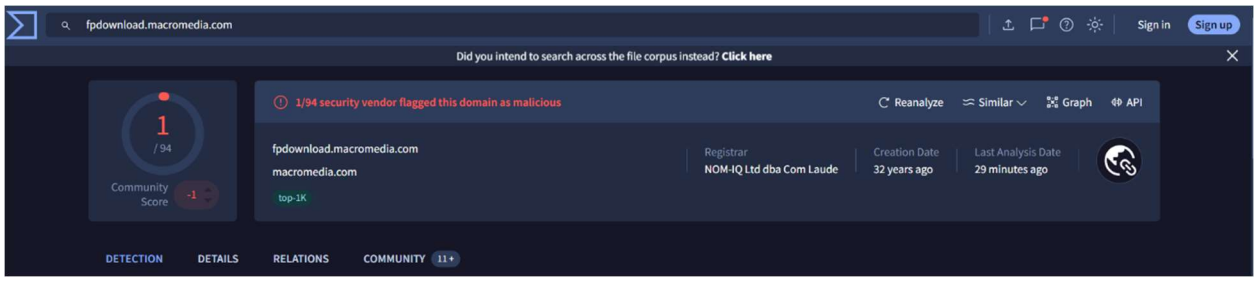
Proactive Final Project

Ranwah Gamal Asala	2106152
Menna Allah Ahmed Saad	2106212
Aml Ibrahim Mohamed	20221443988
Suhaila Adel Aly	20221376543
Nouran Abdelsalam Mohamed	20221377349

Project Steps

1. Execute Zeus banking trojan.
2. Check wireshark traffic for c2 communication indicators.



3. Create suricata rules to detect C2 communication
   - Detect the Specific URI Request: This rule looks for the specific URI path used in the Zeus communication:

     alert http any any -> any any (msg:"Zeus C2 - Specific URI Request"; content:"/get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z"; http_uri; classtype:trojan-activity; sid:1000001; rev:1;)

   - Detect the Specific User-Agent: This rule identifies HTTP requests with the specific User-Agent used in the request:

     alert http any any -> any any (msg:"Zeus C2 - Suspicious User-Agent"; content:"Flash Player Seed/3.0"; http_header; classtype:trojan-activity; sid:1000002; rev:1;)

   - Detect Host Header: This rule matches requests sent to the suspicious Host:

     alert http any any -> any any (msg:"Zeus C2 - Suspicious Host Header"; content:"Host: fpdownload.macromedia.com"; http_header; nocase; classtype:trojan-activity; sid:1000003; rev:1;)

   - Comprehensive Detection (All Conditions): To ensure the rule fires only if all conditions (URI, User-Agent, and Host) are met, you can combine these conditions:

     alert http any any -> any any (msg:"Zeus C2 - Complete Signature Match"; content:"/get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z"; http_uri; content:"Flash Player Seed/3.0"; http_header; content:"Host: fpdownload.macromedia.com"; http_header; nocase; classtype:trojan-activity; sid:1000004; rev:1;)

4. Download “emerging-all.rules” for common threat detection via this link: https://rules.emergingthreats.net/open/

5. Add “zeus.rules” and “emerging-all.rules” to “suricata.yaml”

suricata - Notepad

File Edit Format View Help

```
    # 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: C:\\Program Files\\Suricata\\rules\\

rule-files:
 - emerging-all.rules
 - zeus.rules
#- botcc.rules
#- botcc.portgrouped.rules
#- ciarmy.rules
#- compromised.rules
#- drop.rules
#- dshield.rules
```

6. Start suricata:

   suricata.exe -c suricata.yaml -i 10.0.2.15

Administrator: Command Prompt - suricata.exe -c suricata.yaml -i 10.0.2.15

```
C:\Windows\system32>cd c:\program files\suricata

c:\Program Files\Suricata>suricata.exe -c suricata.yaml -i 10.0.2.15
Info: win32-service: Running as service: no
Info: suricata: translated 10.0.2.15 to pcap device \Device\NPF_{43E2B5DD-04D9-4B1C-BC6C-308C8AEA6B32}
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
i: runmodes: thread stack size of 0 to too small: setting to 512k
W: threshold-config: Error opening file: "C:\Program Files\Suricata\\\threshold.config": No such file or directory
W: suricata: setrlimit unavailable.
i: threads: Threads created -> RX: 1 W: 1 FM: 1 FR: 1   Engine started.
```

