
- 192.168.220.101
- IPs 62.1.38.50 and 93.184.220.29
- LLMNR/NBNS exploitation, HTTP communication to external servers
- 7-10-2024

-
    - Host attempted communication with external IP addresses and over .
    - These external IP addresses may represent a (C2) or are being used for .
    - The HTTP GET requests include (Base64-like), which might indicate communication between the attacker and the compromised host.
-
    - Wireshark packets showing TCP communication to and via HTTP GET requests.
    - Screenshot of TCP/HTTP traffic indicating potential exfiltration attempts.

-
    - Extensive were observed originating from , , and other hosts, targeting 224.0.0.252 and other broadcast addresses.
    - These protocols are often exploited to capture network credentials through using tools like .
    - The attack may have been used for or to steal credentials, which could facilitate within the network.
-
    - Packet captures showing and queries and responses.
    - Screenshots showing .

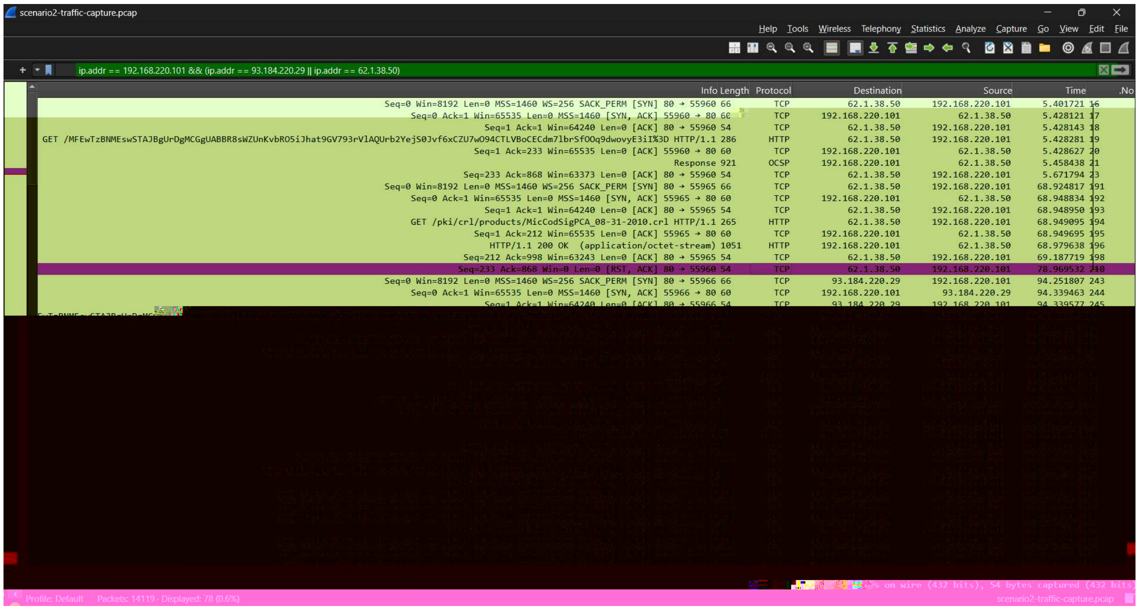
-
    - The compromised host, , initiated HTTP GET requests with in the URL, likely part of the attack communication or exfiltration.
    - These requests to and other URLs are abnormal and potentially malicious.
-
    - Captured HTTP GET requests showing .
    - Screenshots and packet captures showing the suspicious HTTP requests.

The investigation revealed that host was compromised and engaged in with IP addresses that could be associated with . Additionally, traffic indicates the attacker may have been for further lateral movement within the network.

- host and perform a full forensic analysis.
- Investigate and block communication to the external IPs and .
- Disable protocols across the network to prevent credential harvesting attacks.
- Monitor for similar traffic patterns across the network and scan for further signs of lateral movement.

The initial foothold was likely gained through suspicious traffic observed between the compromised host ( ) and external IP addresses (and). This communication included HTTP GET requests with Base64-encoded data, possibly indicating exfiltration of data or communication with a Command and Control (C2) server.

- : Suspicious HTTP GET request with Base64-encoded data sent from to .

