Project: Detecting cyberattacks in network traffic data

1. Introduction

With a given network traffic data, we have conducted a careful analysis to identify cyberattacks by leveraging the analytics capabilities of Splunk. In this report, we will introduce the details of dataset and each attack (SPAM, Port Scan and HTTP) and discuss the methods of identifying attacks, consequences and countermeasures of those attacks.

2. Overview of the network traffic dataset

To start the analysis, the dataset (traffic_capture.pcap) was ingested into PCAP Analyzer by the feature to convert .pcap file to .csv file. Once the dataset was converted to the .csv file (traffic_capture.pcap.csv), we can start to analyse the dataset on Splunk.

The dataset contains 45,853 events from 16/Feb/2021 12:46 to 13:07, which is around 21 minutes.

Figure 2.1: the start and end time of the dataset

The figure 2.2 below shows the graphical overview of the dataset in pie charts. As can be seen from the charts, the most protocols used is TCP. From the figure 2.3, we can also see that it reached around 6.8GB of traffic at peak.

Figure 2.2: graphical overview of the dataset

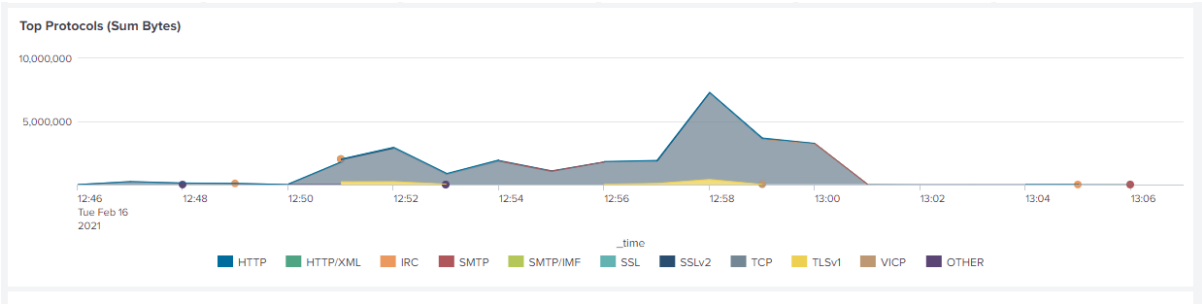


Figure 2.3: Top Protocols

From the figure 2.4, we can see that there is massive traffic between two hosts (249.56.230.66 and 212.117.171.138) from 12:50 to 13:01. Also, we can see that the host (249.56.230.66) was involved in many conversations.

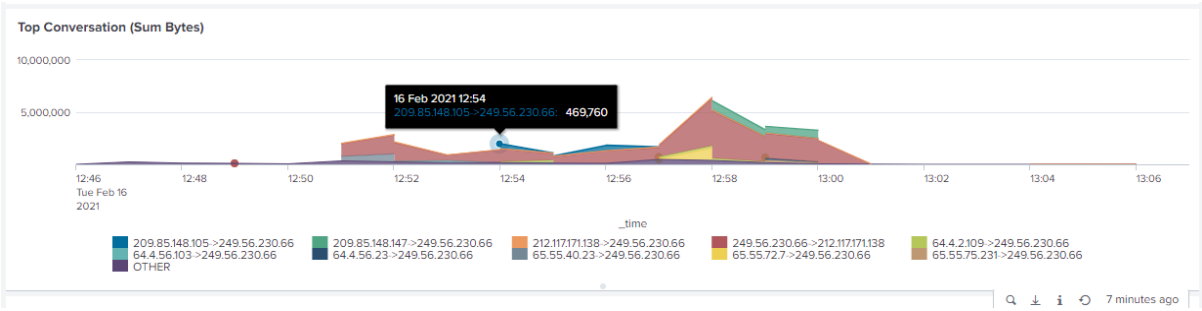


Figure 2.4: Top Conversation

Additionally, from the figure 2.5, we can see that the host (249.56.230.66) sent and received many data, and the host (212.117.171.138) received a lot of data in the same period of time.

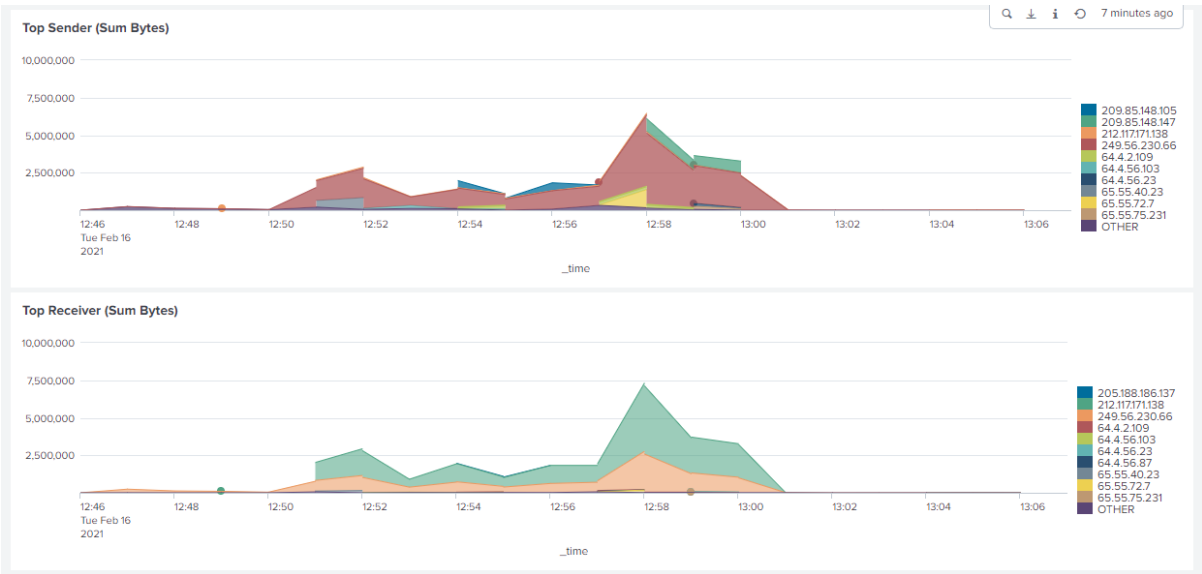


Figure 2.5: Top Sender and Receiver

The figure 2.6 shows that the port 65500 were used the most in the same period of time above.