7. Check Suricata logs for alerts.

Windows-10 (Freshly Installed) [Running] - Oracle VM VirtualBox

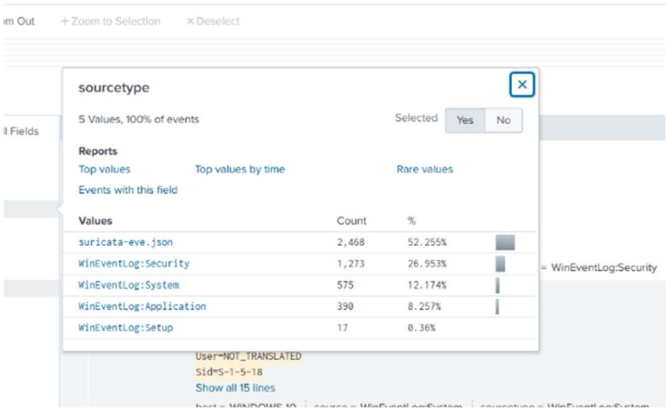
File Machine View Input Devices Help

fast - Notepad

File Edit Format View Help

```
12/20/2024-16:52:36.972662  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:50276 -> 85.114.128.127:53
12/20/2024-16:52:36.973606  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:50277 -> 85.114.128.127:53
12/20/2024-16:52:36.975412  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:50278 -> 85.114.128.127:53
12/20/2024-16:52:36.984855  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:50279 -> 85.114.128.127:53
12/20/2024-16:52:40.780519  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:50280 -> 85.114.128.127:53
12/20/2024-16:52:41.629317  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:50281 -> 85.114.128.127:53
12/20/2024-16:52:43.767307  [**] [1:1000001:1] Zeus C2 - Specific URI Request [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:43.767307  [**] [1:1000002:1] Zeus C2 - Suspicious User-Agent [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:43.767307  [**] [1:1000003:1] Zeus C2 - Suspicious Host Header [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:43.767307  [**] [1:1000004:1] Zeus C2 - Complete Signature Match [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:46.298701  [**] [1:1000001:1] Zeus C2 - Specific URI Request [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:46.298701  [**] [1:1000002:1] Zeus C2 - Suspicious User-Agent [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:46.298701  [**] [1:1000003:1] Zeus C2 - Suspicious Host Header [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:46.298701  [**] [1:1000004:1] Zeus C2 - Complete Signature Match [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51966 -> 23.39.69.211:80
12/20/2024-16:52:47.945765  [**] [1:1000001:1] Zeus C2 - Specific URI Request [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51967 -> 23.39.69.211:80
12/20/2024-16:52:47.945765  [**] [1:1000002:1] Zeus C2 - Suspicious User-Agent [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51967 -> 23.39.69.211:80
12/20/2024-16:52:47.945765  [**] [1:1000003:1] Zeus C2 - Suspicious Host Header [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51967 -> 23.39.69.211:80
12/20/2024-16:52:47.945765  [**] [1:1000004:1] Zeus C2 - Complete Signature Match [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:51967 -> 23.39.69.211:80
12/20/2024-18:28:59.800860  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:61555 -> 85.114.128.127:53
12/20/2024-18:28:59.804066  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:61556 -> 85.114.128.127:53
12/20/2024-18:28:59.804972  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:61557 -> 85.114.128.127:53
12/20/2024-18:28:59.812265  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:61558 -> 85.114.128.127:53
12/20/2024-18:29:04.750473  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:61559 -> 85.114.128.127:53
12/20/2024-18:29:06.297893  [**] [1:2015474:2] ET MALWARE ZeroAccess udp traffic detected [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.0.2.15:61560 -> 85.114.128.127:53
12/20/2024-18:29:07.957189  [**] [1:1000001:1] Zeus C2 - Specific URI Request [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:52860 -> 23.39.69.211:80
12/20/2024-18:29:07.957189  [**] [1:1000002:1] Zeus C2 - Suspicious User-Agent [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:52860 -> 23.39.69.211:80
12/20/2024-18:29:07.957189  [**] [1:1000003:1] Zeus C2 - Suspicious Host Header [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:52860 -> 23.39.69.211:80
12/20/2024-18:29:07.957189  [**] [1:1000004:1] Zeus C2 - Complete Signature Match [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.2.15:52860 -> 23.39.69.211:80
```

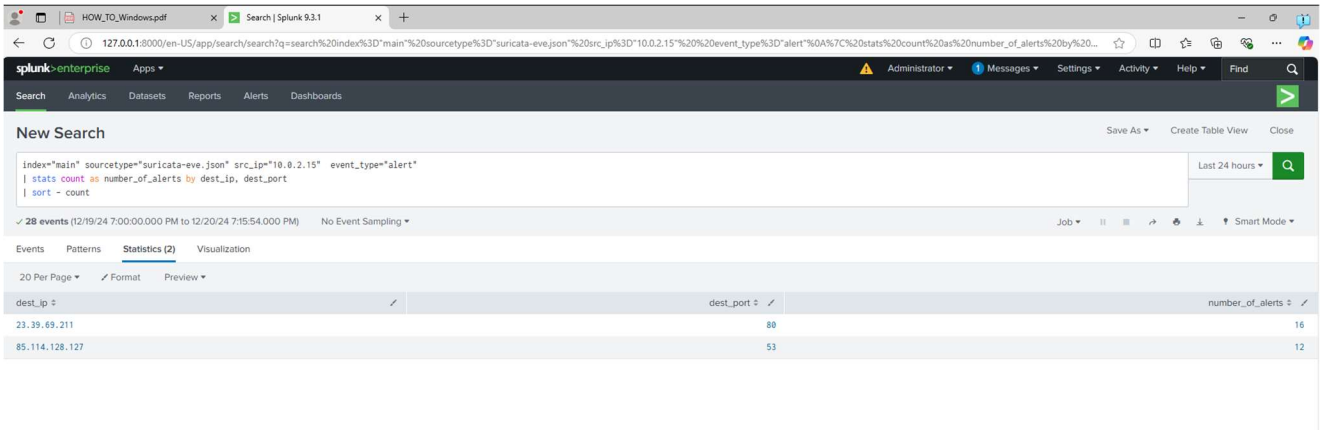
8. Import Suricata and System Logs to Splunk (details are shown in the video)