- 

scenario2-traffic-capture.pcap
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File

```
ip.addr == 192.168.220.101 && (ip.addr == 93.184.220.29 || ip.addr == 62.1.38.50)

                                                                                              Info Length Protocol      Destination           Source        Time  .No
                                                Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 55960 66    TCP       62.1.38.50  192.168.220.101    5.401721 16
                                                   Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 [SYN, ACK] 55960 → 80 60    TCP  192.168.220.101       62.1.38.50    5.428121 17
                                                              Seq=1 Ack=1 Win=64240 Len=0 [ACK] 80 → 55960 54    TCP       62.1.38.50  192.168.220.101    5.428143 18
GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D HTTP/1.1 286   HTTP       62.1.38.50  192.168.220.101    5.428281 19
                                                            Seq=1 Ack=233 Win=65535 Len=0 [ACK] 55960 → 80 60    TCP  192.168.220.101       62.1.38.50    5.428627 20
                                                                                                 Response 921   OCSP  192.168.220.101       62.1.38.50    5.458438 21
                                                           Seq=233 Ack=868 Win=63373 Len=0 [ACK] 80 → 55960 54    TCP       62.1.38.50  192.168.220.101    5.671794 23
                                                Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 55965 66    TCP       62.1.38.50  192.168.220.101   68.924817 191
                                                   Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 [SYN, ACK] 55965 → 80 60    TCP  192.168.220.101       62.1.38.50   68.948834 192
                                                              Seq=1 Ack=1 Win=64240 Len=0 [ACK] 80 → 55965 54    TCP       62.1.38.50  192.168.220.101   68.948950 193
                                                   GET /pki/crl/products/MicCodSigPCA_08-31-2010.crl HTTP/1.1 265   HTTP       62.1.38.50  192.168.220.101   68.949095 194
                                                            Seq=1 Ack=212 Win=65535 Len=0 [ACK] 55965 → 80 60    TCP  192.168.220.101       62.1.38.50   68.949695 195
                                                             HTTP/1.1 200 OK  (application/octet-stream) 1051   HTTP  192.168.220.101       62.1.38.50   68.979638 196
                                                           Seq=212 Ack=998 Win=63243 Len=0 [ACK] 80 → 55965 54    TCP       62.1.38.50  192.168.220.101   69.187719 198
                                                       Seq=233 Ack=868 Win=0 Len=0 [RST, ACK] 80 → 55960 54    TCP       62.1.38.50  192.168.220.101   78.969532 240
                                                Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 80 → 55966 66    TCP    93.184.220.29  192.168.220.101   94.251807 243
                                                   Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 [SYN, ACK] 55966 → 80 60    TCP  192.168.220.101    93.184.220.29   94.339463 244
                                                              Seq=1 Ack=1 Win=64240 Len=0 [ACK] 80 → 55966 54    TCP    93.184.220.29  192.168.220.101   94.339577 245
```

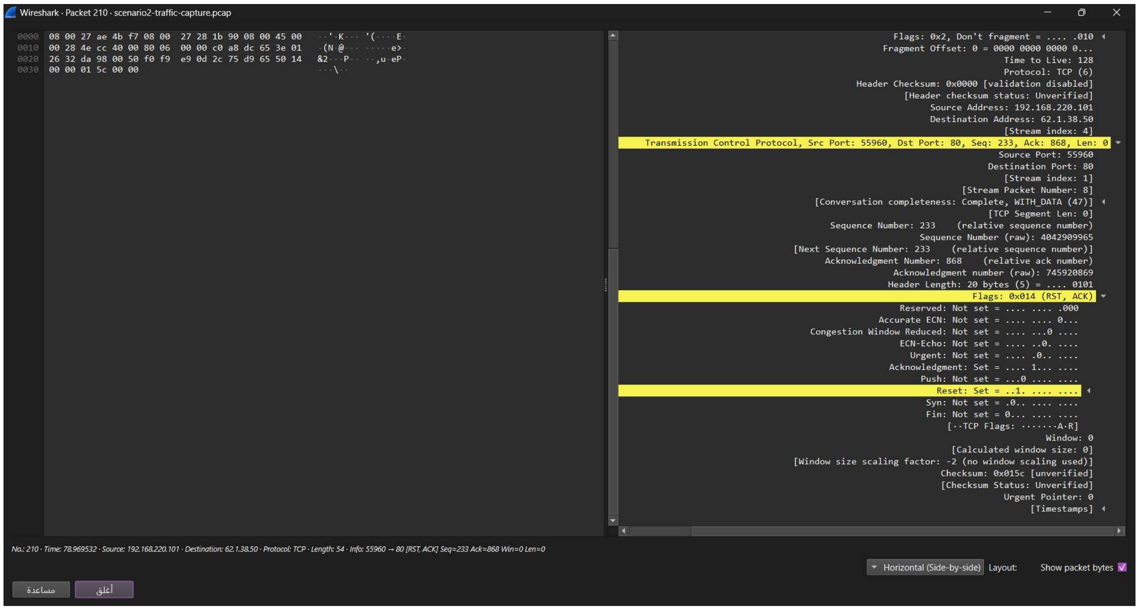
[redacted]

```
s on wire (432 bits), 54 bytes captured (432 bits)
Profile: Default   Packets: 14119 · Displayed: 78 (0.6%)                                    scenario2-traffic-capture.pcap
```

