INCIDENT OVERVIEW	
Investigator	Meenakshi
Date/Time	5/4/2025, 8:00 PM
Target of Attack	IP ADDRESS: 172.16.1.239; MAC ADDRESS: 00:13:d4:10:05:25

BUSINESS IMPACT	
Attack Vector	Malicious excel spreadsheet (Receipt-9650354.xls) and a binary file (file6.bin)
Impact	If the download excel file was opened by a user and contained malicious macros, it could have executed a code that downloaded the .bin file. This may result in unauthorized remote access, data theft, or installation of additional malicious tool impacting the organizational data, system integrity and business continuity.
Recoverability	- Isolate the infected system from the network, - Remove the malicious files, - Perform a system clean-up and scan, - Reset the credentials on the system, and - Monitor the network activity on the system.

DESCRIPTION OF INCIDENT/ACTIVITY			
Date/Time of Initial Breach	July 14, 2021 – 4:31:08 PM	User(s) Impacted	N/A
Record(s) Impacted	N/A	System(s) Impacted	172.16.1.239; 00:13:d4:10:05:25

Executive Summary:

The network investigation of the packet capture file revealed that the host 172.16.1.239 downloaded a suspicious Excel file (Receipt-9650354.xls) via HTTP from the external IP 185.21.216.153 (*see supporting artifacts*). The HTTP response from the external IP returned a 200 OK Status code along with a content body confirming that the excel file was successfully received by the host over HTTP. Shortly after this download, the host downloaded a second file file6.bin from the same external server. This file was a binary file type commonly associated with malware executables. The back-to-back download of a document followed by a binary file suggests a multi-stage infection attempt where the .xls file might be potentially triggering the download of the executable.

These findings point to a malware infection attempt that targeted the internal system.

Indicators of Compromise/Root Cause of incident:

The indicators of the compromise are the HTTP GET calls to download the Receipt-9650354.xls and file6.bin files where the destination IP was an external IP and flagged as a malicious IP by VirusTotal (*see supporting artifacts*).

Suggested mitigation action (how can we resolve this issue?):

This issue can be resolved by,

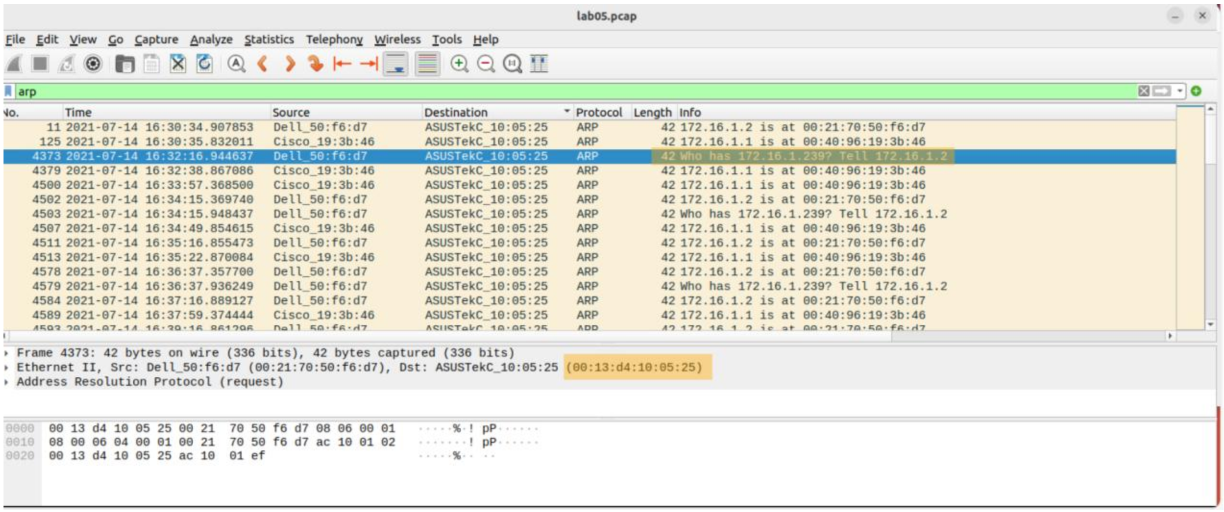
- Immediately isolating the affected system,
- Conducting endpoint malware scans,
- Blocking the external IP 185.21.216.153 at firewall and proxy
- Removing the malicious files,
- Perform a system clean-up and scans,
- Resetting the credentials on the system and auditing for any unauthorized access,
- Monitoring the network activity on the affected system, and
- Reviewing firewall and proxy logs for other devices accessing the same external IP.

