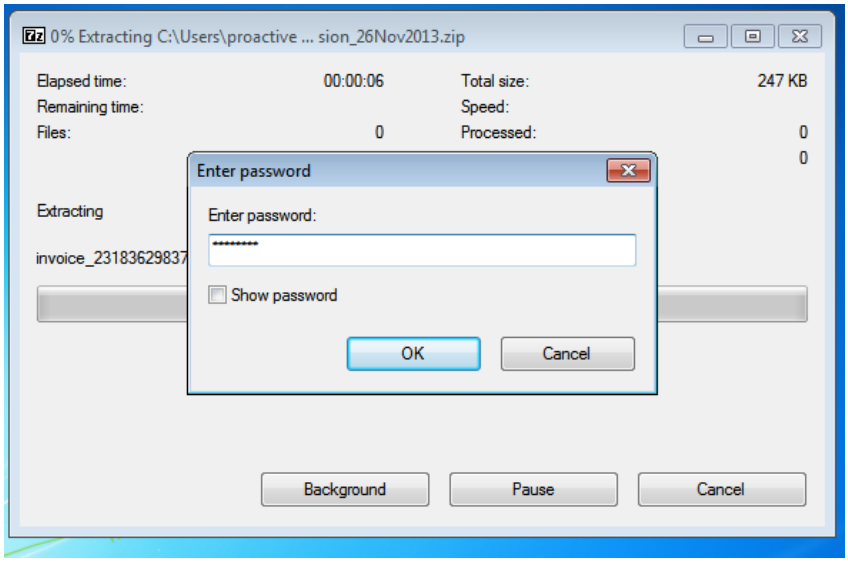
Proactive Final Project Walkthrough

1. Malware Execution

1.1 Password protected Extraction

This step prepares the malicious file (Zeus Trojan) for execution in a controlled environment, such as a VMware (Windows 7).

The extracted file will then be executed to simulate the malware's behavior and activity.

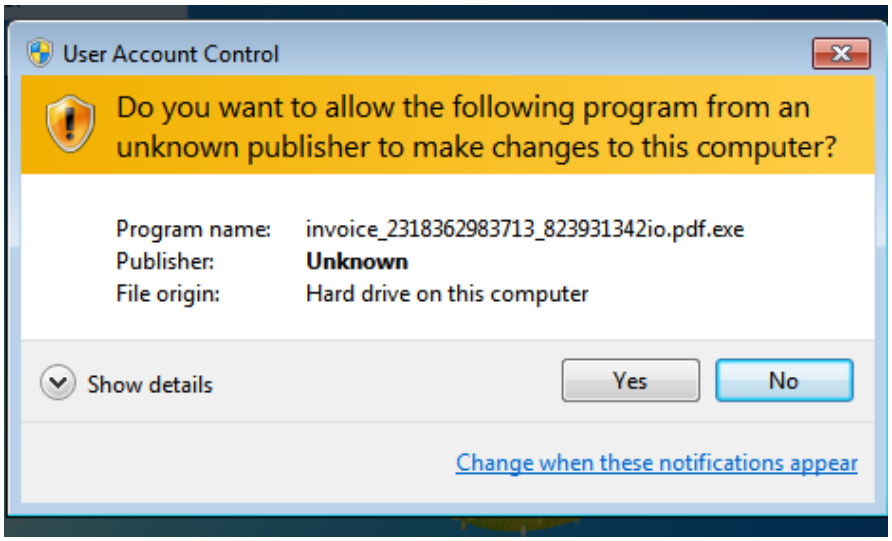


1.2 Elevating Privileges via UAC Prompt

This malware requests administrative privileges to gain elevated permissions that enables the malware to:

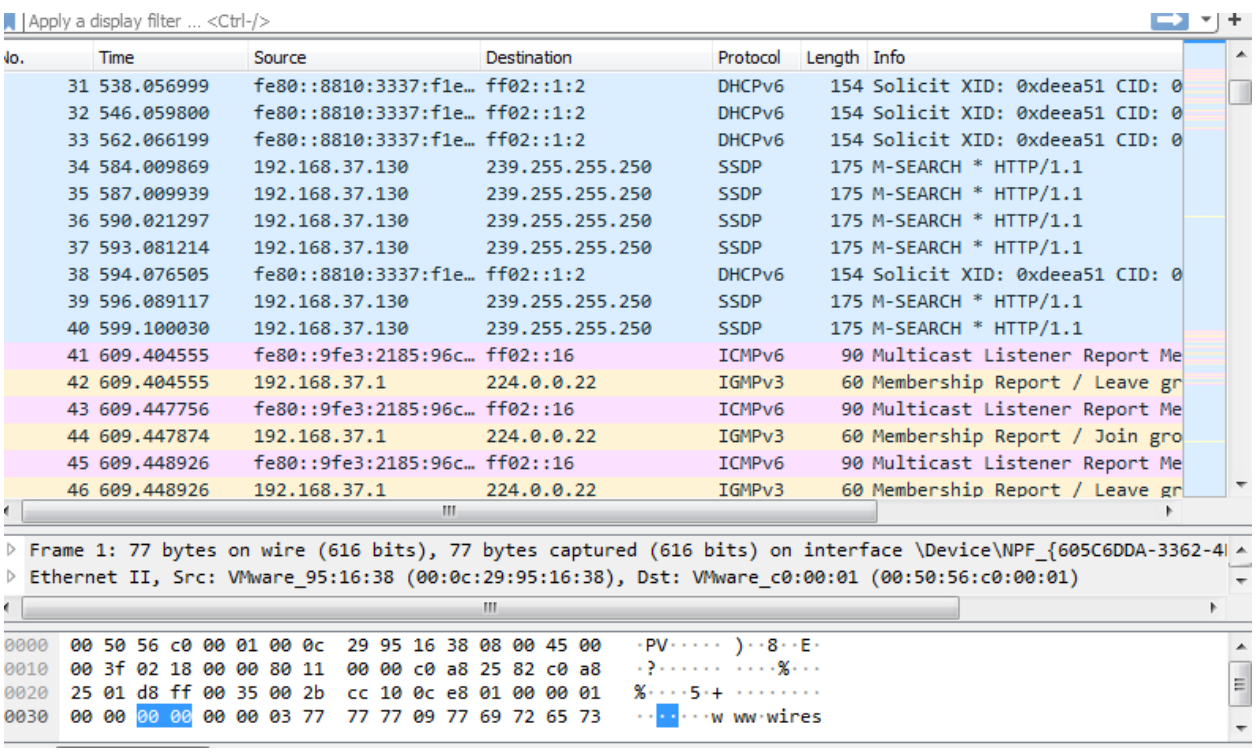
- Install itself deeply into the system.
- Access sensitive data.
- Perform actions that are otherwise restricted for regular users.

The UAC prompt shows the program's **unknown** publisher, indicating it is not from a trusted source. Allowing the prompt would trigger the malware's infection process.



1.3 Network Traffic Analysis in Wireshark

This analysis is crucial for detecting Zeus Trojan's network behavior, such as Command-and-Control (C2) communication. By identifying anomalies or specific patterns (e.g., unexpected multicast traffic or abnormal IPs), the analyst can detect and confirm malicious activity.