From the packet capture analysis, it appears that the only host involved in this communication was the endpoint. There is no evidence of lateral movement to other hosts in the network based on this capture.

No direct evidence of the Domain Controller being accessed was found in this packet capture. However, further logs from the Domain Controller should be reviewed for unusual authentication attempts or suspicious SMB/RDP traffic.

- : There were multiple instances of and queries broadcast from to , indicating possible reconnaissance activity by the attacker.



Wireshark · Packet 210 · scenario2-traffic-capture.pcap

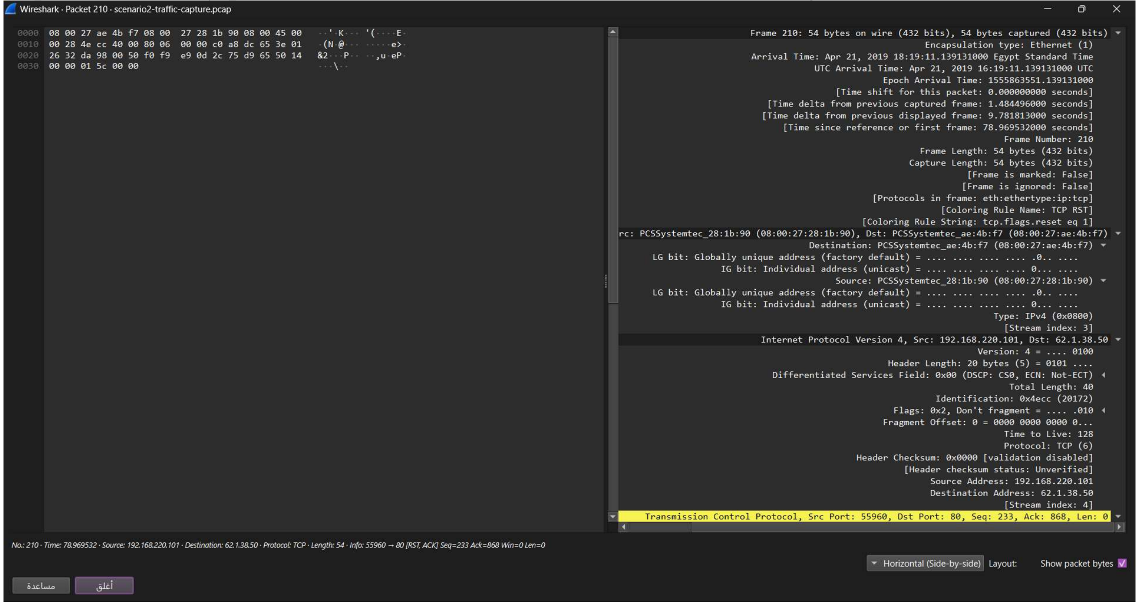
```
0000  08 00 27 ae 4b f7 08 00  27 28 1b 90 08 00 45 00   ··'·K···'(····E·
0010  00 28 4e cc 40 00 80 06  00 00 c0 a8 dc 65 3e 01   ·(N·@·······e>·
0020  26 32 da 98 00 50 f0 f9  e9 0d 2c 75 d9 65 50 14   &2···P····,u·eP·
0030  00 00 01 5c 00 00                                  ···\··
```

```
                          Flags: 0x2, Don't fragment = .... .010
                   Fragment Offset: 0 = 0000 0000 0000 0...
                                           Time to Live: 128
                                           Protocol: TCP (6)
                  Header Checksum: 0x0000 [validation disabled]
                        [Header checksum status: Unverified]
                               Source Address: 192.168.220.101
                              Destination Address: 62.1.38.50
                                            [Stream index: 4]
Transmission Control Protocol, Src Port: 55960, Dst Port: 80, Seq: 233, Ack: 868, Len: 0
                                           Source Port: 55960
                                         Destination Port: 80
                                            [Stream index: 1]
                                     [Stream Packet Number: 8]
           [Conversation completeness: Complete, WITH_DATA (47)]
                                         [TCP Segment Len: 0]
            Sequence Number: 233    (relative sequence number)
                           Sequence Number (raw): 4042909965
      [Next Sequence Number: 233    (relative sequence number)]
           Acknowledgment Number: 868    (relative ack number)
                       Acknowledgment number (raw): 745920869
                      Header Length: 20 bytes (5) = .... 0101
                                       Flags: 0x014 (RST, ACK)
                       Reserved: Not set = .... .... .000
                   Accurate ECN: Not set = .... .... 0...
       Congestion Window Reduced: Not set = .... ...0 ....
                       ECN-Echo: Not set = .... ..0. ....
                         Urgent: Not set = .... .0.. ....
                    Acknowledgment: Set = .... 1... ....
                           Push: Not set = ...0 .... ....
                              Reset: Set = ..1. .... ....
                            Syn: Not set = .0.. .... ....
                            Fin: Not set = 0... .... ....
                                  [··TCP Flags: ·······A·R]
                                                    Window: 0
                                  [Calculated window size: 0]
      [Window size scaling factor: -2 (no window scaling used)]
                            Checksum: 0x015c [unverified]
                            [Checksum Status: Unverified]
                                            Urgent Pointer: 0
                                                 [Timestamps]
```