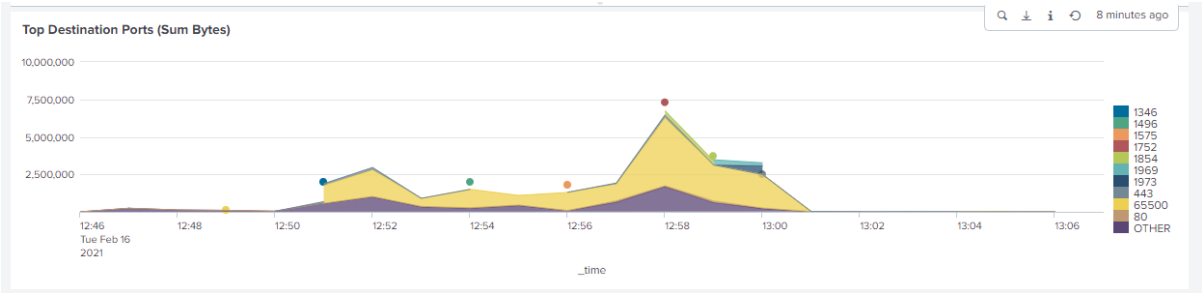


Figure 2.6: Top Destination Port

3. **Summary of detected attack**

   In short, 3 types of attacks were discovered in the dataset: SPAM, Port Scan (TCP SYN) and HTTP. The host (249.56.230.66) accessed to malicious websites: "my.shopandbuy.com" (94.63.149.152) and "chiashop.net" (195.88.191.59). The host and these websites communicated from 12:47 to 12:49 and the host downloaded malwares with GET requests to perform attacks. The host then started to send a SPAM and Port Scan. The SPAM was performed to 110 emails from 12:54 to 13:01. Port Scan was performed mainly to the destination host (46.4.36.120) via destination port 443.

4. **Attacks**

   a. **SPAM**

      i. **Evidence**

      SMTP is a protocol commonly used for email transferring. By filtering with SMPT and RCPE, we can find the emails received as shown in figure 4.a.1 below, which results in 110 events.

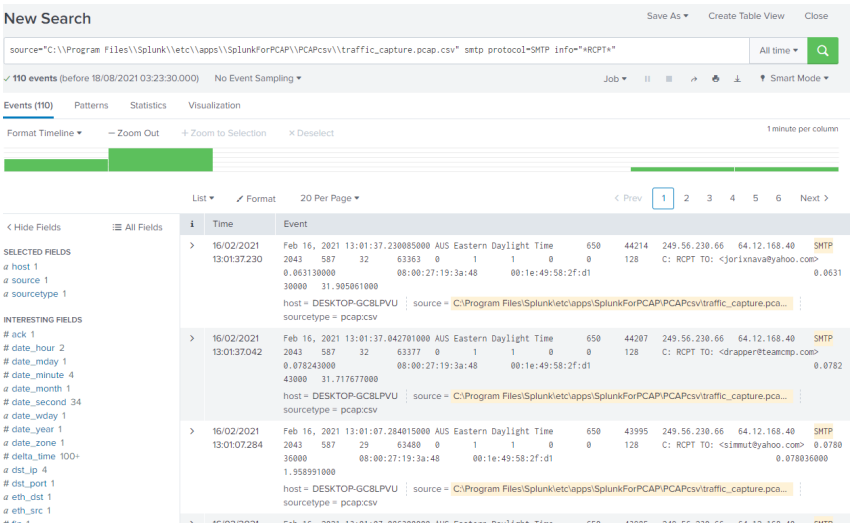


Figure 4.a.1: Emails in the dataset

From the figure 4.a.2, we can see that the emails have been sent by only one IP address (249.56.230.66) in the period between 12:54 to 13:01.

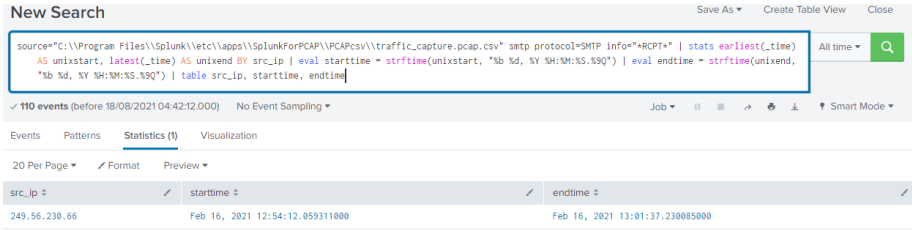


Figure 4.a.2: source IP of emails, start and end timestamp of it

Also, the figure 4.a.3 shows the list of email addresses that received emails from the source IP (249.56.230.66), which results in 110 targeted email addresses.