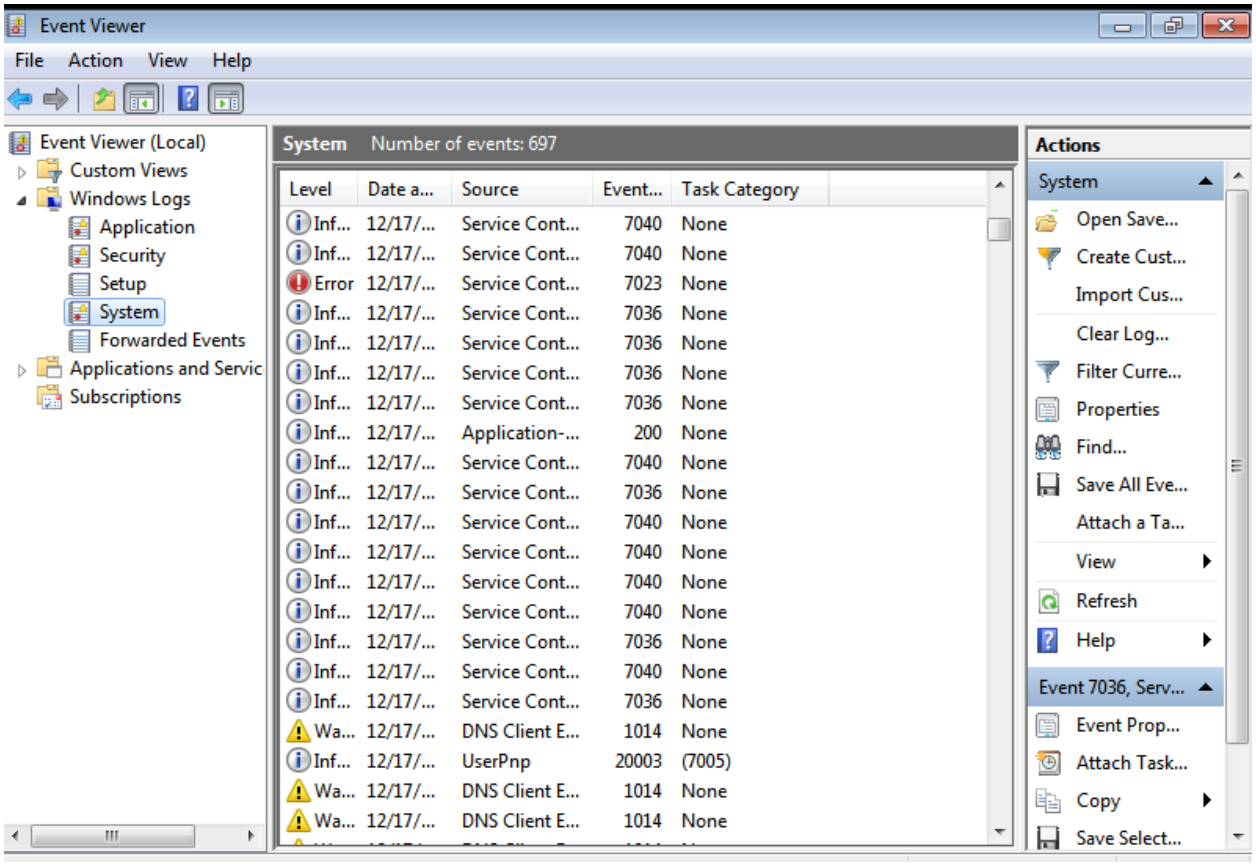


No.	Time	Source	Destination	Protocol	Length	Info
31	538.056999	fe80::8810:3337:f1e…	ff02::1:2	DHCPv6	154	Solicit XID: 0xdeea51 CID: 0
32	546.059800	fe80::8810:3337:f1e…	ff02::1:2	DHCPv6	154	Solicit XID: 0xdeea51 CID: 0
33	562.066199	fe80::8810:3337:f1e…	ff02::1:2	DHCPv6	154	Solicit XID: 0xdeea51 CID: 0
34	584.009869	192.168.37.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
35	587.009939	192.168.37.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
36	590.021297	192.168.37.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
37	593.081214	192.168.37.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
38	594.076505	fe80::8810:3337:f1e…	ff02::1:2	DHCPv6	154	Solicit XID: 0xdeea51 CID: 0
39	596.089117	192.168.37.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
40	599.100030	192.168.37.130	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
41	609.404555	fe80::9fe3:2185:96c…	ff02::16	ICMPv6	90	Multicast Listener Report Me
42	609.404555	192.168.37.1	224.0.0.22	IGMPv3	60	Membership Report / Leave gr
43	609.447756	fe80::9fe3:2185:96c…	ff02::16	ICMPv6	90	Multicast Listener Report Me
44	609.447874	192.168.37.1	224.0.0.22	IGMPv3	60	Membership Report / Join gro
45	609.448926	fe80::9fe3:2185:96c…	ff02::16	ICMPv6	90	Multicast Listener Report Me
46	609.448926	192.168.37.1	224.0.0.22	IGMPv3	60	Membership Report / Leave gr

1.4 Event Viewer Logs

The Windows Event Viewer, which logs system-level events such as service activity, warnings, and errors.

By reviewing these logs, analysts can identify suspicious system changes, abnormal errors, or patterns correlating with known Zeus Trojan activity. For instance, sudden DNS client errors might indicate malicious attempts to resolve or communicate with suspicious domains.



2. Suricata

2.1 Default Suricata Configuration

This command allows us to modify Suricata's configuration, to ensure Suricata can effectively analyze network traffic and apply the correct detection rules for identifying threats such as the Zeus Trojan.

```
┌──(menna㉿kali)-[~]
└─$ sudo nano /etc/suricata/suricata.yaml
[sudo] password for menna:
```

This configuration ensures that Suricata is set up to load and apply default rules for traffic analysis.

```
  GNU nano 7.2                                        /etc/suricata/suricata.yaml *
    ports: [0-1,2-3]

    # When auto-config is enabled the hashmode specifies the algorithm for
    # determining to which stream a given packet is to be delivered.
    # This can be any valid Napatech NTPL hashmode command.
    #
    # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
    # hash5tuple, hash5tuplesorted and roundrobin.
    #
    # See Napatech NTPL documentation other hashmodes and details on their use.
    #
    # This parameter has no effect if auto-config is disabled.
    #
    hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules

##
## Auxiliary configuration files.
```

2.2 Running Suricata with PCAP File

Suricata is used to analyze the network traffic stored in the PCAP file, searching for suspicious patterns or behavior matching its detection rules.

This step allows analysis of previously captured network traffic. The **Zeus PCAP file** likely contains malicious traffic patterns, and Suricata's output will reveal indicators of compromise (e.g., suspicious IP addresses, protocols, or payloads).

```
┌──(menna㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -r /home/menna/Downloads/zeus.pcapng -l /home/menna/Downloads/Project
i: suricata: This is Suricata version 7.0.7 RELEASE running in USER mode
i: threads: Threads created → RX: 1 W: 2 FM: 1 FR: 1   Engine started.
i: suricata: Signal Received.  Stopping engine.
i: pcap: read 1 file, 1015 packets, 215685 bytes
```

Alerts of the default rules: ***268***

```
~/Downloads/Project/suricata.log [Read Only] - Mousepad
File  Edit  Search  View  Document  Help
1 [4025 - Suricata-Main] 2024-12-17 21:02:04 Notice: suricata: This is Suricata version 7.0.7 RELEASE running in USER mode
2 [4025 - Suricata-Main] 2024-12-17 21:02:04 Info: cpu: CPUs/cores online: 2
3 [4025 - Suricata-Main] 2024-12-17 21:02:04 Info: suricata: Setting engine mode to IDS mode by default
4 [4025 - Suricata-Main] 2024-12-17 21:02:04 Info: exception-policy: master exception-policy set to: auto
5 [4025 - Suricata-Main] 2024-12-17 21:02:04 Info: logopenfile: fast output device (regular) initialized: fast.log
6 [4025 - Suricata-Main] 2024-12-17 21:02:04 Info: logopenfile: eve-log output device (regular) initialized: eve.json
7 [4025 - Suricata-Main] 2024-12-17 21:02:04 Info: logopenfile: stats output device (regular) initialized: stats.log
8 [4025 - Suricata-Main] 2024-12-17 21:02:13 Info: detect: 1 rule files processed. 41022 rules successfully loaded, 0 rules failed, 0
9 [4025 - Suricata-Main] 2024-12-17 21:02:13 Info: threshold-config: Threshold config parsed: 0 rule(s) found
10 [4025 - Suricata-Main] 2024-12-17 21:02:13 Info: detect: 41025 signatures processed. 1179 are IP-only rules, 4283 are inspecting packet
   payload, 35354 inspect application layer, 108 are decoder event only
11 [4025 - Suricata-Main] 2024-12-17 21:02:22 Info: unix-manager: unix socket '/var/run/suricata-command.socket'
12 [4164 - RX#01] 2024-12-17 21:02:22 Info: pcap: Starting file run for /home/menna/Downloads/zeus.pcapng
13 [4164 - RX#01] 2024-12-17 21:02:22 Info: checksum: No packets with invalid checksum, assuming checksum offloading is NOT used
14 [4164 - RX#01] 2024-12-17 21:02:22 Info: pcap: pcap file /home/menna/Downloads/zeus.pcapng end of file reached (pcap err code 0)
15 [4025 - Suricata-Main] 2024-12-17 21:02:22 Notice: threads: Threads created → RX: 1 W: 2 FM: 1 FR: 1   Engine started.
16 [4025 - Suricata-Main] 2024-12-17 21:02:22 Notice: suricata: Signal Received.  Stopping engine.
17 [4025 - Suricata-Main] 2024-12-17 21:02:22 Info: suricata: time elapsed 0.049s
18 [4164 - RX#01] 2024-12-17 21:02:22 Notice: pcap: read 1 file, 1015 packets, 215685 bytes
19 [4025 - Suricata-Main] 2024-12-17 21:02:22 Info: counters: Alerts: 268
20
```