No.: 210 · Time: 78.969532 · Source: 192.168.220.101 · Destination: 62.1.38.50 · Protocol: TCP · Length: 54 · Info: 55960 → 80 [RST, ACK] Seq=233 Ack=868 Win=0 Len=0

-
- : Name queries sent by the compromised host via LLMNR and NBNS traffic.

- : The compromised host communicated with and , sending HTTP GET requests with encoded data. These requests are likely part of the exfiltration or C2 communication stage.



Wireshark · Packet 210 · scenario2-traffic-capture.pcap

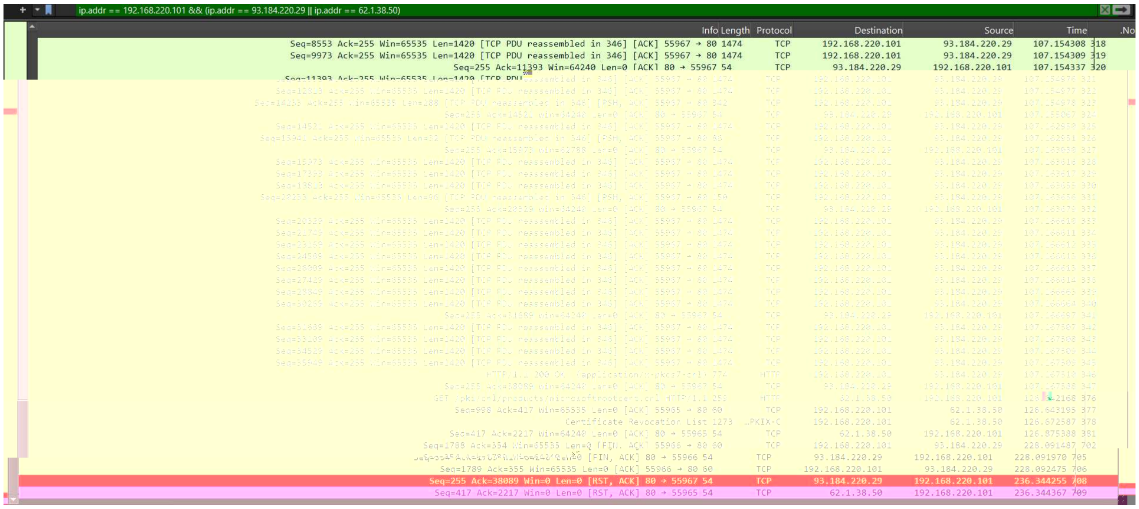
```
0000  08 00 27 ae 4b f7 08 00  27 28 1b 90 08 00 45 00   ··'·K···'(····E·
0010  00 28 4e cc 40 00 80 06  00 00 c0 a8 dc 65 3e 01   ·(N·@·······e>·
0020  26 32 da 98 00 50 f0 f9  e9 0d 2c 75 d9 65 50 14   &2···P····,u·eP·
0030  00 00 01 5c 00 00                                  ···\··
```

```
            Frame 210: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
                                        Encapsulation type: Ethernet (1)
          Arrival Time: Apr 21, 2019 18:19:11.139131000 Egypt Standard Time
                 UTC Arrival Time: Apr 21, 2019 16:19:11.139131000 UTC
                              Epoch Arrival Time: 1555863551.139131000
                      [Time shift for this packet: 0.000000000 seconds]
         [Time delta from previous captured frame: 1.484496000 seconds]
        [Time delta from previous displayed frame: 9.781813000 seconds]
           [Time since reference or first frame: 78.969532000 seconds]
                                                      Frame Number: 210
                                        Frame Length: 54 bytes (432 bits)
                                      Capture Length: 54 bytes (432 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]
rc: PCSSystemtec_28:1b:90 (08:00:27:28:1b:90), Dst: PCSSystemtec_ae:4b:f7 (08:00:27:ae:4b:f7)
                   Destination: PCSSystemtec_ae:4b:f7 (08:00:27:ae:4b:f7)
   LG bit: Globally unique address (factory default) = .... .... .... .... .0.. ....
