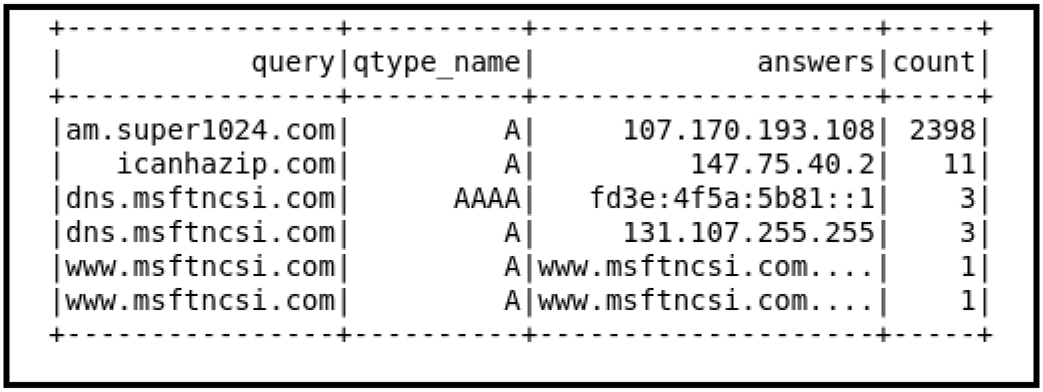
Analysis of DNS, HTTP, Connection, Files and DHCP Logs

I. Introduction

This report presents the analysis of DNS, HTTP, Connection, Files, and DHCP logs. The logs were collected to investigate any suspicious activities on the network. The investigation focused on identifying any indicators of compromise (IOCs) that could be an indication of malicious activity.

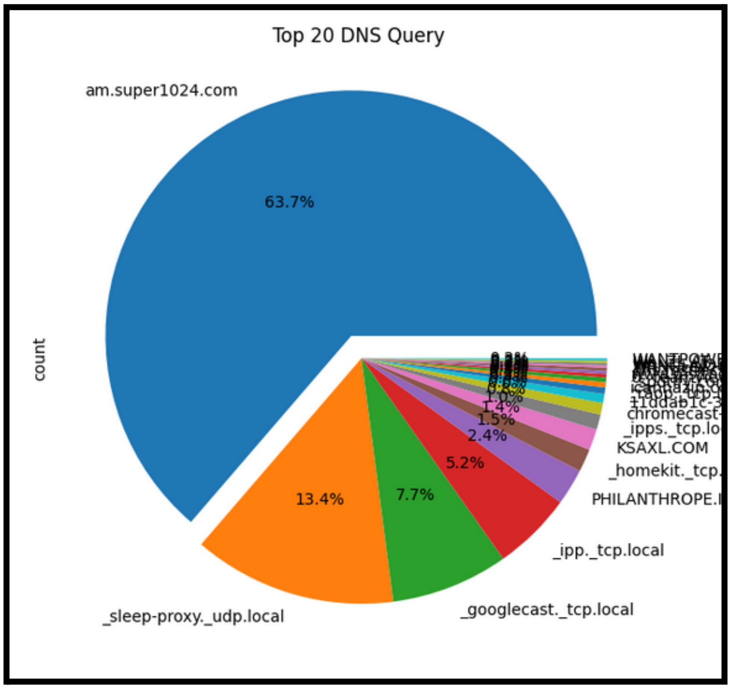
II. Analysis

A. DNS Log



```
+----------------+----------+-------------------+-----+
|           query|qtype_name|            answers|count|
+----------------+----------+-------------------+-----+
|am.super1024.com|         A|    107.170.193.108| 2398|
|   icanhazip.com|         A|        147.75.40.2|   11|
|dns.msftncsi.com|      AAAA|   fd3e:4f5a:5b81::1|    3|
|dns.msftncsi.com|         A|    131.107.255.255|    3|
|www.msftncsi.com|         A|www.msftncsi.com....|    1|
|www.msftncsi.com|         A|www.msftncsi.com....|    1|
+----------------+----------+-------------------+-----+
```