2.3 Zeus Trojan Rules

The displayed rules are tailored to detect multiple aspects of the Zeus Trojan's behavior in network traffic. By targeting Zeus's unique indicators—such as specific URLs, domains, and payload patterns—these rules provide a robust mechanism for identifying Zeus-related threats in real-time.

```
menna@kali: ~
File  Actions  Edit  View  Help
GNU nano 7.2                                                    /var/lib/suricata/rules/zeus.rules
alert http any any → any any (msg:"Zeus Trojan C2 HTTP Traffic"; content:"/gate.php"; http_uri; fast_pattern; nocase; sid:1000001; rev:1;)
alert http any any → any any (msg:"Zeus Trojan C2 User-Agent"; content:"User-Agent|3A| Mozilla/4.0 (compatible|3B| MSIE 7.0|3B| Windows NT 6.0)"; http_header; fast_pattern; sid:1000002;
alert http any any → any any (msg:"Zeus Trojan binary download"; content:"application/octet-stream"; http_header; content:"exe"; http_uri; fast_pattern; sid:1000003; rev:1;)
alert dns any any → any any (msg:"Zeus Trojan C2 Domain Lookup"; dns_query; content:"badzeusdomain.com"; nocase; sid:1000004; rev:1;)
alert ip any any → 192.0.2.1 any (msg:"Zeus Trojan C2 IP Communication"; sid:1000005; rev:1;)
alert ip any any → 203.0.113.1 any (msg:"Zeus Trojan C2 IP Communication"; sid:1000006; rev:1;)
alert tcp any any → any any (msg:"Zeus Trojan SSL Certificate Detection"; tls_cert_subject; content:"CN=badzeus"; sid:1000010; rev:1;)
alert dns any any → any any (msg:"Zeus Trojan DGA-generated Domain"; content:"."; pcre:"/^[a-z0-9]{12,20}\.com$/"; sid:1000008; rev:1;)
alert http any any → any any (msg:"Zeus C2 HTTP Detected"; http.uri; content:"/gate.php"; nocase; sid:100001; rev:1;)
alert dns any any → any any (msg:"Zeus Domain Query Detected"; dns.query; content:"malicious-domain.com"; sid:100002; rev:1;)
alert tcp any any → any any (msg:"Zeus C2 Traffic Detected"; content:"botnet"; nocase; sid:100003; rev:1;)
alert udp any any → any any (msg:"UDP Packet Detected"; sid:100004; rev:1;)
alert dns any any → any any (msg:"Zeus DNS Query Detected"; content:"zeus"; nocase; sid:200001; rev:1;)
alert dns any any → any any (msg:"Dynamic DNS Query Detected (Potential Zeus)"; content:".dyndns.org"; nocase; sid:200002; rev:1;)
alert dns any any → any any (msg:"Suspicious Domain Query (Potential Zeus)"; dns.query; content:"malware"; nocase; sid:200003; rev:1;)
alert udp any any → 239.255.255.250 1900 (msg:"Zeus SSDP Discovery Traffic Detected"; content:"M-SEARCH"; sid:200004; rev:1;)
alert udp any any → 224.0.0.251 any (msg:"Zeus MDNS Traffic Detected"; content:"_tcp.local"; nocase; sid:200005; rev:1;)
alert udp any any → 224.0.0.252 5355 (msg:"Zeus LLMNR Traffic Detected"; content:"Noureldeen"; sid:200006; rev:1;)
alert udp any any → any 547 (msg:"Zeus DHCPv6 Traffic Detected"; content:"REQUEST"; sid:200007; rev:1;)
alert http any any → any any (msg:"Zeus C2 HTTP Detected"; http.uri; content:"/gate.php"; nocase; sid:200009; rev:1;)
alert tcp any any → any any (msg:"Zeus C2 Traffic Detected"; content:"botnet"; nocase; sid:200010; rev:1;)
alert udp any any → any 53 (msg:"Zeus C2 Domain Query"; content:"zeus-c2.com"; nocase; offset:12; fast_pattern:only; sid:200011; rev:1;)
```

2.4Running Suricata with Zeus Rules

This step ensures that the custom *zeus.rules* file is correctly placed in the rules directory for Suricata to load during analysis.

```
┌──(menna㉿kali)-[~]
└─$ ls /var/lib/suricata/rules/
classification.config  suricata.rules  zeus.rules
```

Suricata is executed with the *zeus.rules* file to analyze the provided PCAP file (zeus.pcapng) for malicious network activity.

```
┌──(menna㉿kali)-[~]
└─$ sudo suricata -S /var/lib/suricata/rules/zeus.rules -r /home/menna/Downloads/zeus.pcapng -l /home/menna/Downloads/Project
i: suricata: This is Suricata version 7.0.7 RELEASE running in USER mode
i: threads: Threads created → RX: 1 W: 2 FM: 1 FR: 1   Engine started.
i: suricata: Signal Received.  Stopping engine.
i: pcap: read 1 file, 1015 packets, 215685 bytes
```

The count of 388 alerts indicates that the PCAP file contains significant network activity matching the Zeus Trojan rules. This confirms potential Zeus-related traffic or malicious behavior.

```
[6806 - Suricata-Main] 2024-12-17 21:07:31 Notice: suricata: This is Suricata version 7.0.7 RELEASE running in USER mode
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: cpu: CPUs/cores online: 2
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: suricata: Setting engine mode to IDS mode by default
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: exception-policy: master exception-policy set to: auto
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: logopenfile: fast output device (regular) initialized: fast.log
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: logopenfile: eve-log output device (regular) initialized: eve.json
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: logopenfile: stats output device (regular) initialized: stats.log
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: detect: 1 rule files processed. 21 rules successfully loaded, 0 rules failed, 0
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: threshold-config: Threshold config parsed: 0 rule(s) found
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: detect: 21 signatures processed. 3 are IP-only rules, 9 are inspecting packet payload, 9
  inspect application layer, 0 are decoder event only
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: unix-manager: unix socket '/var/run/suricata-command.socket'
[6807 - RX#01] 2024-12-17 21:07:31 Info: pcap: Starting file run for /home/menna/Downloads/zeus.pcapng
[6807 - RX#01] 2024-12-17 21:07:31 Info: checksum: No packets with invalid checksum, assuming checksum offloading is NOT used
[6807 - RX#01] 2024-12-17 21:07:31 Info: pcap: pcap file /home/menna/Downloads/zeus.pcapng end of file reached (pcap err code 0)
[6806 - Suricata-Main] 2024-12-17 21:07:31 Notice: threads: Threads created → RX: 1 W: 2 FM: 1 FR: 1   Engine started.
[6806 - Suricata-Main] 2024-12-17 21:07:31 Notice: suricata: Signal Received.  Stopping engine.
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: suricata: time elapsed 0.030s
[6807 - RX#01] 2024-12-17 21:07:31 Notice: pcap: read 1 file, 1015 packets, 215685 bytes
[6806 - Suricata-Main] 2024-12-17 21:07:31 Info: counters: Alerts: 388
```

2.5 Default & Zeus Suricata Rules

This ensures Suricata loads both the default and custom rules for comprehensive traffic analysis. The hashmode setting is also included, which influences stream packet delivery algorithms.

```
GNU nano 7.2                                        /etc/suricata/suricata.yaml *
  ports: [0-1,2-3]

  # When auto-config is enabled the hashmode specifies the algorithm for
  # determining to which stream a given packet is to be delivered.
  # This can be any valid Napatech NTPL hashmode command.
  #
  # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
  # hash5tuple, hash5tuplesorted and roundrobin.
  #
  # See Napatech NTPL documentation other hashmodes and details on their use.
  #
  # This parameter has no effect if auto-config is disabled.
  #
  hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - zeus.rules
##
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
```

```
┌──(menna㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -r /home/menna/Downloads/zeus.pcapng -l /home/menna/Downloads/Project
i: suricata: This is Suricata version 7.0.7 RELEASE running in USER mode
i: threads: Threads created → RX: 1 W: 2 FM: 1 FR: 1   Engine started.
i: suricata: Signal Received.  Stopping engine.
i: pcap: read 1 file, 1015 packets, 215685 bytes
```

Alerts of the combined rules: ***656***

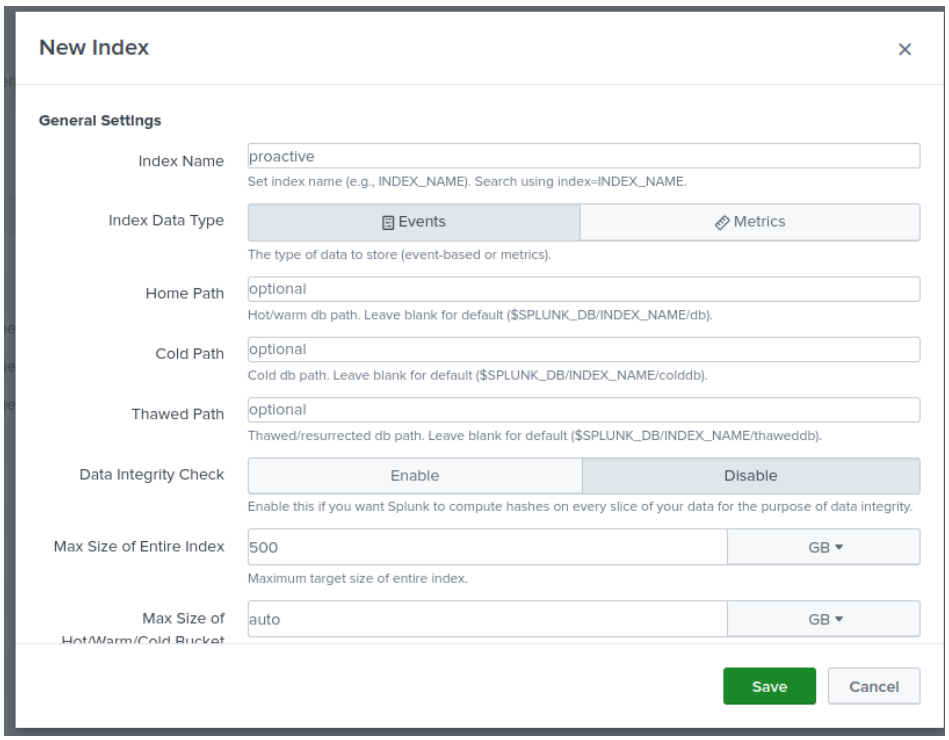
```
~/Downloads/Project/suricata.log [Read Only] - Mousepad
File  Edit  Search  View  Document  Help
1 [8492 - Suricata-Main] 2024-12-17 21:10:49 Notice: suricata: This is Suricata version 7.0.7 RELEASE running in USER mode
2 [8492 - Suricata-Main] 2024-12-17 21:10:49 Info: cpu: CPUs/cores online: 2
3 [8492 - Suricata-Main] 2024-12-17 21:10:49 Info: suricata: Setting engine mode to IDS mode by default
4 [8492 - Suricata-Main] 2024-12-17 21:10:49 Info: exception-policy: master exception-policy set to: auto
5 [8492 - Suricata-Main] 2024-12-17 21:10:49 Info: logopenfile: fast output device (regular) initialized: fast.log
6 [8492 - Suricata-Main] 2024-12-17 21:10:49 Info: logopenfile: eve-log output device (regular) initialized: eve.json
7 [8492 - Suricata-Main] 2024-12-17 21:10:49 Info: logopenfile: stats output device (regular) initialized: stats.log
8 [8492 - Suricata-Main] 2024-12-17 21:10:57 Info: detect: 2 rule files processed. 41043 rules successfully loaded, 0 rules failed, 0
9 [8492 - Suricata-Main] 2024-12-17 21:10:57 Info: threshold-config: Threshold config parsed: 0 rule(s) found
10 [8492 - Suricata-Main] 2024-12-17 21:10:57 Info: detect: 41046 signatures processed. 1182 are IP-only rules, 4292 are inspecting packet
  payload, 35363 inspect application layer, 108 are decoder event only
11 [8492 - Suricata-Main] 2024-12-17 21:11:05 Info: unix-manager: unix socket '/var/run/suricata-command.socket'
12 [8629 - RX#01] 2024-12-17 21:11:05 Info: pcap: Starting file run for /home/menna/Downloads/zeus.pcapng
13 [8629 - RX#01] 2024-12-17 21:11:05 Info: checksum: No packets with invalid checksum, assuming checksum offloading is NOT used
14 [8629 - RX#01] 2024-12-17 21:11:05 Info: pcap: pcap file /home/menna/Downloads/zeus.pcapng end of file reached (pcap err code 0)
15 [8492 - Suricata-Main] 2024-12-17 21:11:05 Notice: threads: Threads created → RX: 1 W: 2 FM: 1 FR: 1   Engine started.
16 [8492 - Suricata-Main] 2024-12-17 21:11:05 Notice: suricata: Signal Received.  Stopping engine.
17 [8492 - Suricata-Main] 2024-12-17 21:11:05 Info: suricata: time elapsed 0.123s
18 [8629 - RX#01] 2024-12-17 21:11:05 Notice: pcap: read 1 file, 1015 packets, 215685 bytes
19 [8492 - Suricata-Main] 2024-12-17 21:11:05 Info: counters: Alerts: 656
20
```