9. Splunk Correlation Rules:
    a. Detecting abnormal outbound traffic:

    index="main" sourcetype="suricata-eve.json" src_ip="10.0.2.15" event_type="alert"
    | stats count as number_of_alerts by dest_ip, dest_port
    | sort – count

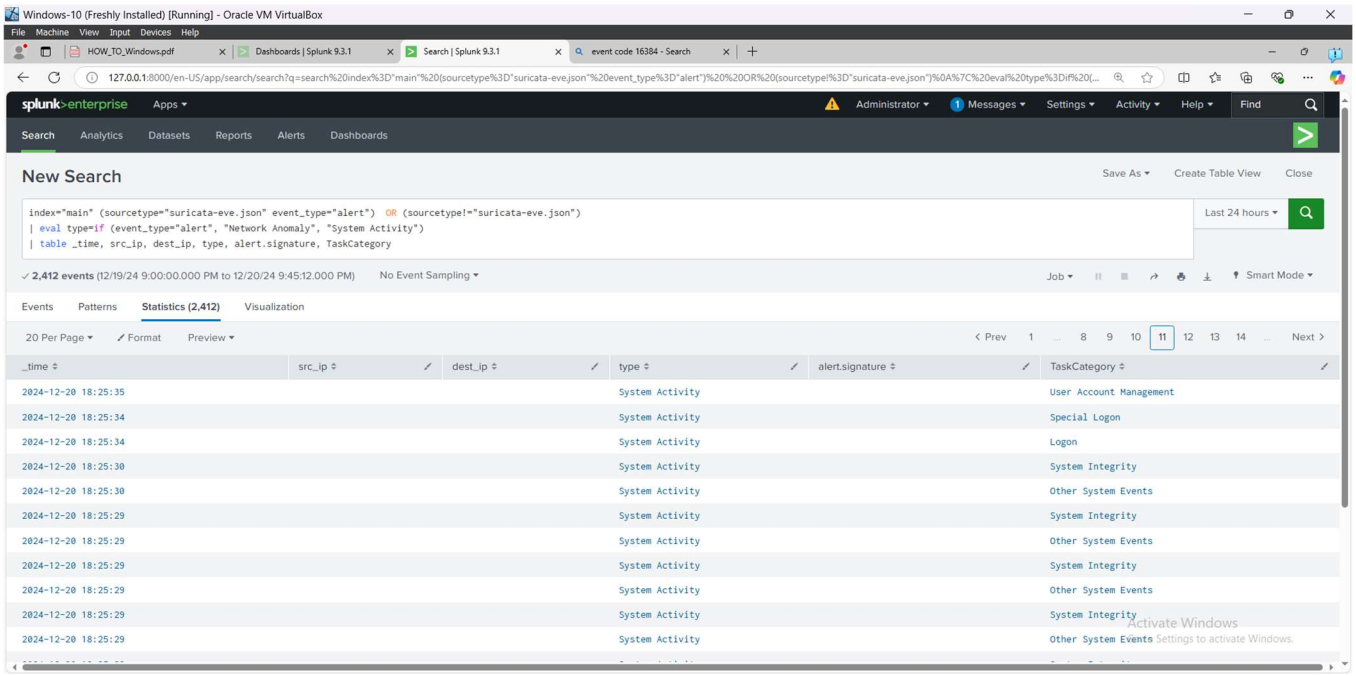
    This search query helps identify **abnormal outbound traffic** by focusing on alerts generated for traffic coming from a specific source IP. It aggregates these alerts by destination IP and port, and by sorting the results, it highlights the destinations with the most suspicious or unusual activity. This can point to potential malicious behavior, such as data exfiltration, command-and-control communication, or the device attempting to contact unauthorized external resources.