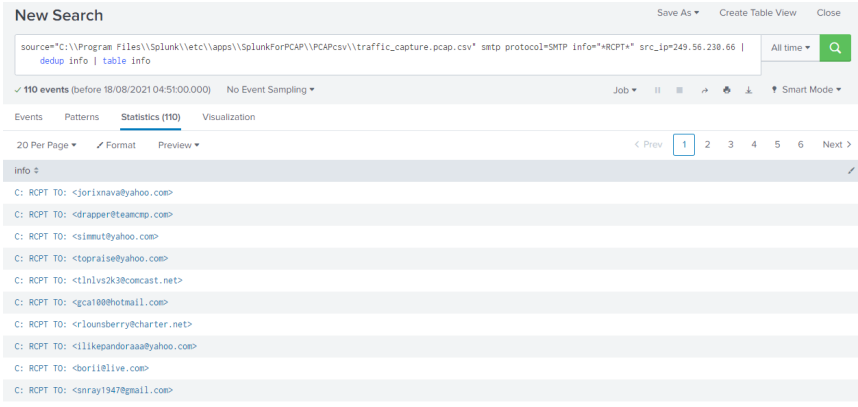


Figure 4.a.3: list of targeted email addresses

From the figure 4.a.4 and 4.a.5, we can see the first targeted email address (joecparkcity@aol.com) at 12:54 and the last targeted email address at 13:01 (jorixnava@yahoo.com).

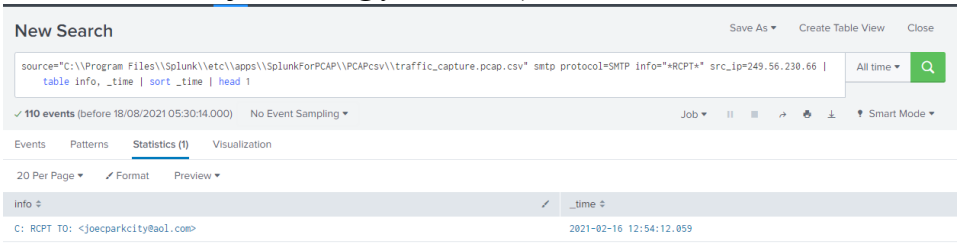


Figure 4.a.4: the first targeted email address

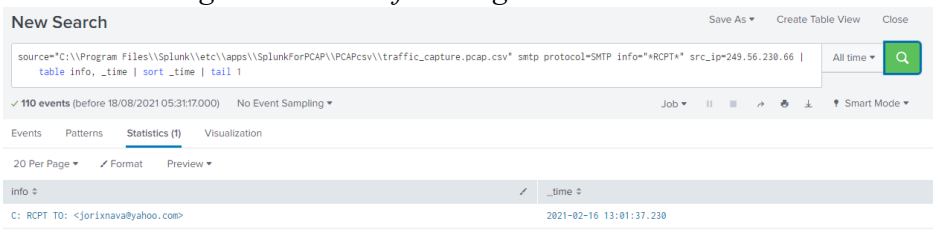


Figure 4.a.5: the last targeted email address

It can be observed from the figure 4.a.6 that the 4 destination IP addresses are targeted for SPAM by the source IP address.

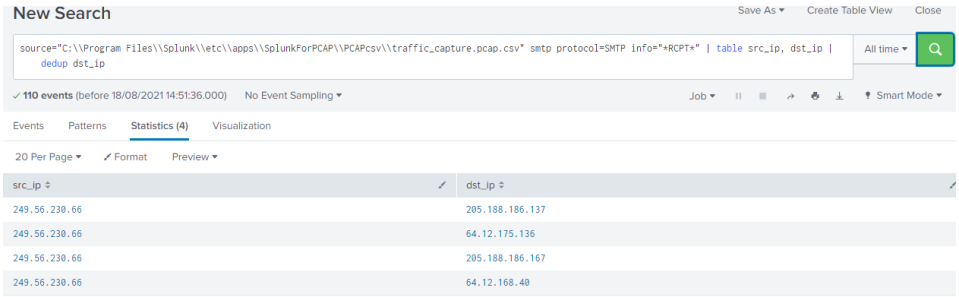


Figure 4.a.6: destination addresses targeted by SPAM

From the figure 4.a.7, these emails were sent only via the destination port 587.

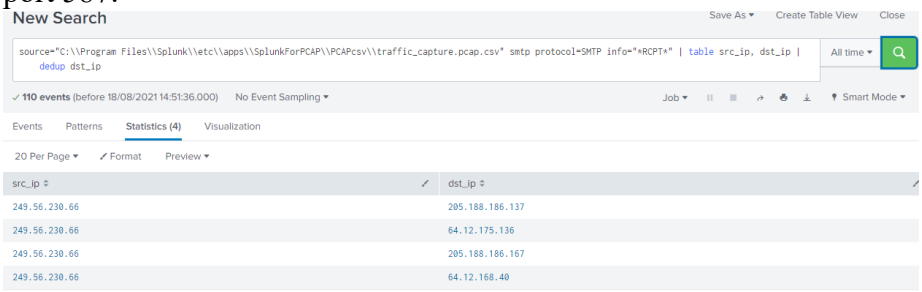


Figure 4.a.8: destination port used for email

From the figure 4.a.9, we can see the number of SPAMs sent per minute.

Figure 4.a.9: number of SPAMs sent per min

ii. Attack narrative

The host (249.56.230.66) sent SPAM to the email address corresponding to 4 destination IP addresses via port 587 using SMTP protocol.