3. Splunk

3.1 Importing Files in Splunk

3.1.1 Creating a New Index in Splunk

Creating an index in Splunk allows storing, organizing, and querying logs or event data for analysis. The **proactive** index will store data like Suricata logs and alerts for further investigation.



3.1.2 Navigating and Managing Index Files

This step imports relevant Suricata logs into the proactive index for Splunk to process and analyze.

- ***eve.json:*** JSON-formatted Suricata log file.
- ***fast.log:*** Quick text-based alerts generated by Suricata.
- ***stats.log:*** Statistical data about Suricata's performance.
- ***suricata.log:*** General logs from Suricata's operations.
- ***System.json:*** Additional system-related log data.

```
┌──(root㉿kali)-[/opt/splunk/var/lib/splunk]
└─# ls
audit           _configtracker.dat  _dsphonehome  _internal.dat       kvstore          modinputs          summarydb
_audit.dat      defaultdb           fishbucket    _internaldb         _metrics         newbot             _telemetry
authDb          _dsappevent         hashDb        _introspection      _metrics.dat     persistentstorage  _telemetry.dat
_configtracker  _dsclient           historydb     _introspection.dat  _metrics_rollup  proactive

┌──(root㉿kali)-[/opt/splunk/var/lib/splunk]
└─# cd proactive
┌──(root㉿kali)-[/opt/…/var/lib/splunk/proactive]
└─# ls
colddb  datamodel_summary  db  thaweddb

┌──(root㉿kali)-[/opt/…/var/lib/splunk/proactive]
└─# rm -r *
zsh: sure you want to delete all 4 files in /opt/splunk/var/lib/splunk/proactive [yn]? y

┌──(root㉿kali)-[/opt/…/var/lib/splunk/proactive]
└─# cp -r /home/menna/Desktop/Project/* .

┌──(root㉿kali)-[/opt/…/var/lib/splunk/proactive]
└─# ls
eve.json  fast.log  stats.log  suricata.log  System.json
```

3.1.3 Configuring Data Inputs in Splunk

The *inputs.conf* file is set up to ingest logs from the Suricata and system directories into the proactive index.

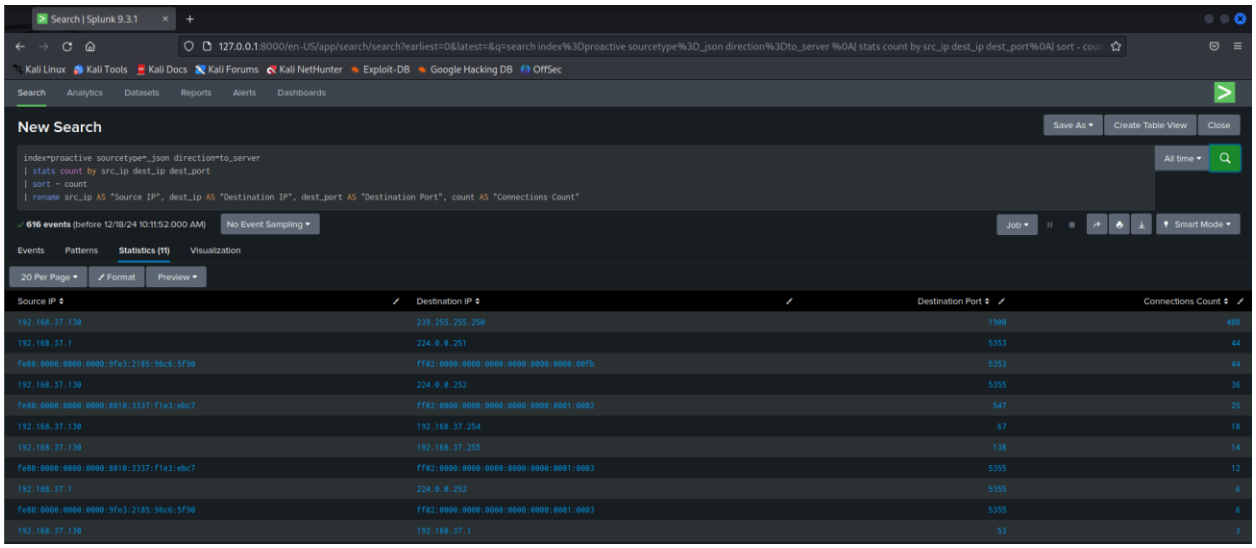
```
root@kali: /opt/splunk/var/lib/splunk/proactive ×   menna@kali: ~ ×
  GNU nano 7.2                    /opt/splunk/etc/system/local/inputs.conf *
[monitor:///opt/splunk/var/lib/splunk/proactive/eve.json]
index = proactive
sourcetype = _json

[monitor:///opt/splunk/var/lib/splunk/proactive/System.json]
index = proactive
sourcetype = _json


[monitor:///opt/splunk/var/lib/splunk/proactive/*.log]
index = proactive
sourcetype = suricata_logs
```

3.2 Splunk Query Analysis

3.2.1 Detect abnormal outbound traffic

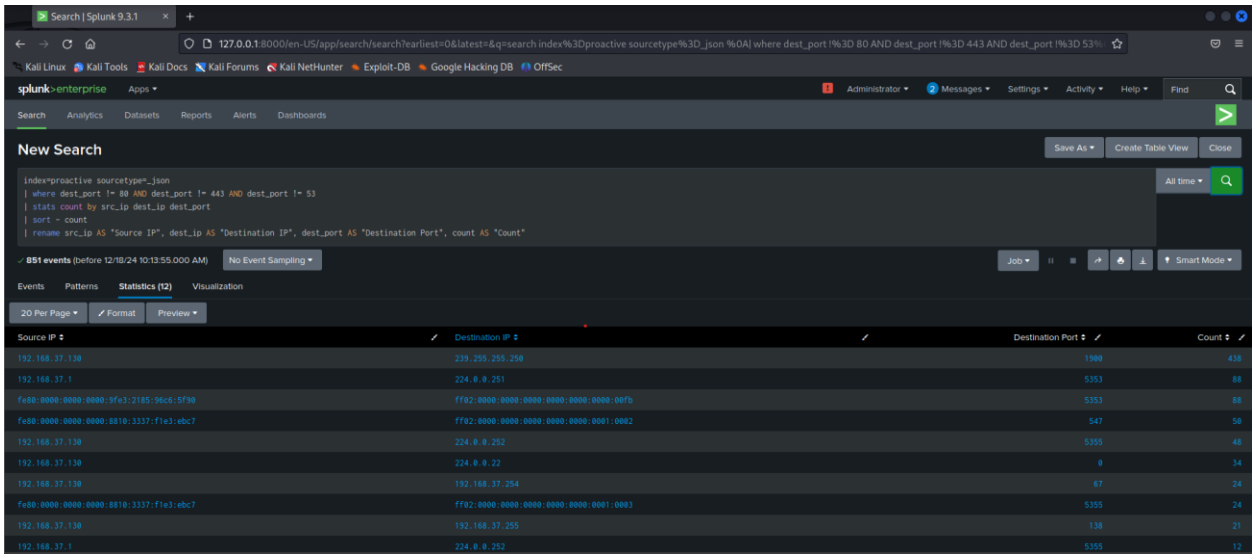
It uses the stats function to group and count events by source IP (src_ip), destination IP (dest_ip), and destination port (dest_port).