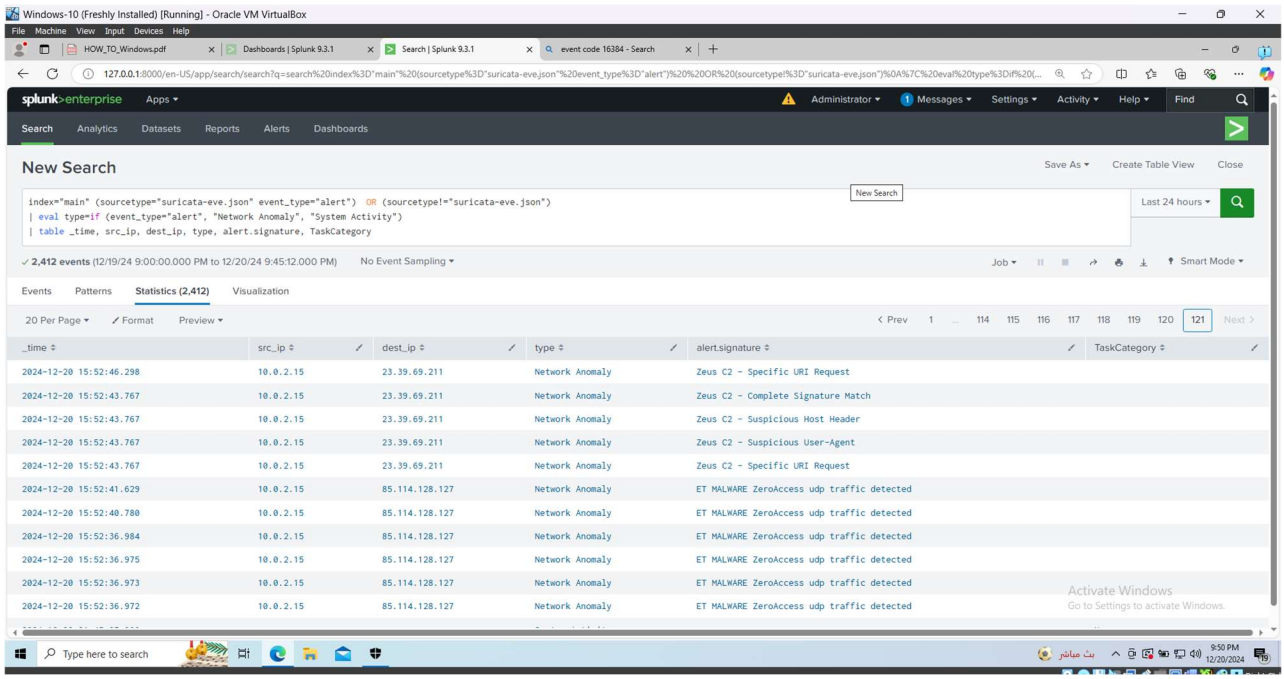


b. Linking Network Anomalies With System Activities

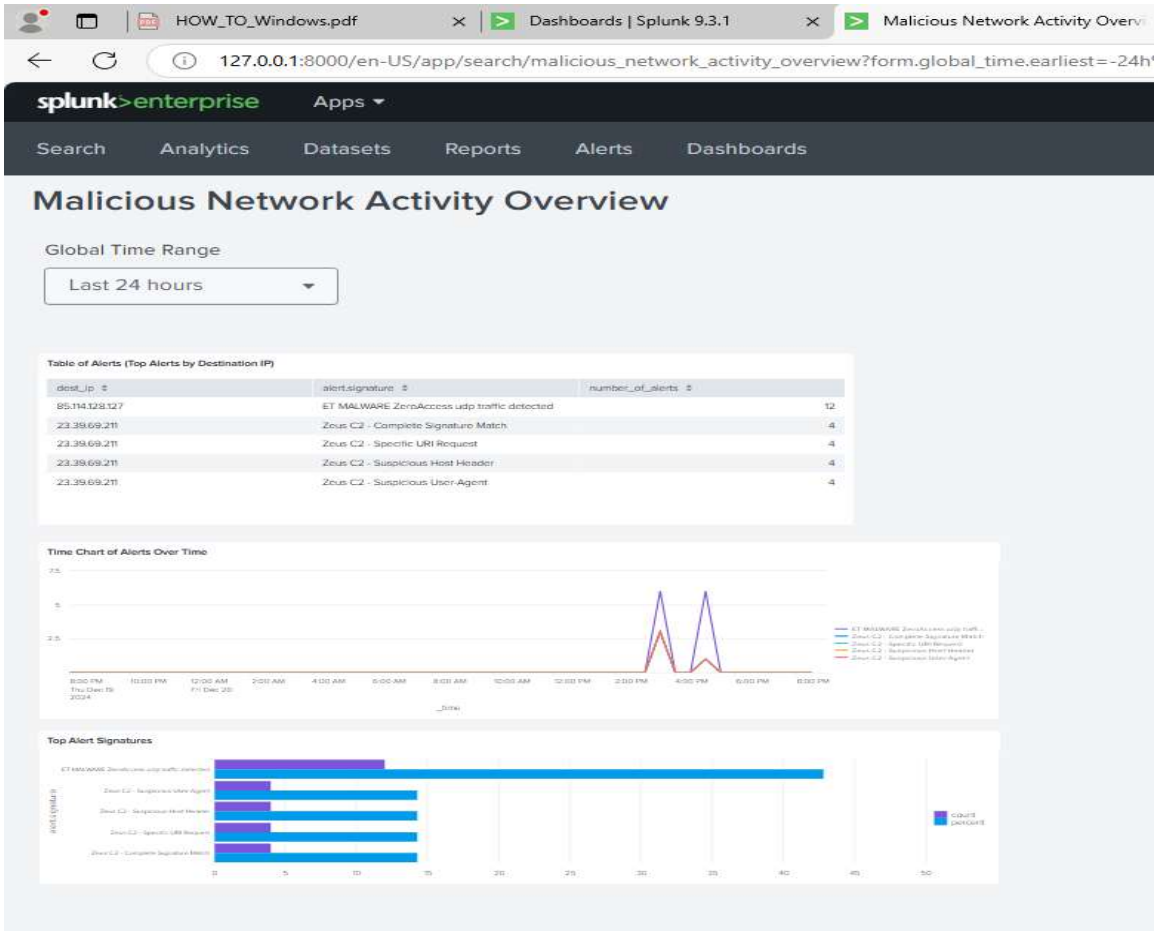
index="main" (sourcetype="suricata-eve.json" event_type="alert") OR (sourcetype!="suricata-eve.json")
| eval type=if (event_type="alert", "Network Anomaly", "System Activity")
| table _time, src_ip, dest_ip, type, alert.signature, TaskCategory