            IG bit: Individual address (unicast) = .... .... .... .... 0... ....
                        Source: PCSSystemtec_28:1b:90 (08:00:27:28:1b:90)
   LG bit: Globally unique address (factory default) = .... .... .... .... .0.. ....
            IG bit: Individual address (unicast) = .... .... .... .... 0... ....
                                                      Type: IPv4 (0x0800)
                                                        [Stream index: 3]
                 Internet Protocol Version 4, Src: 192.168.220.101, Dst: 62.1.38.50
                                                    Version: 4 = .... 0100
                                      Header Length: 20 bytes (5) = 0101 ....
                  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                                                        Total Length: 40
                                              Identification: 0x4ecc (20172)
                                      Flags: 0x2, Don't fragment = .... .010
                               Fragment Offset: 0 = 0000 0000 0000 0...
                                                       Time to Live: 128
                                                       Protocol: TCP (6)
                              Header Checksum: 0x0000 [validation disabled]
                                    [Header checksum status: Unverified]
                                           Source Address: 192.168.220.101
                                          Destination Address: 62.1.38.50
                                                        [Stream index: 4]
Transmission Control Protocol, Src Port: 55960, Dst Port: 80, Seq: 233, Ack: 868, Len: 0
```

No.: 210 · Time: 78.969532 · Source: 192.168.220.101 · Destination: 62.1.38.50 · Protocol: TCP · Length: 54 · Info: 55960 → 80 [RST, ACK] Seq=233 Ack=868 Win=0 Len=0

-
- : HTTP GET request showing communication to an external IP.