From the result, we noticed that there are some abnormal destination ports so we are going to do further detailed queries.



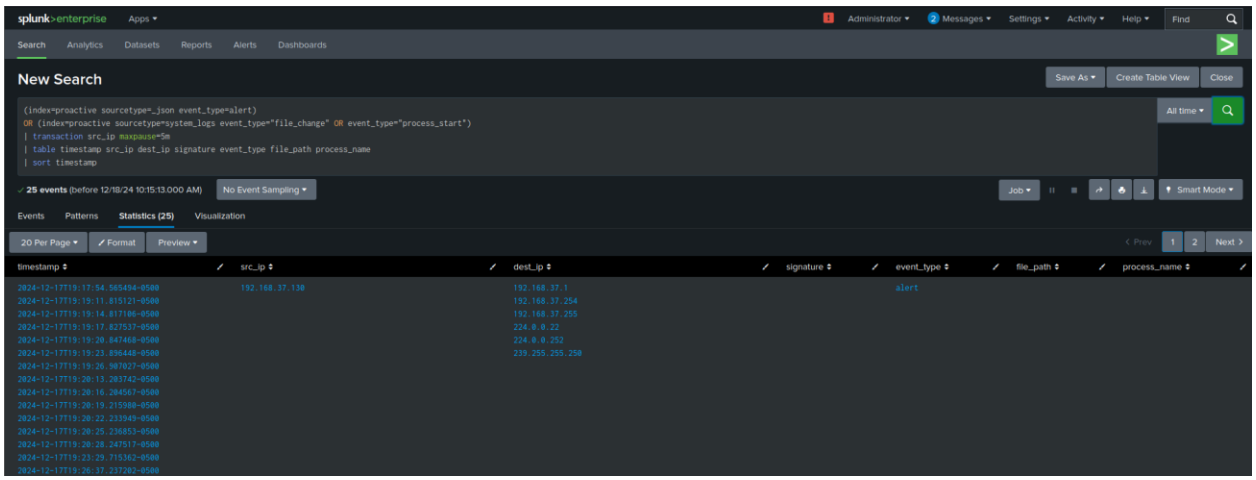
Our query filters out common destination ports 80 (HTTP), 443 (HTTPS), and 53 (DNS), narrowing the analysis to traffic targeting less typical ports.

It's clear now that these remaining ports are abnormal, and with little investigation we identified that these ports might be used by Zeus Trojan for scanning, lateral movement, or malware activity.



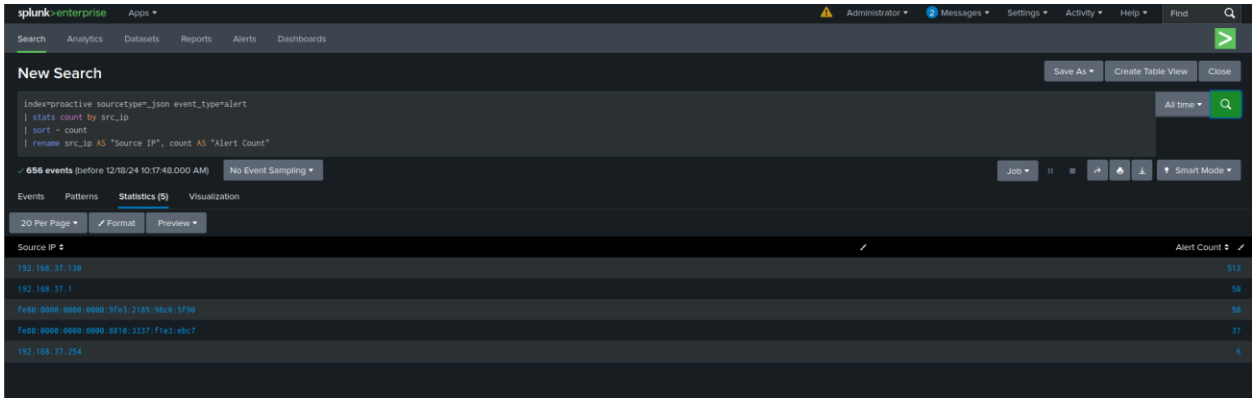
3.2.2 Link network anomalies with system activity

This Splunk query combines and analyzes logs from the proactive index where either the sourcetype is *_json* with an event_type of **"alert"** or the sourcetype is *system_logs* with an event_type of **"file_change"** or **"process_start."**

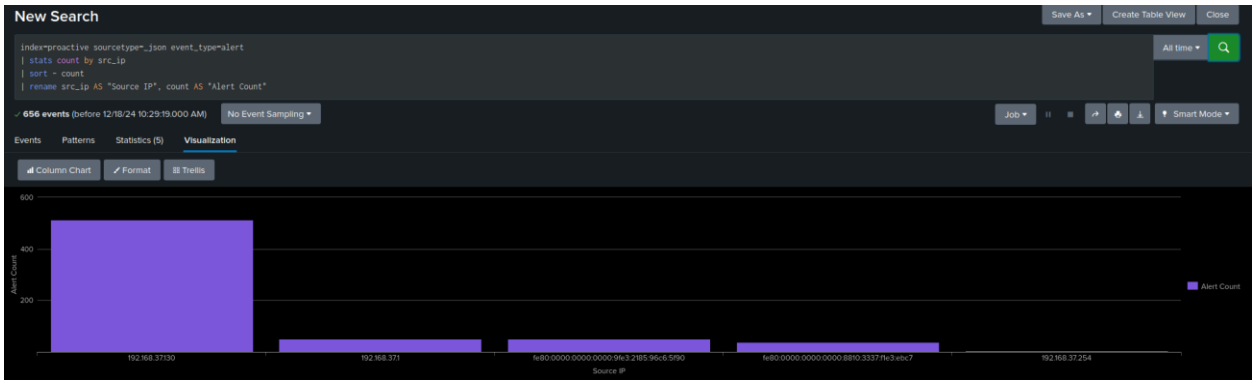


3.2.3 Create visual dashboards in Splunk to track malicious activity

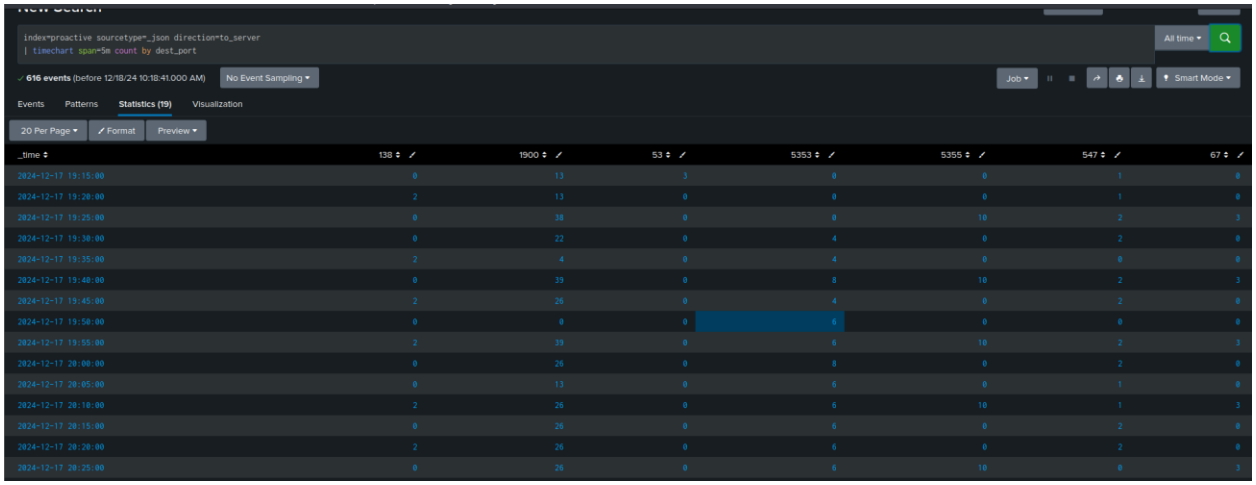
Our query analyzes logs with a JSON sourcetype where the event_type is **"alert."** It aggregates the number of alert events by src_ip using the stats command to count occurrences for each source IP.



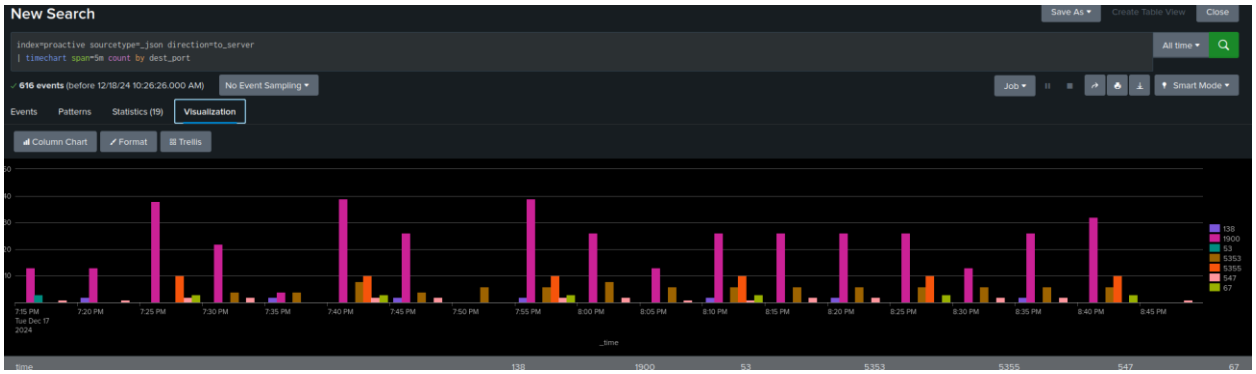
It provides a clear summary of which source IPs are generating the most alerts, helping identify potentially malicious or anomalous activity for further investigation.