This query links network anomalies and system activities by combining Suricata alerts with other system logs into a unified view. It classifies events as either "Network Anomaly" (for Suricata alerts) or "System Activity" (for other system logs) using an eval statement. By displaying key fields such as the timestamp, source IP, destination IP, alert signature, and system activity category, it enables correlation between suspicious network behavior and corresponding system-level changes. This helps identify patterns, such as a network alert followed by suspicious process creation, providing a clear timeline of potential malicious activity for deeper investigation.





c. Create a visual dashboard to track malicious activity



10. use volatility to

- Identify active and injected processes related to Zeus

-Identify the running processes

```
┌──(menna㉿kali)-[~]
└─$ python3 ~/volatility3/vol.py -f ~/Downloads/zeus2×4.vmem windows.pslist

Volatility 3 Framework 2.13.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. The
se should be placed in the same directory with the same file name, e.g. zeus2×4.vmem and zeus2×4.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×823c8a00      57      671     N/A     False   N/A     N/A     Disabled
596     4       smss.exe        0×82292da0      3       19      N/A     False   2010-09-02 12:25:18.000000 UTC  N/A     Disabled
668     596     csrss.exe       0×821f2978      14      471     0       False   2010-09-02 12:25:21.000000 UTC  N/A     Disabled
692     596     winlogon.exe    0×822c09f8      21      588     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
744     692     services.exe    0×821a5da0      15      279     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
756     692     lsass.exe       0×822c8798      24      437     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
912     744     svchost.exe     0×82150b90      20      202     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
992     744     svchost.exe     0×822c8bf8      10      277     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1084    744     svchost.exe     0×82151da0      58      1327    0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1140    744     svchost.exe     0×821521b0      6       81      0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1192    744     svchost.exe     0×8214f488      13      175     0       False   2010-09-02 12:25:23.000000 UTC  N/A     Disabled
1436    744     iscsiexe.exe    0×8221e278      6       78      0       False   2010-09-02 12:25:24.000000 UTC  N/A     Disabled
1616    744     spoolsv.exe     0×82095500      13      140     0       False   2010-09-02 12:25:24.000000 UTC  N/A     Disabled
1752    1720    explorer.exe    0×821b2020      22      520     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1900    1752    SharedIntApp.ex 0×822b96c0      3       75      0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1908    1752    prl_cc.exe      0×820ee580      14      133     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1936    1752    jusched.exe     0×8212ada0      1       43      0       False   2010-09-02 12:25:26.000000 UTC  N/A     Disabled
364     744     svchost.exe     0×82129370      4       88      0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
472     744     jqs.exe 0×82089558      5       146     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
488     744     sqlservr.exe    0×8208abf0      25      306     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
572     744     coherence.exe   0×82077da0      4       51      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
436     744     prl_tools_servi 0×82189530      3       78      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
632     436     prl_tools.exe   0×82086798      9       107     0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
```

```
menna@kali: ~
File  Actions  Edit  View  Help
1140    744     svchost.exe     0×821521b0      6       81      0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1192    744     svchost.exe     0×8214f488      13      175     0       False   2010-09-02 12:25:23.000000 UTC  N/A     Disabled
1436    744     iscsiexe.exe    0×8221e278      6       78      0       False   2010-09-02 12:25:24.000000 UTC  N/A     Disabled
1616    744     spoolsv.exe     0×82095500      13      140     0       False   2010-09-02 12:25:24.000000 UTC  N/A     Disabled
1752    1720    explorer.exe    0×821b2020      22      520     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1900    1752    SharedIntApp.ex 0×822b96c0      3       75      0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1908    1752    prl_cc.exe      0×820ee580      14      133     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
1936    1752    jusched.exe     0×8212ada0      1       43      0       False   2010-09-02 12:25:26.000000 UTC  N/A     Disabled
364     744     svchost.exe     0×82129370      4       88      0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
472     744     jqs.exe 0×82089558      5       146     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
488     744     sqlservr.exe    0×8208abf0      25      306     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
572     744     coherence.exe   0×82077da0      4       51      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
436     744     prl_tools_servi 0×82189530      3       78      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
632     436     prl_tools.exe   0×82086798      9       107     0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
660     744     sqlwriter.exe   0×821aa7e8      4       84      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
2180    1084    wscntfy.exe     0×8213dda0      3       48      0       False   2010-09-02 12:25:41.000000 UTC  N/A     Disabled
2588    744     alg.exe 0×81e8a368      6       107     0       False   2010-09-02 12:25:44.000000 UTC  N/A     Disabled
940     1084    wuauclt.exe     0×8205dda0      4       126     0       False   2010-09-02 12:26:40.000000 UTC  N/A     Disabled
2972    1752    ImmunityDebugge 0×82001ad0      2       87      0       False   2010-09-08 19:14:36.000000 UTC  N/A     Disabled
2204    2972    nifek_locked.ex 0×8207bda0      2       38      0       False   2010-09-08 19:14:36.000000 UTC  N/A     Disabled
1932    1752    ImmunityDebugge 0×82282380      2       86      0       False   2010-09-08 19:23:02.000000 UTC  N/A     Disabled
952     1932    vaelh.exe       0×8223c020      2       40      0       False   2010-09-08 19:23:02.000000 UTC  N/A     Disabled
3788    1752    ImmunityDebugge 0×81ffb6d8      2       103     0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
3508    3788    anaxu.exe       0×8219e5c8      2       54      0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
3984    1084    wuauclt.exe     0×81eab2f8      8       325     0       False   2010-09-09 19:52:45.000000 UTC  N/A     Disabled
2404    1752    ImmunityDebugge 0×82066478      2       85      0       False   2010-09-09 19:56:19.000000 UTC  N/A     Disabled
3772    2404    b98679df6defbb3 0×81f4bb28      1       46      0       False   2010-09-09 19:56:19.000000 UTC  N/A     Disabled
3276    3772    ihah.exe        0×81e87da0      1       45      0       False   2010-09-09 19:56:32.000000 UTC  N/A     Disabled
3768    1084    rundll32.exe    0×82311648      1       53      0       False   2010-09-09 19:56:33.000000 UTC  N/A     Disabled
```