Number of targeted email addresses: 110

Start time of this SPAM attack: Feb 16, 2021 12:54:12.059311000

End time of this SPAM attack: Feb 16, 2021 13:01:37.230085000

First recipient and time: joecparkcity@aol.com at 2021-02-16 12:54:12.059

Last recipient and time: jorixnava@yahoo.com at 2021-02-16 13:01:37.230

iii. How to extract features

src_ip + dst_port + protocol

We have seen that the SPAM was sent by one source IP (249.56.230.66) via one port (587) by SMTP protocol.

b. Port Scan

i. Evidence

TCP SYN scan is one of the most common port scanning techniques. As the host (249.56.230.66) has high traffic and identified as a suspicious host in the previous section (SPAM), we are going to analyse the activities of this host.

As can be seen from the figure 4.b.1, the host (249.56.230.66) sent many SYN packets, which results in 3,292 events. Also, we can find that the host (249.56.230.66) received many SYN ACK packets, which results in 409 events.

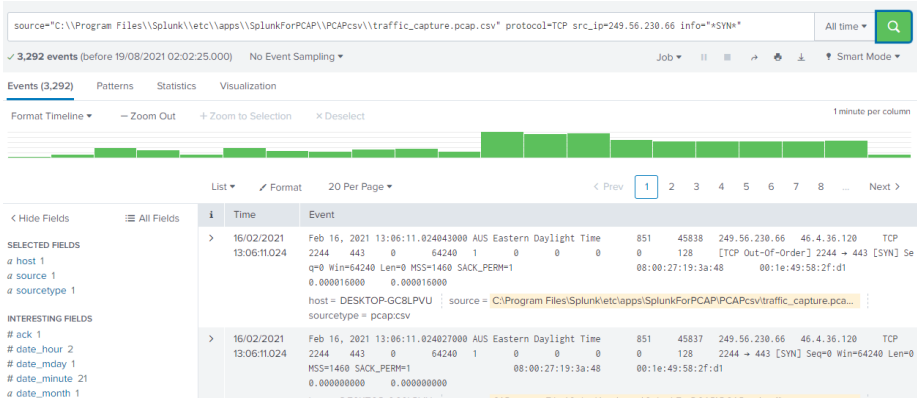


Figure 4.b.1: SYN packets

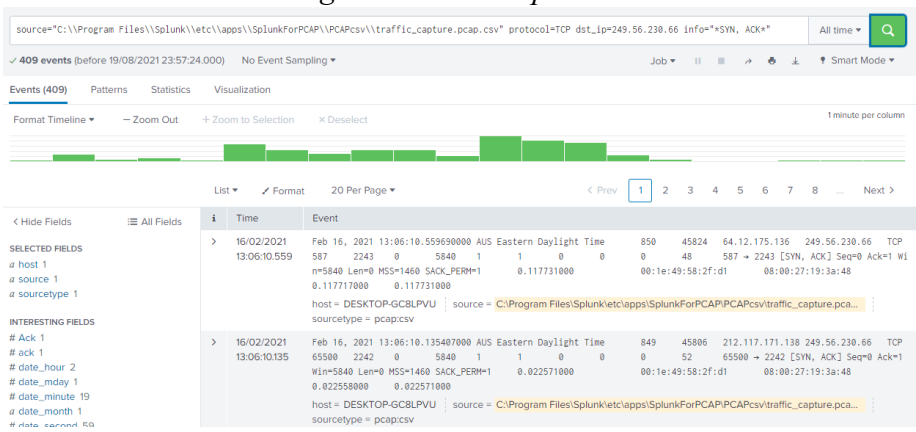


Figure 4.b.2: SYN ACK packets

The figure 4.b.3 shows the statistic of SYN packets sent by the host (249.56.230.66) each minute. We can see that the largest SYN packet size (94,804 bytes) was sent at 12:57. The figure 4.b.4 shows the statistic of SYN ACK packets received by the host (249.56.230.66) each minute. The figure 4.b.5 shows the statistics of RST ACK packets received by the host (249.56.230.66) each minute. Finally, the figure 4.b.6 shows the total packets sent and received by the host each minute.

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP src_ip=249.56.230.66 info="*SYN*" | eval bytes
    =len(_raw) | stats sum(bytes) BY date_hour, date_minute
```

All time

✓ **3,292 events** (before 19/08/2021 02:28:12.000) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (21)** Visualization

20 Per Page Format Preview

Prev 1 2 Next

date_hour	date_minute	sum(bytes)
12	46	1040
12	47	11530
12	48	35042
12	49	28250
12	50	10280
12	51	33841
12	52	23703

Figure 4.b.3: SYN packets sent by the host (249.56.230.66) each min

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP dst_ip=249.56.230.66 info="*SYN*" | eval
    bytes=len(_raw) | stats sum(bytes) BY date_hour, date_minute
```

All time

✓ **409 events** (before 20/08/2021 00:02:47.000) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (19)** Visualization

20 Per Page Format Preview

date_hour	date_minute	sum(bytes)
12	46	539
12	47	4958
12	48	1087
12	49	2440
12	50	813
12	51	12747
12	52	8314
12	53	5551
12	54	8061
12	55	8367
12	56	3897
12	57	18607
12	58	15839

Figure 4.b.4: SYN ACK received by the host (249.56.230.66) each min

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP dst_ip=249.56.230.66 info="*RST*" | eval bytes
    =len(_raw) | stats sum(bytes) BY date_hour, date_minute
```

All time

✓ **877 events** (before 22/08/2021 00:29:24.000) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (18)** Visualization

20 Per Page Format Preview

date_hour	date_minute	sum(bytes)
12	49	753
12	50	744
12	51	747
12	52	771
12	53	1500
12	54	756
12	55	753
12	56	2964
12	57	22793
12	58	20501
12	59	23242
13	0	21769

Figure 4.b.5: RST ACK received by host (249.56.230.66) each min

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP (dst_ip=249.56.230.66 OR src_ip=249.56.230.66
    ) info="*SYN*" | eval bytes=len(_raw) | stats sum(bytes) BY date_hour, date_minute
```