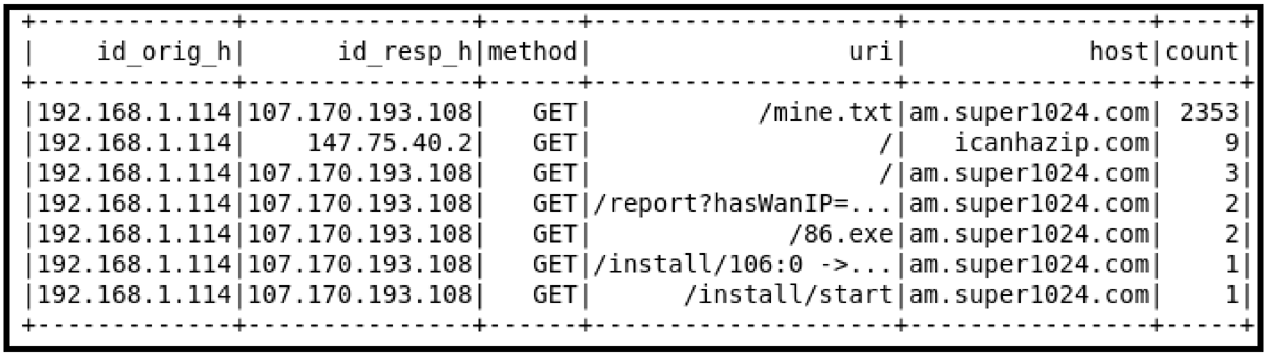
Figure 1: The number of DNS query over time



The DNS log revealed that am.super1024.com was the most requested domain. The log showed that 2398 DNS query requests were sent, accounting for about 63.7% in the Top 20 DNS Query. Excluding all the blank DNS, we end up with only five domains. This could be an indication that this domain is being targeted for malicious activity.

Figure 2: Top 20 DNS Queries by Percentage

B. HTTP Log

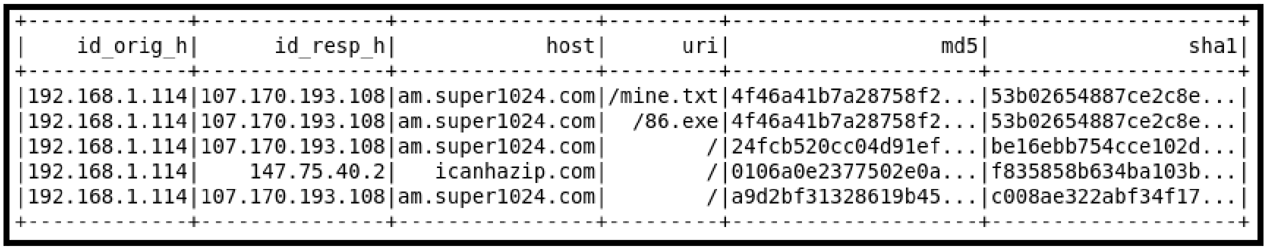


```
+-------------+---------------+------+--------------------+----------------+-----+
|    id_orig_h|      id_resp_h|method|                 uri|            host|count|
+-------------+---------------+------+--------------------+----------------+-----+
|192.168.1.114|107.170.193.108|   GET|           /mine.txt|am.super1024.com| 2353|
|192.168.1.114|    147.75.40.2|   GET|                   /|   icanhazip.com|    9|
|192.168.1.114|107.170.193.108|   GET|                   /|am.super1024.com|    3|
|192.168.1.114|107.170.193.108|   GET|/report?hasWanIP=...|am.super1024.com|    2|
|192.168.1.114|107.170.193.108|   GET|             /86.exe|am.super1024.com|    2|
|192.168.1.114|107.170.193.108|   GET|/install/106:0 ->...|am.super1024.com|    1|
|192.168.1.114|107.170.193.108|   GET|      /install/start|am.super1024.com|    1|
+-------------+---------------+------+--------------------+----------------+-----+
```

Figure 3: Suspicious HTTP requests

The HTTP log revealed that 192.168.1.114 communicated with am.super1024.com more than 2353 times. The excessive number of requests like this should be considered an IOC. This could be an indication that this IP address is being used to perform malicious activities on the network.