Immunity Debugger Processes (ImmunityDebugge):

- These processes (e.g., ImmunityDebugge with child processes like nifek_locked.exe, vaelh.exe, anaxu.exe, ihah.exe) are potentially malicious. Immunity Debugger is a popular debugger used in reverse engineering and analysis of malware. If these processes are running on an infected machine, they could indicate the presence of malware being debugged or analyzed, which is a sign of the malware's operation or testing phase.

Suspicious Executables (e.g., nifek_locked.exe, vaelh.exe, anaxu.exe, ihah.exe):

- These processes do not appear to be legitimate Windows system processes. The names of these executables (e.g., nifek_locked.exe, vaelh.exe) are suspicious and could be custom or obfuscated names used by the Trojan to avoid detection. Such names are often associated with malware running on the system.

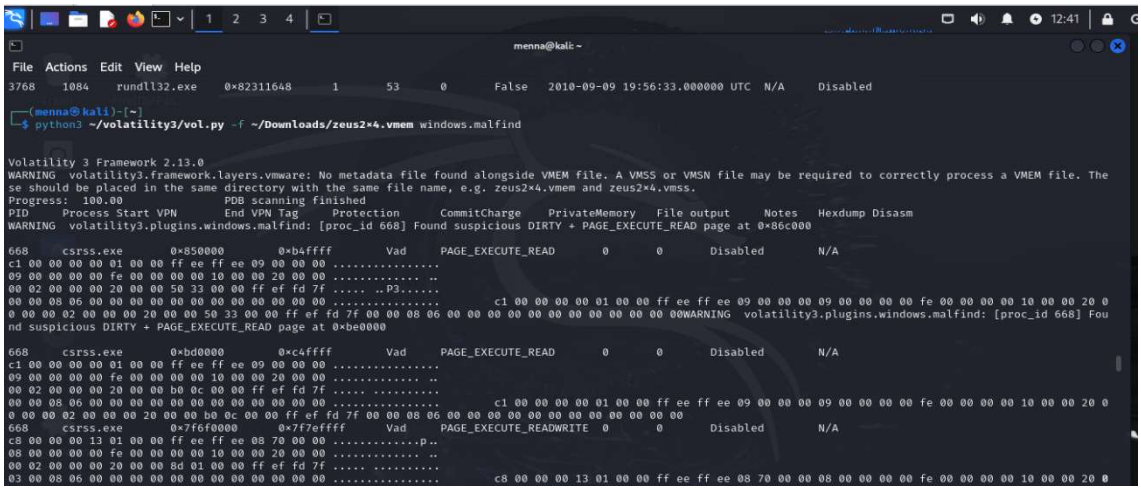
Rundll32.exe:

- The rundll32.exe process is a legitimate Windows process used to run DLL files. However, it is often abused by malware to execute malicious code from DLLs. In this case, if it is running from a suspicious location or executing a non-system DLL, it could be malicious.