✓ 3,701 events (before 20/08/2021 00:06:00.000) No Event Sampling

Events Patterns Statistics (21) Visualization

20 Per Page Format Preview

date_hour	date_minute	sum(bytes)
12	46	1579
12	47	16488
12	48	36129
12	49	30690
12	50	11093
12	51	46588
12	52	32017
12	53	26655
12	54	36772
12	55	40887
12	56	26716
12	57	113411
12	58	102267
12	59	102280
13	0	68935

Figure 4.b.6: Total packets sent and received by the host (249.56.230.66) each min

From the figure 4.b.7, we can see the list of hosts that were communicated with the host (249.56.230.66), which results in 180 IP addresses. From the figure 4.b.8, we can know that the IP address (46.4.36.120) communicated with the host (249.56.230.66) the most.

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP src_ip=249.56.230.66 info="*SYN*" | table dst_ip
    | dedup dst_ip
```

✓ 3,292 events (before 19/08/2021 02:39:13.000) No Event Sampling

Events Patterns Statistics (180) Visualization

20 Per Page Format Preview

dst_ip
65.55.75.231
46.4.36.120
212.117.171.138
92.47.5.149
74.125.39.27
64.4.56.23
61.17.216.4
64.4.2.109
209.85.148.147
59.94.194.59
221.130.69.202
74.125.93.27

Figure 4.b.7: list of hosts scanned

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP src_ip=249.56.230.66 SYN | chart count by
    dst_ip | sort - count
```

✓ 3,292 events (before 19/08/2021 03:00:34.000) No Event Sampling

Events Patterns Statistics (180) Visualization

20 Per Page Format Preview

dst_ip	count
46.4.36.120	1646
212.117.171.138	362
91.220.0.52	52
60.190.223.75	42

Figure 4.b.8: list of hosts scanned with count

Also, it is observed that the SYN packet was started to send out from 12:46 and ended at 13:06 from the figure 4.b.9. Also, as we can see from the figure 4.b.10 and 4.b.11, The first SYN packet was sent to the targeted IP address “74.125.232.195” at 12:46, and the last SYN packet was sent to the targeted IP address “46.4.36.120” at 13:06.

Figure 4.b.9: SYN packet start time and end time

Figure 4.b.10: First SYN packet target and time

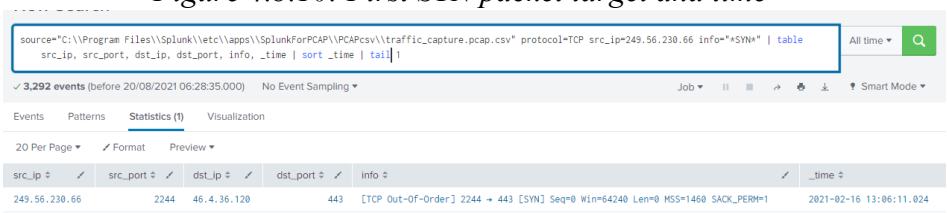


Figure 4.b.11: Last SYN packet target and time

The figure 4.b.12 shows Ip addresses and port number of source and destination of SYN packet traffic sent by the host (249.56.230.66). As can be seen from the figures 4.b.12 and 4.b.13, the host (249.56.230.66) sent SYN packets with different source ports (from 1027 to 1521) in increasing order along with timestamp. For reply to those SYN packets, the hosts who received SYN packets sent back the SYN ACK packets with a source port as the destination port of SYN packets.