- The communication between the compromised host and the external IPs was terminated with packets, which may indicate deliberate session termination by the attacker or a disruption in communication.



```
ip.addr == 192.168.220.101 && (ip.addr == 93.184.220.29 || ip.addr == 62.1.38.50)

                                                                                     Info Length  Protocol      Destination          Source         Time  .No
 Seq=8553 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.154308 318
 Seq=9973 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.154309 319
                        Seq=255 Ack=11393 Win=64240 Len=0 [ACK] 80 → 55967 54              TCP      93.184.220.29   192.168.220.101   107.154337 320
Seq=11393 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.154976 321
Seq=12813 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.154977 322
Seq=14233 Ack=255 Win=65535 Len=288 [TCP PDU reassembled in 346] [PSH, ACK] 55967 → 80 342 TCP    192.168.220.101     93.184.220.29   107.154978 323
                        Seq=255 Ack=14521 Win=64240 Len=0 [ACK] 80 → 55967 54              TCP      93.184.220.29   192.168.220.101   107.155067 324
Seq=14521 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.162950 325
Seq=15941 Ack=255 Win=65535 Len=32 [TCP PDU reassembled in 346] [PSH, ACK] 55967 → 80 86   TCP    192.168.220.101     93.184.220.29   107.162951 326
                        Seq=255 Ack=15973 Win=62788 Len=0 [ACK] 80 → 55967 54              TCP      93.184.220.29   192.168.220.101   107.163050 327
Seq=15973 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.163616 328
Seq=17393 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.163617 329
Seq=18813 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.163655 330
Seq=20233 Ack=255 Win=65535 Len=96 [TCP PDU reassembled in 346] [PSH, ACK] 55967 → 80 150  TCP    192.168.220.101     93.184.220.29   107.163656 331
                        Seq=255 Ack=20329 Win=64240 Len=0 [ACK] 80 → 55967 54              TCP      93.184.220.29   192.168.220.101   107.163679 332
Seq=20329 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166610 333
Seq=21749 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166611 334
Seq=23169 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166612 335
Seq=24589 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166613 336
Seq=26009 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166613 337
Seq=27429 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166614 338
Seq=28849 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166663 339
Seq=30269 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.166664 340
                        Seq=255 Ack=31689 Win=64240 Len=0 [ACK] 80 → 55967 54              TCP      93.184.220.29   192.168.220.101   107.166697 341
Seq=31689 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.167507 342
Seq=33109 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.167508 343
Seq=34529 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.167509 344
Seq=35949 Ack=255 Win=65535 Len=1420 [TCP PDU reassembled in 346] [ACK] 55967 → 80 1474    TCP    192.168.220.101     93.184.220.29   107.167509 345
                       HTTP/1.1 200 OK  (application/x-pkcs7-crl) 774                     HTTP    192.168.220.101     93.184.220.29   107.167510 346
                        Seq=255 Ack=38089 Win=64240 Len=0 [ACK] 80 → 55967 54              TCP      93.184.220.29   192.168.220.101   107.167588 347
              GET /pki/crl/products/microsoftrootcert.crl HTTP/1.1 259                     HTTP         62.1.38.50   192.168.220.101   12[illegible]2168 376
                          Seq=998 Ack=417 Win=65535 Len=0 [ACK] 55965 → 80 60              TCP    192.168.220.101        62.1.38.50   126.643195 377
                                             Certificate Revocation List 1273            …PKIX-C  192.168.220.101        62.1.38.50   126.672587 378
                         Seq=417 Ack=2217 Win=64240 Len=0 [ACK] 80 → 55965 54              TCP         62.1.38.50   192.168.220.101   126.875388 381
                   Seq=1788 Ack=354 Win=65535 Len=0 [FIN, ACK] 55966 → 80 60               TCP    192.168.220.101     93.184.220.29   228.091487 702
                   Seq=354 Ack=1789 Win=64240 Len=0 [FIN, ACK] 80 → 55966 54               TCP      93.184.220.29   192.168.220.101   228.091970 705
                        Seq=1789 Ack=355 Win=65535 Len=0 [ACK] 55966 → 80 60               TCP    192.168.220.101     93.184.220.29   228.092475 706
                   Seq=255 Ack=38089 Win=0 Len=0 [RST, ACK] 80 → 55967 54                  TCP      93.184.220.29   192.168.220.101   236.344255 708
                    Seq=417 Ack=2217 Win=0 Len=0 [RST, ACK] 80 → 55965 54                  TCP         62.1.38.50   192.168.220.101   236.344367 709
```

-
- : RST, ACK packet indicating termination of the session between and .

Based on the captured network traffic, it is evident that the compromised host ( ) engaged in suspicious communication with external servers, possibly indicating data exfiltration or C2 activity. Further investigation of logs on the host and the network should be conducted to confirm the full extent of the breach.