Lessons Learned/Opportunity for Improvement (how can we avoid this in the future?):

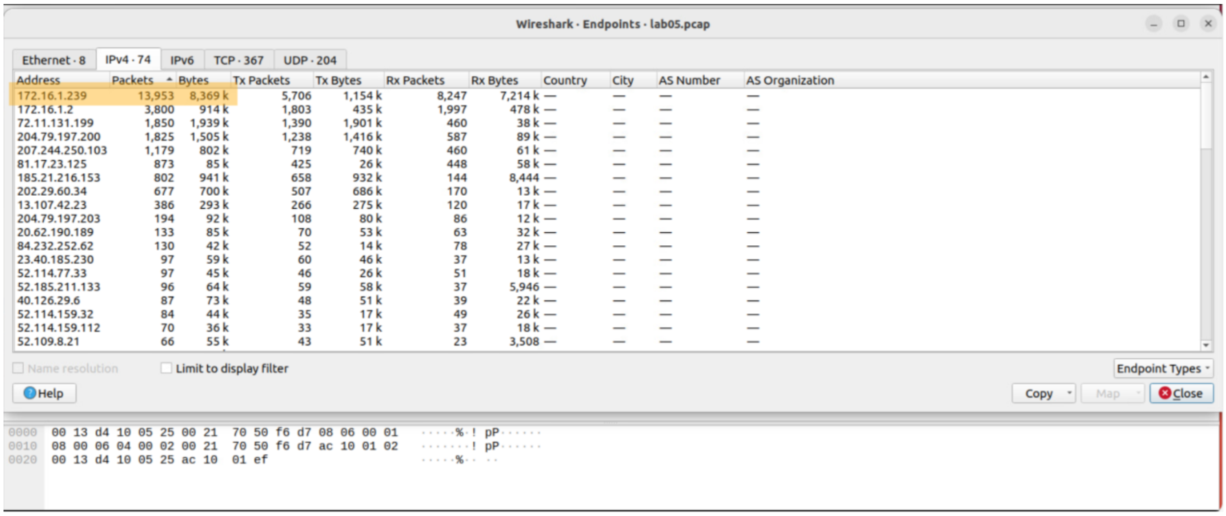
These incidents and attacks can be avoided by implementing the following measures,

- Use of HTTPS only for file downloads and restricted access to known-safe domains.
- Stronger content inspection and sandboxing for incoming files.
- User awareness trainings on phishing and malicious activity through documents
- Network log monitoring for early detection of file downloads from external sources