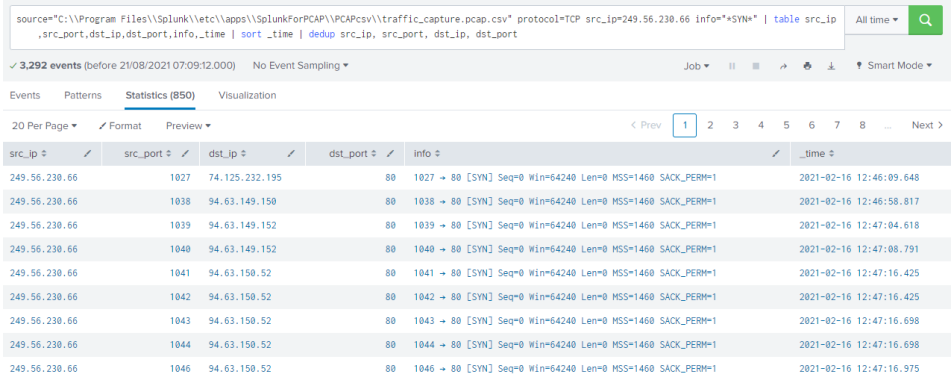


Figure 4.b.12: SYN packet traffic (src and dst) IPs and ports

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP (src_ip=249.56.230.66 OR dst_ip=249.56.230.66)
    info="*SYN*" | table src_ip,src_port,dst_ip,dst_port,info,_time | sort _time | dedup src_ip, src_port, dst_ip, dst_port
```

All time

✓ 3,701 events (before 21/08/2021 07:11:36.000) No Event Sampling — Job — Smart Mode

Events | Patterns | Statistics (1,259) | Visualization

20 Per Page — Format — Preview — Prev 1 2 3 4 5 6 7 8 ... Next

src_ip	src_port	dst_ip	dst_port	info	_time
249.56.230.66	1027	74.125.232.195	80	1027 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:46:09.648
74.125.232.195	80	249.56.230.66	1027	80 → 1027 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1	2021-02-16 12:46:09.656
249.56.230.66	1038	94.63.149.150	80	1038 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:46:58.817
94.63.149.150	80	249.56.230.66	1038	80 → 1038 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:46:58.852
249.56.230.66	1039	94.63.149.152	80	1039 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:47:04.618
94.63.149.152	80	249.56.230.66	1039	80 → 1039 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:47:04.653
249.56.230.66	1040	94.63.149.152	80	1040 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:47:08.791
94.63.149.152	80	249.56.230.66	1040	80 → 1040 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:47:08.826
249.56.230.66	1041	94.63.150.52	80	1041 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	2021-02-16 12:47:16.425

Figure 4.b.13: SYN and SYN ACK packet traffic (src and dst) Ips and ports

From the figure 4.b.14, we can see that port 443 was targeted the most. Also, we can know that it was mainly targeted to 46.4.36.120 with port 443.

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP src_ip=249.56.230.66 info="*SYN*" | chart count
    by dst_port | sort -count
```

All time

✓ 3,292 events (before 22/08/2021 00:37:54.000) No Event Sampling — Job — Smart Mode

Events | Patterns | Statistics (10) | Visualization

20 Per Page — Format — Preview —

dst_port	count
443	1792
6667	478
65500	362
80	290
3128	178
25	110
587	38
88	36
2012	6
139	2

Figure 4.b.14: count the destination port of the SYN packets

```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" protocol=TCP src_ip=249.56.230.66 info="*SYN*" dst_port=443
    | chart count by dst_ip
```

All time

✓ 1,792 events (before 22/08/2021 00:39:44.000) No Event Sampling — Job — Smart Mode

Events | Patterns | Statistics (17) | Visualization

20 Per Page — Format — Preview —

dst_ip	count
46.4.36.120	1646
65.54.165.169	2
65.54.165.179	2
65.54.186.10	26
65.54.186.19	2
65.54.186.47	6
65.54.186.107	2
65.54.234.24	6
65.54.234.78	10

Figure 4.b.15: count the destination IP addresses in port 443 of the SYN packets

ii. Attack narrative

The source host (249.56.230.66) sent SYN packets to multiple IP addresses with increasing source port number (1027 to 1521) by TCP protocol for Port Scan. The packets were sent out from the source host from 12:45 to 13:06. For replies of the SYN packets, the destination hosts sent back SYN ACK packets to the source host with the destination port that is the source port of SYN packets. The IP address (46.4.36.120) was targeted the most via port 443 in this Port Scan. The total number of the SYN packets sent by the source host is 3,292 and

the number of the SYN ACK packets received by the source host is 409 events. The peak amount of SYN packets by a minute was 94,804 bytes, which was sent at12:57.
The number of targeted hosts: 180
The first IP address targeted: 74.125.232.195 at 12:46
The last IP address targeted: 46.4.36.120 at 13:06
Start and end time of SYN packets: 12:45 to 13:06
Most targeted IP addresses and destination Port: 46.4.36.120, port 443

iii. **How to extract features**

src_ip + src_port + protocol

There were many SYN packets sent by the source IP address (249.56.230.66) to many IP addresses via TCP protocol. The SYN packets were sent with multiple source ports (1027 to 1521), in order to receive SYN ACK packets.

c. **HTTP**

i. **Evidence**

Now we are going to look at the activities of suspicious website ("my.shopandbuy.com" and "chiashop.net") in details.

From the figure 4.c.1, we can see 3 events corresponding to "my.shopandbuy.com". It asks DNS server to resolve domain name to IP address.

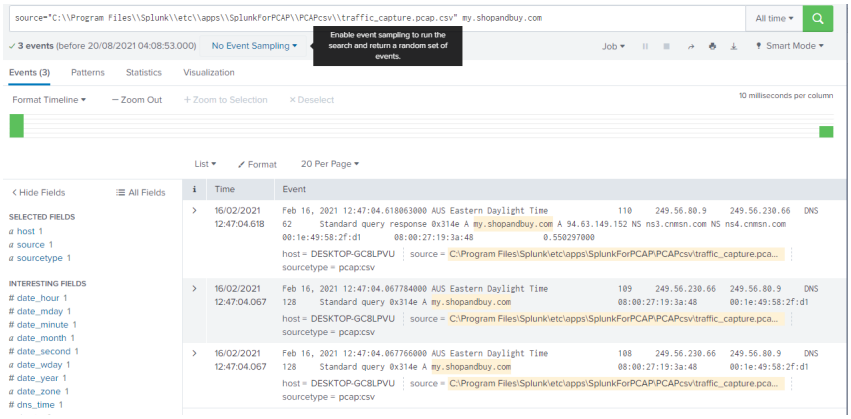


Figure 4.c.1: events corresponding to "my.shopandbuy.com"

From the figure 4.c.2, we can know the information sent between the DNS server and the host (249.56.230.66), that is identified as a suspicious IP address in previous sections. The IP address of "my.shopandbuy.com" is 94.63.149.152.

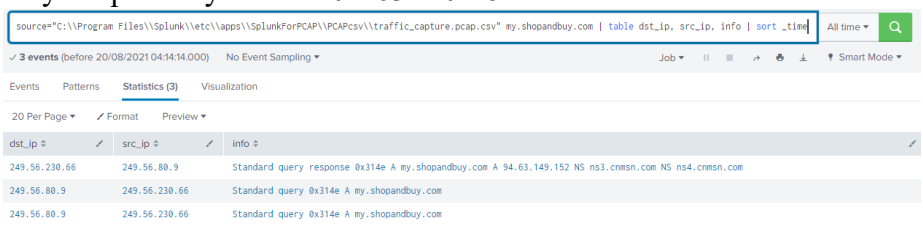


Figure 4.c.2: information sent between DNS server and the host

From the figure 4.c.3 and 4.c.4, we can see that the host (249.56.230.66) created 2 GET requests to "my.shopandbuy.com".

