.17.215	51.104.15.252	90	63 kB	22	163	55.21%	90	63 kB	0	0 bytes	26.605909	132.6771	3804 b
10.1.17.215	208.89.12.153	97	9 kB	40	240	40.42%	97	9 kB	0	0 bytes	64.134918	180.4370	380 b
10.1.17.215	20.189.173.11	99	94 kB	42	167	59.28%	99	94 kB	0	0 bytes	64.878689	129.7219	5811 b
10.1.17.215	23.221.220.40	101	11 kB	18	255	39.61%	101	11 kB	0	0 bytes	26.154193	158.5094	559 b
10.1.17.215	13.107.21.239	120	42 kB	27	248	48.39%	120	42 kB	0	0 bytes	29.497494	2566.8286	131 b
10.1.17.215	13.107.246.57	187	43 kB	20	395	47.34%	187	43 kB	0	0 bytes	26.437270	2835.8769	121 b
10.1.17.215	199.232.214.172	188	14 kB	61	556	33.81%	188	14 kB	0	0 bytes	86.675316	1111.2989	101 b
10.1.17.215	204.79.197.203	255	53 kB	11	594	42.93%	255	53 kB	0	0 bytes	16.644573	1717.1930	246 b
10.1.17.215	23.205.110.143	261	137 kB	26	552	47.28%	261	137 kB	0	0 bytes	29.369530	128.7335	8434 b
10.1.17.215	23.207.166.9	275	37 kB	82	550	50.00%	275	37 kB	0	0 bytes	624.094807	109.5821	2667 b
10.1.17.215	23.55.125.176	423	199 kB	35	1,018	41.55%	423	199 kB	0	0 bytes	61.995061	455.4947	3491 b
10.1.17.215	45.125.66.252	466	39 kB	109	1,369	34.04%	466	39 kB	0	0 bytes	917.407874	2283.1342	136 b
10.1.17.215	82.221.136.26	834	53 kB	31	2,470	33.77%	834	53 kB	0	0 bytes	39.388705	74.4499	5673 b
10.1.17.215	5.252.153.241	3,475	235 kB	34	9,076	38.29%	3,475	235 kB	0	0 bytes	60.135270	3142.2528	599 b
10.1.17.215	45.125.66.32	3,737	587 kB	95	10,940	34.16%	3,737	587 kB	0	0 bytes	889.561525	1720.6308	2729 b