Supporting Artifacts (any screenshots of evidence)
Page 1 of 2


lab05.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

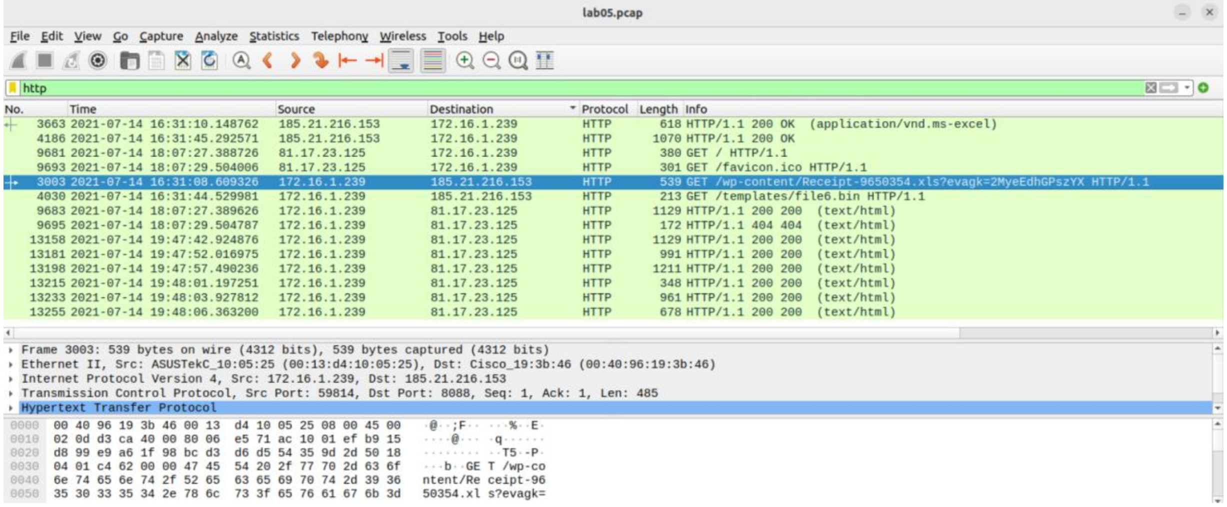
```
arp
No.   Time                        Source           Destination        Protocol Length Info
   11 2021-07-14 16:30:34.907853  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 172.16.1.2 is at 00:21:70:50:f6:d7
  125 2021-07-14 16:30:35.832011  Cisco_19:3b:46   ASUSTekC_10:05:25  ARP      42 172.16.1.1 is at 00:40:96:19:3b:46
 4373 2021-07-14 16:32:16.944637  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 Who has 172.16.1.239? Tell 172.16.1.2
 4379 2021-07-14 16:32:38.867086  Cisco_19:3b:46   ASUSTekC_10:05:25  ARP      42 172.16.1.1 is at 00:40:96:19:3b:46
 4500 2021-07-14 16:33:57.368500  Cisco_19:3b:46   ASUSTekC_10:05:25  ARP      42 172.16.1.1 is at 00:40:96:19:3b:46
 4502 2021-07-14 16:34:15.369740  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 172.16.1.2 is at 00:21:70:50:f6:d7
 4503 2021-07-14 16:34:15.948437  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 Who has 172.16.1.239? Tell 172.16.1.2
 4507 2021-07-14 16:34:49.854615  Cisco_19:3b:46   ASUSTekC_10:05:25  ARP      42 172.16.1.1 is at 00:40:96:19:3b:46
 4511 2021-07-14 16:35:16.855473  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 172.16.1.2 is at 00:21:70:50:f6:d7
 4513 2021-07-14 16:35:22.870084  Cisco_19:3b:46   ASUSTekC_10:05:25  ARP      42 172.16.1.1 is at 00:40:96:19:3b:46
 4578 2021-07-14 16:36:37.357700  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 172.16.1.2 is at 00:21:70:50:f6:d7
 4579 2021-07-14 16:36:37.936249  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 Who has 172.16.1.239? Tell 172.16.1.2
 4584 2021-07-14 16:37:16.889127  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 172.16.1.2 is at 00:21:70:50:f6:d7
 4589 2021-07-14 16:37:59.374444  Cisco_19:3b:46   ASUSTekC_10:05:25  ARP      42 172.16.1.1 is at 00:40:96:19:3b:46
 4593 2021-07-14 16:39:16.861296  Dell_50:f6:d7    ASUSTekC_10:05:25  ARP      42 172.16.1.2 is at 00:21:70:50:f6:d7

› Frame 4373: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
› Ethernet II, Src: Dell_50:f6:d7 (00:21:70:50:f6:d7), Dst: ASUSTekC_10:05:25 (00:13:d4:10:05:25)
› Address Resolution Protocol (request)

0000  00 13 d4 10 05 25 00 21  70 50 f6 d7 08 06 00 01   ·····%·! pP······
0010  08 00 06 04 00 01 00 21  70 50 f6 d7 ac 10 01 02   ·······! pP······
0020  00 13 d4 10 05 25 ac 10  01 ef                     ·····%·· ··
```