High Number of Threads and Handles in Certain Processes:

- Some processes like svchost.exe have a large number of threads and handles. While svchost.exe is a legitimate process, malware often hijacks this process for persistence or to run malicious code. The fact that multiple instances of svchost.exe are running may warrant closer inspection.

-identify injected processes



Key Elements of the Output:

1. **DIRTY + PAGE_EXECUTE_READ**:
    - **DIRTY**: This means that the memory page has been modified after it was loaded. It's not in its original state, suggesting it has been altered or injected with new code.
    - **PAGE_EXECUTE_READ**: This means the memory page is both **readable** and **executable**. This is a key flag because code that can execute from a page like this is commonly used by malicious software to run injected code (e.g., malware exploits).

- Analyze Zeus-related network connections.

```
┌──(menna㉿kali)-[~/volatility]
└─$ python2 vol.py -f ~/Downloads/zeus2x4.vmem --profile=WinXPSP3x86 connscan

Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x020f5410 10.211.55.5:1427         65.54.81.89:80            1084
0x02125008 10.211.55.5:1423         207.46.21.123:80          1084
0x022ace08 10.211.55.5:1432         193.43.134.14:80          1752
```

-The **connscan** plugin scans memory for network connections and will help identify all active TCP/UDP connections, including those made by the Zeus Trojan for C&C communication.
-10.211.55.5 is the local IP address.
- local machine is connected to a remote server at IP 65.54.81.89, 207.46.21.123:80 and 193.43.134.14:80.

```
File  Actions  Edit  View  Help

┌──(menna㉿kali)-[~/volatility]
└─$ python2 vol.py -f ~/Downloads/zeus2x4.vmem --profile=WinXPSP3x86 connections

Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x822ace08 10.211.55.5:1432         193.43.134.14:80          1752
```

The output shows:
Local Address: IP and port on the local machine.(10.211.55.5)
Remote Address: IP and port of the external machine(193.43.134.14).
PID: Process ID of the process using the connection.

```
┌──(menna㉿kali)-[~/volatility]
└─$ python2 vol.py -f ~/Downloads/zeus2x4.vmem --profile=WinXPSP3x86  sockets

Volatility Foundation Volatility Framework 2.6.1
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -------------
0x81f0cc90     1192   1900     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x820046e0      756    500     17 UDP             0.0.0.0         2010-09-02 12:25:37 UTC+0000
0x81e7c548        4    139      6 TCP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x81f358f0     1752  16441      6 TCP             0.0.0.0         2010-09-09 19:56:32 UTC+0000
0x821715f8        4    445      6 TCP             0.0.0.0         2010-09-02 12:25:18 UTC+0000
0x82154e98      992    135      6 TCP             0.0.0.0         2010-09-02 12:25:22 UTC+0000
0x81e7e458        4    137     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x81eafe98     2588   1033      6 TCP             127.0.0.1       2010-09-02 12:25:44 UTC+0000
0x82078798      756      0    255 Reserved        0.0.0.0         2010-09-02 12:25:37 UTC+0000
0x8223fb90     1084    123     17 UDP             127.0.0.1       2010-09-09 19:52:48 UTC+0000
0x81eea480        4    138     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x820596d0     1084    123     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x8205ae98     1752   1432      6 TCP             0.0.0.0         2010-09-09 19:56:34 UTC+0000
0x81e7ed30     1192   1900     17 UDP             127.0.0.1       2010-09-09 19:52:48 UTC+0000
0x81ffdb18      756   4500     17 UDP             0.0.0.0         2010-09-02 12:25:37 UTC+0000
```

The sockets command revealed multiple active connections over ports such as 1900, 16444, 445, which could indicate Zeus-related activity.
Suspicious UDP and TCP traffic from processes like PID 1192 and 1752 suggested communication to external servers potentially linked to data exfiltration.