Also, we can see two URIs that might be related to the malware: “GET /rus.php HTTP/1.0” and “GET /gc.exe HTTP/1.0”, which both were requested around 12:47.

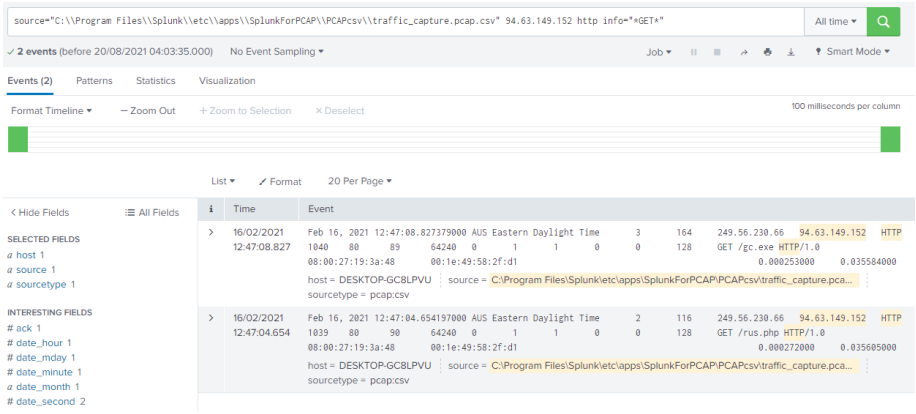


Figure 4.c.3: HTTP GET requests from the host (249.56.230.66)to “my.shopandbuy.com”

Figure 4.c.4: the information of HTTP GET requests from the host (249.56.230.66)to “my.shopandbuy.com”

We can do the same things to “chiashop.net”. Firstly, we search for the IP address of “chiashop.net”. As we can see from the figure 4.c.5, the IP address is “195.88.191.59”.

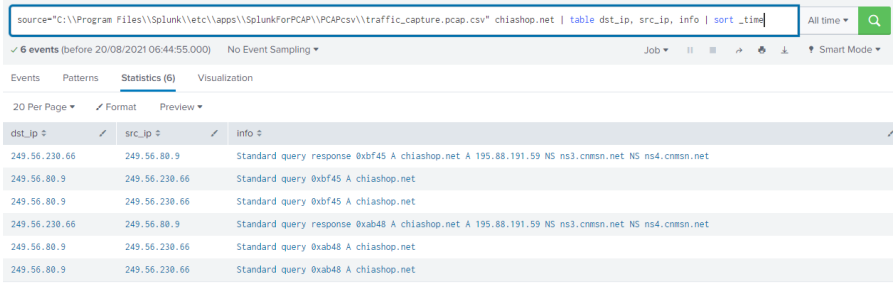
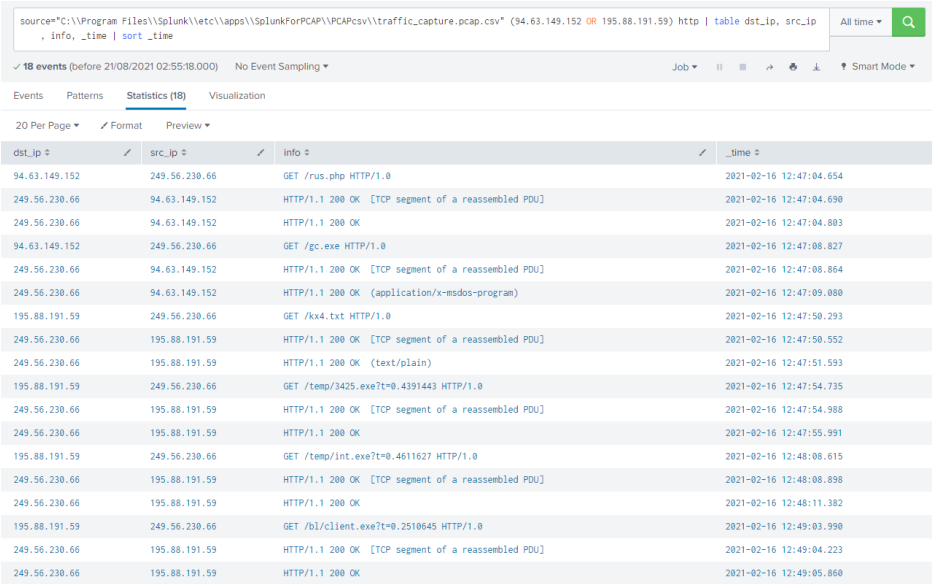


Figure 4.c.5: the information of the conversation between the DNS server and the host

The figure 4.c.6 shows few URIs that might related to malware: “GET /temp/int.exe?t=0.4611627 HTTP/1.0”, “GET /temp/3425.exe?t=0.4391443 HTTP/1.0”, “GET /kx4.txt HTTP/1.0”, “GET /bl/client.exe?t=0.2510645 HTTP/1.0”, which were requested from 12:47 to 12:49.