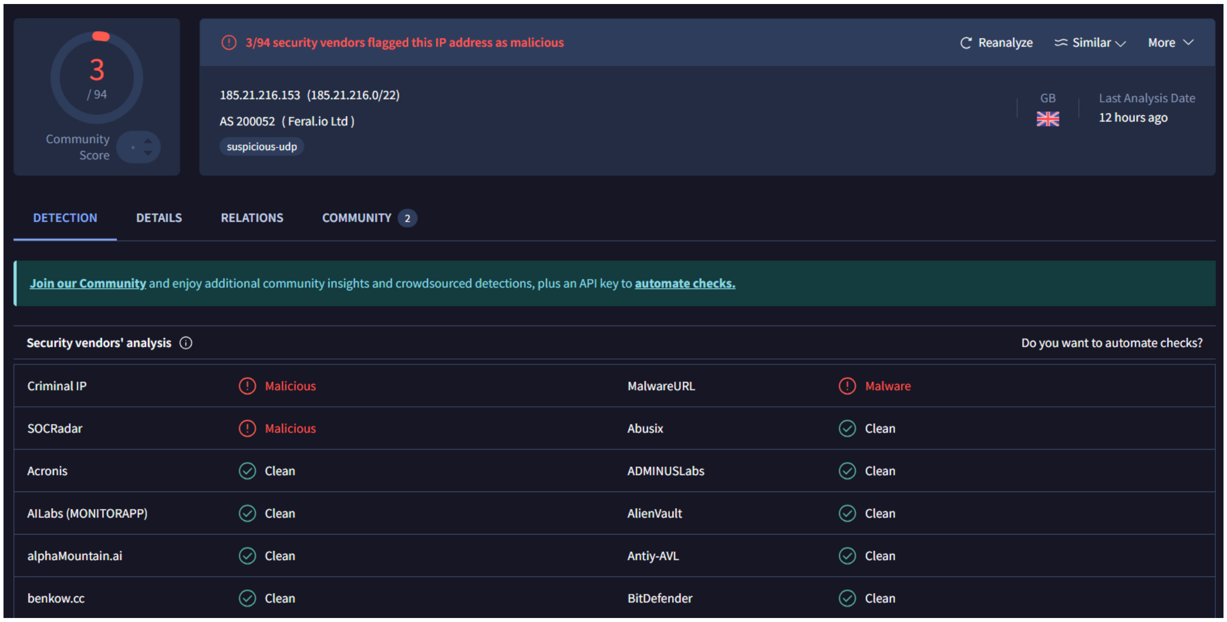
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
172.16.1.239	13,953	8,369 k	5,706	1,154 k	8,247	7,214 k	—	—	—	—
172.16.1.2	3,800	914 k	1,803	435 k	1,997	478 k	—	—	—	—
72.11.131.199	1,850	1,939 k	1,390	1,901 k	460	38 k	—	—	—	—
204.79.197.200	1,825	1,505 k	1,238	1,416 k	587	89 k	—	—	—	—
207.244.250.103	1,179	802 k	719	740 k	460	61 k	—	—	—	—
81.17.23.125	873	85 k	425	26 k	448	58 k	—	—	—	—
185.21.216.153	802	941 k	658	932 k	144	8,444	—	—	—	—
202.29.60.34	677	700 k	507	686 k	170	13 k	—	—	—	—
13.107.42.23	386	293 k	266	275 k	120	17 k	—	—	—	—
204.79.197.203	194	92 k	108	80 k	86	12 k	—	—	—	—
20.62.190.189	133	85 k	70	53 k	63	32 k	—	—	—	—
84.232.252.62	130	42 k	52	14 k	78	27 k	—	—	—	—
23.40.185.230	97	59 k	60	46 k	37	13 k	—	—	—	—
52.114.77.33	97	45 k	46	26 k	51	18 k	—	—	—	—
52.185.211.133	96	64 k	59	58 k	37	5,946	—	—	—	—
40.126.29.6	87	73 k	48	51 k	39	22 k	—	—	—	—
52.114.159.32	84	44 k	35	17 k	49	26 k	—	—	—	—
52.114.159.112	70	36 k	33	17 k	37	18 k	—	—	—	—
52.109.8.21	66	55 k	43	51 k	23	3,508	—	—	—	—