In this query we are using the **timechart** command to create a time-based visualization, aggregating the count of events for each dest_port (destination port) over 5-minute intervals (span=5m).



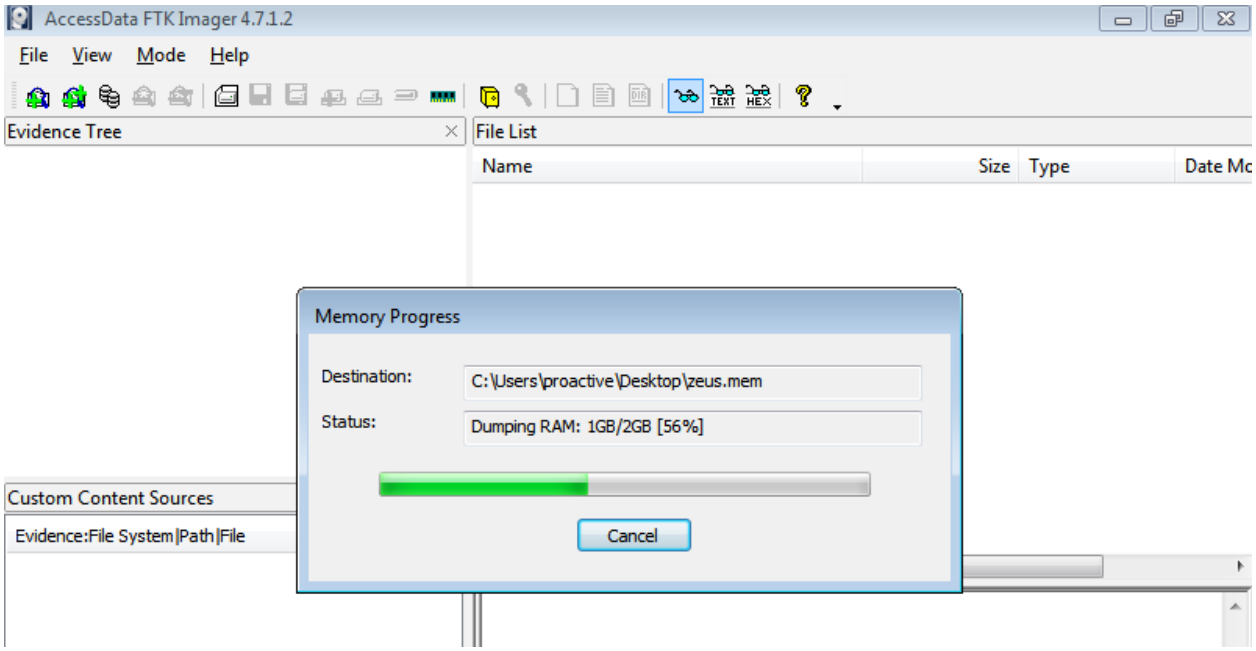
_time	138	1900	53	5353	5355	547	67
2024-12-17 19:15:00	0	13	3	0	0	1	0
2024-12-17 19:20:00	2	13	0	0	0	1	0
2024-12-17 19:25:00	0	38	0	0	10	2	3
2024-12-17 19:30:00	0	22	0	4	0	2	0
2024-12-17 19:35:00	2	4	0	4	0	0	0
2024-12-17 19:40:00	0	39	0	8	10	2	3
2024-12-17 19:45:00	2	26	0	4	0	2	0
2024-12-17 19:50:00	0	0	0	6	0	0	0
2024-12-17 19:55:00	2	39	0	6	10	2	3
2024-12-17 20:00:00	0	26	0	8	0	2	0
2024-12-17 20:05:00	0	13	0	6	0	1	0
2024-12-17 20:10:00	2	26	0	6	10	1	3
2024-12-17 20:15:00	0	26	0	6	0	2	0
2024-12-17 20:20:00	2	26	0	6	0	2	0
2024-12-17 20:25:00	0	26	0	6	10	0	3



4. Volatility

4.1 Capturing a Memory Dump using FTK Imager

This memory dump will later be analyzed to detect malicious processes or behaviors, such as those associated with the Zeus Trojan.



4.2 Analyzing the Memory Dump with Volatility

This output allows identification of running processes during the memory dump. There might be some suspicious processes, to make sure of our hypothesis we will move forward to the next step for deeper analysis.

```
┌──(menna㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 vol.py -f '/home/menna/Desktop/zeus.mem' windows.pslist
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xfa8018d4a990  86      643     N/A     False   2024-12-18 02:15:49.000000 UTC  N/A     Disabled
260     4       smss.exe        0xfa801a992380  2       29      N/A     False   2024-12-18 02:15:49.000000 UTC  N/A     Disabled
340     332     csrss.exe       0xfa801a0806b0  9       386     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
376     332     wininit.exe     0xfa801aa15060  3       72      0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
388     368     csrss.exe       0xfa801aa16b30  7       226     1       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
428     368     winlogon.exe    0xfa801b014060  4       113     1       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
472     376     services.exe    0xfa801b038b30  9       207     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
480     376     lsass.exe       0xfa801b042b30  7       525     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
488     376     lsm.exe 0xfa801b043530  10      139     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
600     472     svchost.exe     0xfa801b007b30  11      361     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
680     472     svchost.exe     0xfa801b223120  6       257     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
760     472     svchost.exe     0xfa801b23ab30  18      387     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
840     472     svchost.exe     0xfa801b27cb30  20      490     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
880     472     svchost.exe     0xfa801b2b2740  35      825     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
948     760     audiodg.exe     0xfa801b2dd3a0  5       122     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
1016    472     svchost.exe     0xfa801b308660  12      173     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
936     472     svchost.exe     0xfa801b362060  16      364     0       False   2024-12-18 02:15:50.000000 UTC  N/A     Disabled
1100    472     spoolsv.exe     0xfa801b3c7b30  13      265     0       False   2024-12-18 02:15:51.000000 UTC  N/A     Disabled
1108    880     taskeng.exe     0xfa801b3cbb30  5       77      0       False   2024-12-18 02:15:51.000000 UTC  N/A     Disabled
1240    472     svchost.exe     0xfa801b489b30  9       147     0       False   2024-12-18 02:15:51.000000 UTC  N/A     Disabled
1764    472     taskhost.exe    0xfa801b587b30  8       144     1       False   2024-12-18 02:15:56.000000 UTC  N/A     Disabled
1816    840     dwm.exe 0xfa801b596b30  4       69      1       False   2024-12-18 02:15:56.000000 UTC  N/A     Disabled
1852    1784    explorer.exe    0xfa801b5bd5a0  36      814     1       False   2024-12-18 02:15:56.000000 UTC  N/A     Disabled
1680    472     SearchIndexer.  0xfa801b588060  13      690     0       False   2024-12-18 02:16:02.000000 UTC  N/A     Disabled
664     1680    SearchProtocol  0xfa801b6d7b30  6       220     1       False   2024-12-18 02:16:03.000000 UTC  N/A     Disabled
1424    600     WmiPrvSE.exe    0xfa801b6c4b30  8       129     0       False   2024-12-18 02:17:25.000000 UTC  N/A     Disabled
1120    840     WUDFHost.exe    0xfa801b6fdb30  8       196     0       False   2024-12-18 02:17:45.000000 UTC  N/A     Disabled
1404    472     svchost.exe     0xfa801b775b30  10      143     0       False   2024-12-18 02:17:52.000000 UTC  N/A     Disabled
276     472     sppsvc.exe      0xfa801b6c37f0  5       141     0       False   2024-12-18 02:17:52.000000 UTC  N/A     Disabled
2224    472     msiexec.exe     0xfa8019c39310  14      224     0       False   2024-12-18 02:18:10.000000 UTC  N/A     Disabled
2264    2224    msiexec.exe     0xfa8019be9b30  0       -       1       False   2024-12-18 02:18:10.000000 UTC  2024-12-18 02:18:24.000000 UTC  Disabled
2312    472     VSSVC.exe       0xfa801b516b30  12      200     0       False   2024-12-18 02:18:18.000000 UTC  N/A     Disabled
2344    472     svchost.exe     0xfa801adc6630  5       67      0       False   2024-12-18 02:18:18.000000 UTC  N/A     Disabled
2664    2196    FTK Imager.exe  0xfa8019158b30  18      419     1       False   2024-12-18 02:18:23.000000 UTC  N/A     Disabled
2768    600     WmiPrvSE.exe    0xfa8019adb930  9       172     0       False   2024-12-18 02:18:38.000000 UTC  N/A     Disabled
2920    1680    SearchProtocol  0xfa801914c750  8       318     0       False   2024-12-18 02:19:03.000000 UTC  N/A     Disabled
2940    1680    SearchFilterHo  0xfa80191bf780  5       97      0       False   2024-12-18 02:19:03.000000 UTC  N/A     Disabled
```

4.3 Analyzing Malicious Memory Artifacts with Volatility

The ***windows.malfind*** plugin in Volatility is used to identify malicious code or injected processes in the memory dump (zeus.mem).