C. HTTP Log, Connection Log, and Files Log

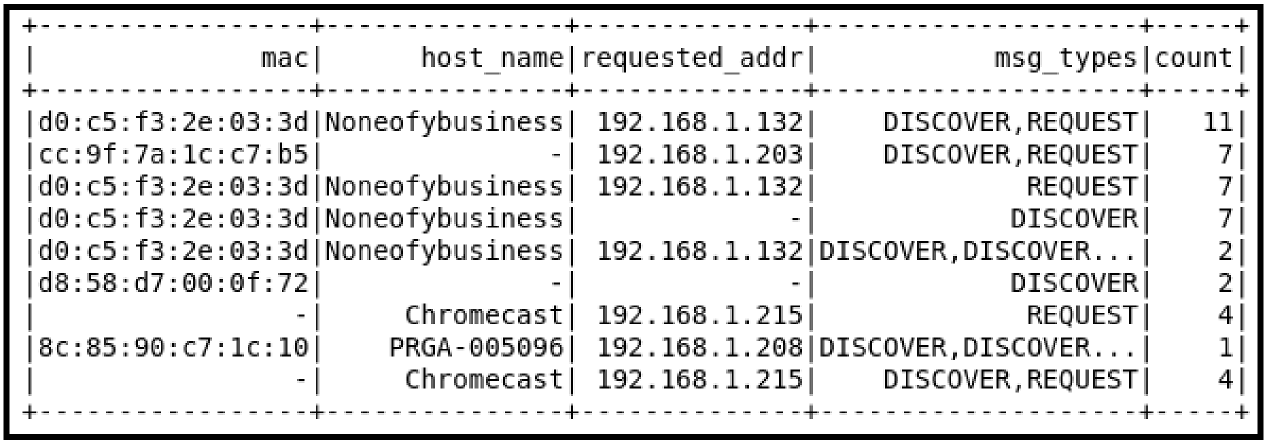


```
+-------------+---------------+----------------+---------+--------------------+--------------------+
|    id_orig_h|      id_resp_h|            host|      uri|                 md5|                sha1|
+-------------+---------------+----------------+---------+--------------------+--------------------+
|192.168.1.114|107.170.193.108|am.super1024.com|/mine.txt|4f46a41b7a28758f2...|53b02654887ce2c8e...|
|192.168.1.114|107.170.193.108|am.super1024.com|  /86.exe|4f46a41b7a28758f2...|53b02654887ce2c8e...|
|192.168.1.114|107.170.193.108|am.super1024.com|        /|24fcb520cc04d91ef...|be16ebb754cce102d...|
|192.168.1.114|    147.75.40.2|   icanhazip.com|        /|0106a0e2377502e0a...|f835858b634ba103b...|
|192.168.1.114|107.170.193.108|am.super1024.com|        /|a9d2bf31328619b45...|c008ae322abf34f17...|
+-------------+---------------+----------------+---------+--------------------+--------------------+
```

Figure 4: Metadata by linking multiple logs

After connecting the three logs, it was discovered that both /mine.txt and /86.exe have the same md5 and sha1. Therefore, it was suspected that these md5 hash and sha1 are packet hashing, not the files hash. Further investigation is needed to confirm this suspicion.