☐ Name resolution ☐ Limit to display filter

```
0000  00 13 d4 10 05 25 00 21  70 50 f6 d7 08 06 00 01   ·····%·! pP······
0010  08 00 06 04 00 02 00 21  70 50 f6 d7 ac 10 01 02   ·······! pP······
0020  00 13 d4 10 05 25 ac 10  01 ef                     ·····%·· ··
```


lab05.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.    Time                        Source           Destination      Protocol Length Info
  3663 2021-07-14 16:31:10.148762  185.21.216.153   172.16.1.239     HTTP     618 HTTP/1.1 200 OK  (application/vnd.ms-excel)
  4186 2021-07-14 16:31:45.292571  185.21.216.153   172.16.1.239     HTTP    1070 HTTP/1.1 200 OK
  9681 2021-07-14 18:07:27.388726  81.17.23.125     172.16.1.239     HTTP     380 GET / HTTP/1.1
  9693 2021-07-14 18:07:29.504006  81.17.23.125     172.16.1.239     HTTP     301 GET /favicon.ico HTTP/1.1
  3003 2021-07-14 16:31:08.609326  172.16.1.239     185.21.216.153   HTTP     539 GET /wp-content/Receipt-9650354.xls?evagk=2MyeEdhGPszYX HTTP/1.1
  4030 2021-07-14 16:31:44.529981  172.16.1.239     185.21.216.153   HTTP     213 GET /templates/file6.bin HTTP/1.1
  9683 2021-07-14 18:07:27.389626  172.16.1.239     81.17.23.125     HTTP    1129 HTTP/1.1 200 200  (text/html)
  9695 2021-07-14 18:07:29.504787  172.16.1.239     81.17.23.125     HTTP     172 HTTP/1.1 404 404  (text/html)
 13158 2021-07-14 19:47:42.924876  172.16.1.239     81.17.23.125     HTTP    1129 HTTP/1.1 200 200  (text/html)
 13181 2021-07-14 19:47:52.016975  172.16.1.239     81.17.23.125     HTTP     991 HTTP/1.1 200 200  (text/html)
 13198 2021-07-14 19:47:57.490236  172.16.1.239     81.17.23.125     HTTP    1211 HTTP/1.1 200 200  (text/html)
 13215 2021-07-14 19:48:01.197251  172.16.1.239     81.17.23.125     HTTP     348 HTTP/1.1 200 200  (text/html)
 13233 2021-07-14 19:48:03.927812  172.16.1.239     81.17.23.125     HTTP     961 HTTP/1.1 200 200  (text/html)
 13255 2021-07-14 19:48:06.363200  172.16.1.239     81.17.23.125     HTTP     678 HTTP/1.1 200 200  (text/html)

› Frame 3003: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)
› Ethernet II, Src: ASUSTekC_10:05:25 (00:13:d4:10:05:25), Dst: Cisco_19:3b:46 (00:40:96:19:3b:46)
› Internet Protocol Version 4, Src: 172.16.1.239, Dst: 185.21.216.153
› Transmission Control Protocol, Src Port: 59814, Dst Port: 8088, Seq: 1, Ack: 1, Len: 485
› Hypertext Transfer Protocol

0000  00 40 96 19 3b 46 00 13  d4 10 05 25 08 00 45 00   ·@··;F·· ···%··E·
0010  02 0d d3 ca 40 00 80 06  e5 71 ac 10 01 ef b9 15   ····@··· ·q······
0020  d8 99 e9 a6 1f 98 bc d3  d6 d5 54 35 9d 2d 50 18   ········ ··T5·-P·
0030  04 01 c4 62 00 00 47 45  54 20 2f 77 70 2d 63 6f   ···b··GE T /wp-co
0040  6e 74 65 6e 74 2f 52 65  63 65 69 70 74 2d 39 36   ntent/Re ceipt-96
0050  35 30 33 35 34 2e 78 6c  73 3f 65 76 61 67 6b 3d   50354.xl s?evagk=
```



3/94 security vendors flagged this IP address as malicious

185.21.216.153 (185.21.216.0/22)

AS 200052 (Feral.io Ltd)

suspicious-udp

GB

Last Analysis Date
12 hours 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?

Criminal IP	Malicious	MalwareURL	Malware
SOCRadar	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
benkow.cc	Clean	BitDefender	Clean