Figure 4.c.6: the information of HTTP GET requests from the host (249.56.230.66)to "chiashop.net"

The figure 4.c.7 shows all the conversations between the host and 2 malicious websites. The conversations started from "my.shopandbuy.com" at 12:47:04 and once "application/x-msdos-program" was happened, the host started conversation to "chiashop.net" at 12:47:50.



```
source="C:\\Program Files\\Splunk\\etc\\apps\\SplunkForPCAP\\PCAPcsv\\traffic_capture.pcap.csv" (94.63.149.152 OR 195.88.191.59) http | table dst_ip, src_ip
    , info, _time | sort _time
```

All time

✓ 18 events (before 21/08/2021 02:55:18.000) No Event Sampling Job Smart Mode

Events Patterns Statistics (18) Visualization

20 Per Page Format Preview

dst_ip	src_ip	info	_time
94.63.149.152	249.56.230.66	GET /rus.php HTTP/1.0	2021-02-16 12:47:04.654
249.56.230.66	94.63.149.152	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	2021-02-16 12:47:04.690
249.56.230.66	94.63.149.152	HTTP/1.1 200 OK	2021-02-16 12:47:04.803
94.63.149.152	249.56.230.66	GET /gc.exe HTTP/1.0	2021-02-16 12:47:08.827
249.56.230.66	94.63.149.152	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	2021-02-16 12:47:08.864
249.56.230.66	94.63.149.152	HTTP/1.1 200 OK (application/x-msdos-program)	2021-02-16 12:47:09.080
195.88.191.59	249.56.230.66	GET /kx4.txt HTTP/1.0	2021-02-16 12:47:50.293
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	2021-02-16 12:47:50.552
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK (text/plain)	2021-02-16 12:47:51.593
195.88.191.59	249.56.230.66	GET /temp/3425.exe?t=0.4391443 HTTP/1.0	2021-02-16 12:47:54.735
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	2021-02-16 12:47:54.988
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK	2021-02-16 12:47:55.991
195.88.191.59	249.56.230.66	GET /temp/int.exe?t=0.4611627 HTTP/1.0	2021-02-16 12:48:08.615
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	2021-02-16 12:48:08.898
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK	2021-02-16 12:48:11.382
195.88.191.59	249.56.230.66	GET /bl/client.exe?t=0.2510645 HTTP/1.0	2021-02-16 12:49:03.990
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]	2021-02-16 12:49:04.223
249.56.230.66	195.88.191.59	HTTP/1.1 200 OK	2021-02-16 12:49:05.860

Figure 4.c.7: whole conversations between the host and 2 malicious websites with timestamp

ii. Attack narrative

The host (249.56.230.66) had access histories to two malicious websites: "my.shopandbuy.com" and "chiashop.net" via HTTP protocol and downloaded some files that might related to malwares. The host first started conversation with "my.shopandbuy.com" at 12:47:04 and made two GET requests to "/rus.php" and "/gc.exe" in order. One conversation at 12:47:09 shows "application/x-msdos-program" that denotes the presence of MS DOS application and executable files [1]. After that, the host started conversation with "chiashop.net" at 12:47:50 and made 4 GET requests to "/kx4.txt", "/temp/3425.exe?t=0.4391443", "/temp/int.exe?t=0.4611627", "/bl/client.exe?t=0.2510645".

URI:
"my.shopandbuy.com": /rus.php, /gc.exe
"chiashop.net": /kx4.txt, /temp/3425.exe?t=0.4391443, /temp/int.exe?t=0.4611627, /bl/client.exe?t=0.2510645

Considering the fact that the host (249.56.230.66) got infected by the malware from 12:47 to 12:49, the SPAM and Port Scan might be occurred because of malware after the infection.

iii. How to extract features

src_ip + protocol

The source IP accessing malicious websites via HTTP protocol. It might also be worth to see if the GET requests are made to download executable files and URIs.

5. **Consequences of Attacks**

   SPAM: When a massive amount of SPAM is sent to the targeted server, it consumes the server's resources and bandwidth. Then it may bring down the server and no one would be able to access to the service. Thus, it would affect the availability. Also, the spam emails might contain malwares which delete/modify or leak sensitive information of the user or server, that affect the confidentiality and integrity.

   Port Scan: The infected host could send a massive amount of SYN packets and bring down the server, which cause Denial of Service, that affect availability. Also, once an attacker found the opened port and they exploit the vulnerability to get file access, it would affect the confidentiality.

   HTTP: When an attacker downloads the Malware from the malicious websites, the malware could delete/modify the sensitive files on the host machine, change the privilege of user, open access remotely. This could cause confidentiality and integrity issues.

6. **Countermeasure**

   SPAM: the SPAM is sent by specific source IPs via specific ports by SMTP protocol. Thus, monitor the network traffic and once found the large volume of emails and this patter, we can detect this. We can then filter the source IPs with its port and check the contents if there is weird strings, URLs, or files.

   Port Scan (TCP SYN scan): when there is a large volume of SYN packets sent by specific source IP address to many IP addresses via TCP protocol, we can detect there might be port scan happening. We can then filter the source IP and check the destination/source ports to verify this attack.

   HTTP: when there is GET request via HTTP protocol and the file contains executable and suspicious string, we may be able to detect this. We can then filter the source IP that downloaded the malwares and the accessed suspicious websites.

7. **Conclusion**

   We have discovered 3 types of attacks by analysing the dataset: SPAM, Port Scan, and HTTP. Once the host (249.56.230.66) has been infected by the malware from "my.shopandbuy.com" and "chiashop.net", the host started SPAM and Port Scan attacks. The patterns to detect the attacks were also found based on the analysis. The SPAM is sent by specific source IP addresses via specific ports by SMTP protocol. Port Scan is to sends SYN packets by a specific source IP address via TCP protocol. HTTP attack contains GET request to malicious files via HTTP protocol. Finally, countermeasures to each attack were given in this report to detect and mitigate the attack based on these patterns.

8. **Reference**

[1] https://mimeapplication.net/x-msdos-program