- ***Services.exe (PID 472)***
  - **Sevices.exe** is a legitimate Windows system process responsible for managing background services.
  - **Malware**, such as Zeus, frequently injects malicious code into this process to achieve persistence and evade detection.
  - The presence of executable memory regions (PAGE_EXECUTE_READWRITE) and a PE header is abnormal and strongly indicative of code injection.
- ***Explorer.exe (PID 1852)***
  - **Explorer.exe** is the Windows shell process, responsible for the user interface.
  - **Malware** often targets this process for injecting malicious code due to its persistence and frequent use.
  - The presence of multiple PE headers and executable memory regions indicates potential malicious injection or the presence of packed malware
- ***FTK Imager.exe (PID 2664)***
  - It's a good point that volatility detected that FTK Imager could be used in an unethical manner, but we used for memory dump so it's okay.

- ***SearchFilterHost.exe (PID 2940)***
    - **SearchFilterHost.exe** is a legitimate process used by Windows Search functionality.
    - **Malware** often uses less obvious processes like SearchFilterHost.exe to perform stealthy operations.
    - Executable memory regions without an MZ header suggest the presence of custom shellcode or obfuscated malicious data.

```
┌──(menna㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 vol.py -f '/home/menna/Desktop/zeus.mem' windows.malfind
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm

472     services.exe    0x2a0000        0x2b1fff        Vad     PAGE_EXECUTE_READWRITE  0       0       Disabled        MZ header
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 ................        4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 d8 00 00 00
1852    explorer.exe    0x3a30000       0x3a41fff       Vad     PAGE_EXECUTE_READWRITE  0       0       Disabled        MZ header
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 ................        4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 d8 00 00 00
1852    explorer.exe    0x3bf0000       0x3bf0fff       VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 bf 03 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 03 00 00
 00 00 00 00 00 00 00 00 00
1852    explorer.exe    0x4e40000       0x4e4ffff       VadS    PAGE_EXECUTE_READWRITE  16      1       Disabled        N/A
41 ba 80 00 00 00 48 b8 38 a1 3c fe fe 07 00 00 A.....H.8.<.....
48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 3c fe H. .A.....H.8.<.
fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8 ....H. .A.....H.
38 a1 3c fe fe 07 00 00 48 ff 20 90 41 ba 83 00 8.<.....H. .A...        41 ba 80 00 00 00 48 b8 38 a1 3c fe fe 07 00 00 48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 3c fe fe 07 00 00 48 ff
 00 48 ff 20 90 41 ba 83 00
2664    FTK Imager.exe  0x6060000       0x6060fff       VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 06 06 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 06 00 00
 00 00 00 00 00 00 00 00 00
2664    FTK Imager.exe  0x60a0000       0x60affff       VadS    PAGE_EXECUTE_READWRITE  16      1       Disabled        N/A
41 ba 80 00 00 00 48 b8 38 a1 3c fe fe 07 00 00 A.....H.8.<.....
48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 3c fe H. .A.....H.8.<.
fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8 ....H. .A.....H.
38 a1 3c fe fe 07 00 00 48 ff 20 90 41 ba 83 00 8.<.....H. .A...        41 ba 80 00 00 00 48 b8 38 a1 3c fe fe 07 00 00 48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 3c fe fe 07 00 00 48 ff
 00 48 ff 20 90 41 ba 83 00
2940    SearchFilterHo  0xb00000        0xb7ffff        VadS    PAGE_EXECUTE_READWRITE  2       1       Disabled        N/A
00 00 00 00 00 00 00 00 04 5d 76 b9 e8 24 00 01 .........]v..$..
ee ff ee ff 00 00 00 00 28 01 b0 00 00 00 00 00 ........(.......
28 01 b0 00 00 00 00 00 00 00 b0 00 00 00 00 00 (...............
```

4.4 Analysis of Volatility Process Details

The **windows.pstree** plugin in Volatility generates a hierarchical view of the processes running in the memory dump (zeus.mem). It allows analysts to examine the parent-child relationships of processes, helping to detect anomalies or suspicious behavior. The --pid 472 argument restricts the analysis to the process with Process ID (PID) 472, identified earlier as services.exe.

- ***Parent and Child Processes*** such as *wininit.exe*, *svchost.exe* and *taskhost.exe* are all used in background services which ensures our assumptions that they could be malicious.
- ***Suspicious Indicators***
    - A large number of *svchost.exe* instances may indicate potential misuse, as this process is commonly exploited by malware for persistence.
    - Some child processes, like *SearchProtocolHost.exe* and *SearchFilterHost.exe*, show complex arguments and might warrant further inspection for anomalies.

```
┌──(menna㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 vol.py -f '/home/menna/Desktop/zeus.mem' windows.pstree --pid 472
[sudo] password for menna:
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

376     332     wininit.exe     0xfa801aa15060  3       72      0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\wininit.exe    wininit.exe     C:\Windows\system32\wininit.exe
* 472   376     services.exe    0xfa801b038b30  9       207     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\services.exe   C:\Windows\system32\services.exe        C:\Windows\system32\
services.exe
** 1764 472     taskhost.exe    0xfa801b587b30  8       144     1       False   2024-12-18 02:15:56.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskhost.exe   "taskhost.exe"  C:\Windows\system32\taskhost.exe
** 840  472     svchost.exe     0xfa801b27cb30  20      490     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestric
ted     C:\Windows\System32\svchost.exe
*** 1816        840     dwm.exe 0xfa801b596b30  4       69      1       False   2024-12-18 02:15:56.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\dwm.exe        "C:\Windows\system32\Dwm.exe"   C:\Windows\system32\Dwm.exe
*** 1120        840     WUDFHost.exe    0xfa801b6fdb30  8       196     0       False   2024-12-18 02:17:45.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\WUDFHost.exe   "C:\Windows\system32\WUDFHost.exe" -HostGUID:{193a18
20-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:HostProcess-875ca0d4-7064-4435-b3b5-8d27032dd602 -SystemEventPortName:HostProcess-fa5f4078-000a-4989-9a44-ef613c7b0e3c -IoCancelEventPortName:HostProcess-e3f7be71-7fc9-4872-b87e-6584b25d7
690 -NonStateChangingEventPortName:HostProcess-3e6d4830-876b-4035-8079-838a8736aee0 -Service5ID:S-1-5-80-2652678385-582572993-1835434367-1344795993-749280709 -LifetimeId:f070c398-32b2-42d4-853f-9c9b3412b179  C:\Windows\system32\WUDFHost
.exe
** 680  472     svchost.exe     0xfa801b223120  6       257     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k RPCSS        C:\Windows\s
ystem32\svchost.exe
** 936  472     svchost.exe     0xfa801b362060  16      364     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k NetworkService       C:\W
indows\system32\svchost.exe
** 2312 472     VSSVC.exe       0xfa801b516b30  12      200     0       False   2024-12-18 02:18:18.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\VSSVC.exe      C:\Windows\system32\vssvc.exe   C:\Windows\system32\vssvc.ex
e
** 1100 472     spoolsv.exe     0xfa801b3c7b30  13      265     0       False   2024-12-18 02:15:51.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\spoolsv.exe    C:\Windows\System32\spoolsv.exe C:\Windows\System32\spoolsv.
exe
** 2344 472     svchost.exe     0xfa801adc6630  5       67      0       False   2024-12-18 02:18:18.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\System32\svchost.exe -k swprv        C:\Windows\S
ystem32\svchost.exe
** 760  472     svchost.exe     0xfa801b23ab30  18      387     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestri
cted    C:\Windows\System32\svchost.exe
** 948 760     audiodg.exe     0xfa801b2dd3a0  5       122     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\audiodg.exe    C:\Windows\system32\AUDIODG.EXE 0x2ac   C:\Windows\system32\
AUDIODG.EXE
** 880  472     svchost.exe     0xfa801b2b2740  35      825     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k netsvcs      C:\Windows\s
ystem32\svchost.exe
*** 1180        880     taskeng.exe     0xfa801b3cbb30  5       77      0       False   2024-12-18 02:15:51.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskeng.exe    taskeng.exe {AC3F4CCE-52BA-496D-A03E-8F16765BED05} C
:\Windows\system32\taskeng.exe
** 1680 472     SearchIndexer.  0xfa801b588060  13      690     0       False   2024-12-18 02:16:02.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\SearchIndexer.exe      C:\Windows\system32\SearchIndexer.exe /Embedding   C
:\Windows\system32\SearchIndexer.exe
*** 664 1680    SearchProtocol  0xfa801b6d7b30  6       220     1       False   2024-12-18 02:16:03.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\SearchProtocolHost.exe "C:\Windows\system32\SearchProtocolHost.exe" Global\
UsGthrFltPipeMssGthrPipe_S-1-5-21-1798409883-3693947551-2283680810-10002_ Global\UsGthrCtrlFltPipeMssGthrPipe_S-1-5-21-1798409883-3693947551-2283680810-10002 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MS
```