D. DHCP Log

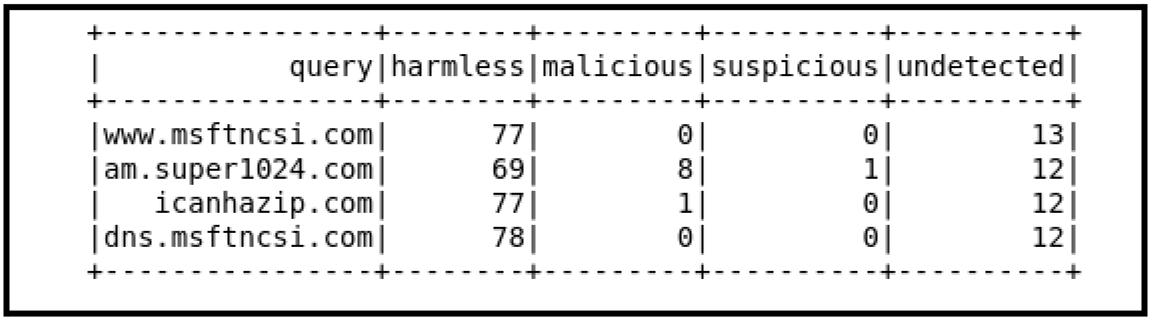


```
+-----------------+---------------+--------------+--------------------+-----+
|              mac|      host_name|requested_addr|           msg_types|count|
+-----------------+---------------+--------------+--------------------+-----+
|d0:c5:f3:2e:03:3d|Noneofybusiness| 192.168.1.132|    DISCOVER,REQUEST|   11|
|cc:9f:7a:1c:c7:b5|              -| 192.168.1.203|    DISCOVER,REQUEST|    7|
|d0:c5:f3:2e:03:3d|Noneofybusiness| 192.168.1.132|             REQUEST|    7|
|d0:c5:f3:2e:03:3d|Noneofybusiness|             -|            DISCOVER|    7|
|d0:c5:f3:2e:03:3d|Noneofybusiness| 192.168.1.132|DISCOVER,DISCOVER...|    2|
|d8:58:d7:00:0f:72|              -|             -|            DISCOVER|    2|
|                -|     Chromecast| 192.168.1.215|             REQUEST|    4|
|8c:85:90:c7:1c:10|    PRGA-005096| 192.168.1.208|DISCOVER,DISCOVER...|    1|
|                -|     Chromecast| 192.168.1.215|    DISCOVER,REQUEST|    4|
+-----------------+---------------+--------------+--------------------+-----+
```

Figure 5: DHCP log statistics

The DHCP log revealed a suspicious host name called Noneofybusiness. However, further investigation on the network did not reveal any suspicious activities. It is suggested that the owner of this device be identified before concluding it to be a false positive.

E. IOCs Investigation



```
+----------------+--------+---------+----------+----------+
|           query|harmless|malicious|suspicious|undetected|
+----------------+--------+---------+----------+----------+
|www.msftncsi.com|      77|        0|         0|        13|
|am.super1024.com|      69|        8|         1|        12|
|   icanhazip.com|      77|        1|         0|        12|
|dns.msftncsi.com|      78|        0|         0|        12|
+----------------+--------+---------+----------+----------+
```

Figure 6: IOCs detected by AV Vendors using VirusTotal

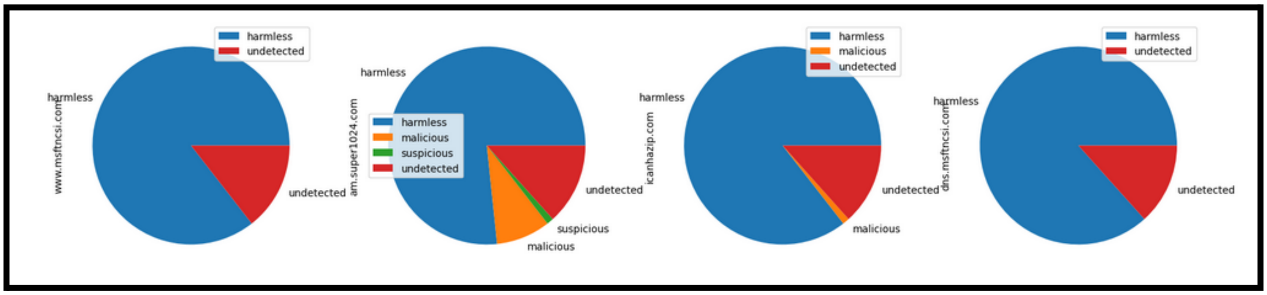


Figure 7: The chart of IOC

Further investigation on the suspicious domain revealed that VirusTotal marked am.super1024.com and icanhazip.com as malicious domains. This is a clear indication that the network is being targeted for malicious activities, and there is a need to take immediate action to prevent any potential threats.

III. Conclusion

The analysis of DNS, HTTP, Connection, Files, and DHCP logs revealed several indicators of compromise (IOCs) that could be an indication of malicious activity on the network. The investigation highlighted the need for immediate action to prevent any potential threats. Therefore, it is recommended that appropriate measures be taken to mitigate any potential risks and protect the network from malicious activities.