From the result we couldn't find any malicious indicators, but it could be used by Zeus Trojan to evade detection by using multiple instances of it.

```
┌──(menna㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 vol.py -f '/home/menna/Desktop/zeus.mem' windows.pstree --pid 1852
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

1852    1784    explorer.exe    0xfa801b5bd5a0  36      814     1       False   2024-12-18 02:15:56.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\
```

Suspicious Indicators

- ***SearchIndexer.exe*** inherits suspicious parent process.
- ***SearchFilterHo*** truncated name.
- Unusual command-line arguments, possibly indicating malicious payload execution.

```
┌──(menna㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 vol.py -f '/home/menna/Desktop/zeus.mem' windows.pstree --pid 2940
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

376     332     wininit.exe     0xfa801aa15060  3       72      0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\wininit.exe
* 472   376     services.exe    0xfa801b038b30  9       207     0       False   2024-12-18 02:15:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\services.exe
services.exe
** 1680 472     SearchIndexer.  0xfa801b588060  13      690     0       False   2024-12-18 02:16:02.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\SearchIndexer.
:\Windows\system32\SearchIndexer.exe
*** 2940        1680    SearchFilterHo  0xfa80191bf780  5       97      0       False   2024-12-18 02:19:03.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\Search
 504 508 516 65536 512  C:\Windows\system32\SearchFilterHost.exe
```

4.5 Analysis of Volatility Network Scan Output

The **windows.netscan** plugin in Volatility is used to analyze active network connections and listening ports in the memory dump (zeus.mem). It provides details about the processes managing network activities and their associated IP addresses, ports, and states. This analysis helps detect malicious network behavior, such as unauthorized communication or command-and-control (C2) activity.

```
┌──(menna㉿kali)-[~/Downloads/volatility3]
└─$ sudo python3 vol.py -f '/home/menna/Desktop/zeus.mem' windows.netscan
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x7d40d240      UDPv4   0.0.0.0 5355    *       0               936     svchost.exe     2024-12-18 02:16:05.000000 UTC
0x7d465bb0      UDPv4   169.254.85.38   1900    *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
0x7d48da50      UDPv6   ::1     1900    *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
0x7d4a24e0      TCPv4   169.254.85.38   139     0.0.0.0 0       LISTENING       4       System  -
0x7d4a8ec0      UDPv4   169.254.85.38   138     *       0               4       System  2024-12-18 02:16:05.000000 UTC
0x7d4edd70      UDPv4   169.254.85.38   137     *       0               4       System  2024-12-18 02:16:05.000000 UTC
0x7d52d1b0      UDPv4   0.0.0.0 0       *       0               936     svchost.exe     2024-12-18 02:16:05.000000 UTC
0x7d52d1b0      UDPv6   ::      0       *       0               936     svchost.exe     2024-12-18 02:16:05.000000 UTC
0x7d5742c0      UDPv4   127.0.0.1       1900    *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
0x7d584240      UDPv4   192.168.37.130  1900    *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
0x7d668c60      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       472     services.exe    -
0x7d668c60      TCPv6   ::      49155   ::      0       LISTENING       472     services.exe    -
0x7d67b290      TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0x7d67b290      TCPv6   ::      445     ::      0       LISTENING       4       System  -
0x7d7678d0      UDPv4   0.0.0.0 5355    *       0               936     svchost.exe     2024-12-18 02:16:05.000000 UTC
0x7d7678d0      UDPv6   ::      5355    *       0               936     svchost.exe     2024-12-18 02:16:05.000000 UTC
0x7d7fcd20      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       480     lsass.exe       -
0x7d7fcd20      TCPv6   ::      49156   ::      0       LISTENING       480     lsass.exe       -
0x7d82def0      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       680     svchost.exe     -
0x7d82e5e0      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       680     svchost.exe     -
0x7d82e5e0      TCPv6   ::      135     ::      0       LISTENING       680     svchost.exe     -
0x7d8378d0      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       376     wininit.exe     -
0x7d8378d0      TCPv6   ::      49152   ::      0       LISTENING       376     wininit.exe     -
0x7d8739d0      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       760     svchost.exe     -
0x7d874830      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       760     svchost.exe     -
0x7d874830      TCPv6   ::      49153   ::      0       LISTENING       760     svchost.exe     -
0x7d8ddec0      UDPv6   fe80::8810:3337:f1e3:ebc7       53482   *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
0x7d9437b0      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       480     lsass.exe       -
0x7d96d2e0      TCPv4   0.0.0.0 16470   0.0.0.0 0       LISTENING       472     services.exe    -
0x7d992d40      UDPv4   192.168.37.130  137     *       0               4       System  2024-12-18 02:15:50.000000 UTC
0x7d9961c0      UDPv4   192.168.37.130  138     *       0               4       System  2024-12-18 02:15:50.000000 UTC
0x7db32200      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       376     wininit.exe     -
0x7dbb2bb0      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       880     svchost.exe     -
0x7dbb4670      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       880     svchost.exe     -
0x7dbb4670      TCPv6   ::      49154   ::      0       LISTENING       880     svchost.exe     -
0x7dc242f0      TCPv4   192.168.37.130  139     0.0.0.0 0       LISTENING       4       System  -
0x7dfe8760      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       472     services.exe    -
0x7e46b260      UDPv6   ::1     53483   *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
0x7e6c31e0      UDPv4   127.0.0.1       53486   *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
0x7e6d61e0      UDPv6   fe80::1121:30bb:ed5b:5526       53481   *       0               1404    svchost.exe     2024-12-18 02:17:52.000000 UTC
```

Process	PID	Protocol	Local Address	Local Port	Reason for Suspicion
services.exe	472	TCPv4	0.0.0.0	49155	Unusual high dynamic port usage.
		TCPv4	0.0.0.0	49156	High port usage; potential backdoor activity.
		UDPv4	0.0.0.0	16470	Dynamic port open without foreign connections.
svchost.exe	936	UDPv4	0.0.0.0	5355	Handles multicast DNS; often exploited by malware.
	1404	UDPv4	169.254.85.38	1900	High multicast traffic; potential misuse.
		UDPv6	::	5355	Listening on wildcard address; suspicious usage.

Side Notes:

- **Dynamic Ports:** Ports above 49152 are usually temporary and should not remain open persistently, which makes it more suspicious.
- **Multicast and Wildcard Addresses:** Processes using 0.0.0.0, ::, or multicast addresses (5355, 1900) may indicate unauthorized or suspicious activity, especially if unrelated to the system's normal role.
- **Critical Services Misuse:** Both services.exe and svchost.exe are legitimate processes but are frequently exploited by malware like Zeus to maintain persistence or facilitate communication with external servers.

5. YARA Rules

This rule is designed to detect Zeus malware artifacts in binaries, configuration files, and memory dumps. It uses a combination of static strings and byte patterns that are commonly associated with Zeus malware.

```
  GNU nano 7.2                    /home/menna/Desktop/yarazeus.yar
rule Zeus_Malware_General
{
    meta:
        description = "Detect Zeus malware artifacts in binaries, config files, and memory dumps"
        author = "Your Name"
        date = "2024-12-18"

    strings:
        $zeus_str1 = "ZeuS"
        $zeus_config_keyword = "ZeusConfig"
        $c2_traffic = "GET /update HTTP/1.1"
        $c2_request = "POST /commands HTTP/1.1"
        $user_agent = "Mozilla/5.0"
        $mz_header = { 4D 5A }
        $pe_header = { 50 45 00 00 }
        $nop_sled = { 90 90 90 90 }
        $shellcode_pattern = { 41 BA 80 00 00 00 48 B8 38 A1 }

    condition:
        // Ensure $nop_sled is matched with other Zeus indicators
        ($nop_sled and any of ($zeus_str1, $zeus_config_keyword, $c2_traffic, $c2_request, $user_agent))
        or $mz_header or $pe_header or $shellcode_pattern
}
```

The result of executing the YARA Rules we created on the memory dump file

```
┌──(menna㉿kali)-[~/Desktop]
└─$ yara -r yarazeus.yar /home/menna/Desktop/zeus.mem
warning: rule "Zeus_Malware_General": too many matches for $nop_sled, results for this rule may be incorrect
Zeus_Malware_General /home/menna/Desktop/zeus.mem
```

For more detailed output, we added the **-s** argument

```
┌──(menna㉿kali)-[~/Desktop]
└─$ yara -r -s  yarazeus.yar /home/menna/Desktop/zeus.mem
warning: rule "Zeus_Malware_General": too many matches for $nop_sled, results for this rule may be incorrect
Zeus_Malware_General /home/menna/Desktop/zeus.mem
0×160b4:$mz_header: 4D 5A
0×86000:$mz_header: 4D 5A
0×8f000:$mz_header: 4D 5A
0×9b000:$mz_header: 4D 5A
0×169d34:$mz_header: 4D 5A
0×171000:$mz_header: 4D 5A
0×1f0000:$mz_header: 4D 5A
0×21133e:$mz_header: 4D 5A
0×244000:$mz_header: 4D 5A
0×245000:$mz_header: 4D 5A
0×24d000:$mz_header: 4D 5A
0×2c6000:$mz_header: 4D 5A
0×2cc000:$mz_header: 4D 5A
0×2ed184:$mz_header: 4D 5A
```

Thank you!

Team Members:

Haneen Amr Abdelhameed ID: 2106150

Menna Mohamed Islam ID: 20221457144

Tasneem Khaled El-Ashry ID: 20221443994