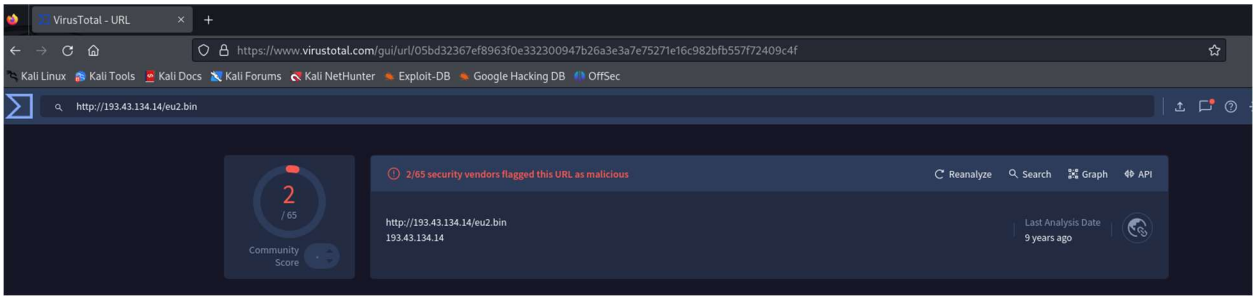
The network connections identified in the memory analysis reveal that the infected VM was actively communicating with external servers over common HTTP ports (port 80), a tactic used by Zeus to send stolen data to C2 servers.
The use of specific ports and external IP addresses can be directly correlated with Zeus malware activity, confirming the malware's presence and its external communication.
Multiple suspicious connections suggest that Zeus was attempting to exfiltrate data or communicate with a malicious server.

11. Detect Zeus Using Yara Rules

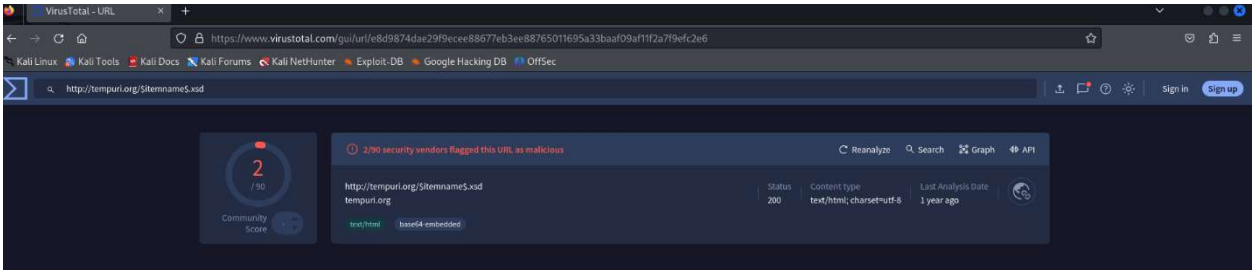
1. Extract urls from “zeus2x4.vmem”

```
┌──(kali㉿kali)-[~]
└─$ strings ~/Downloads/zeus2x4.vmem| grep -Eo 'https?://[^ ]+'
http://ocsp.verisign.com0
http://crl.verisign.com/tss-ca.crl0
http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl0O
http://www.microsoft.com/pki/certs/CodeSignPCA2.crt0
http://office.microsoft.com
http://+:80/Temporary_Listen_Addresses/
http://cdn.eyewonder.com/100125/760579/1206329/bannerInc.js"></scr'+'ipt>');
http://www.hardware-update.com
http://auth.immunityinc.com/ImmunityDebugger/ID_auth.py
http://auth.immunityinc.com/immauth.html
http://auth.immunityinc.com/ImmunityDebugger/ID_auth.py
http://auth.immunityinc.com/immauth.html
http://auth.immunityinc.com/immauth.html
http://auth.immunityinc.com/ImmunityDebugger/ID_reg.py
http://a
http://home.netscape.com/NC-rdf#"
http://www.w3.org/1999/02/22-rdf-syntax-ns#">
http://www.w3.org/1999/02/22-rdf-syntax-ns#"
http://home.netscape.com/NC-rdf#"
http://www.w3.org/1999/02/22-rdf-syntax-ns#">
http://dl.javafx.com/javafx-cache.jnlp
http://dl.javafx.com/1.3/javafx-rt.jnlp
http://www.w3.org/xmlns/2000/
http://schemas.xmlsoap.org/wsdl/soap/
http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20Secure%20Server%20Authority(8).crl
http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20Secure%20Server%20Authority(8).crl
```

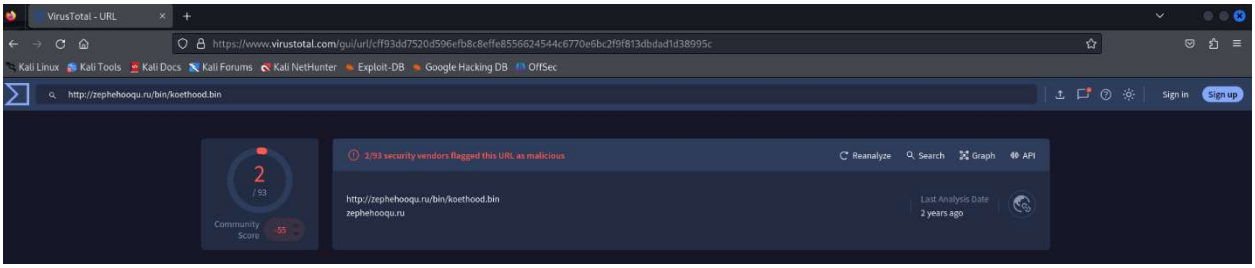
2. Detect suspicious URLs using virustotal
    - http://193.43.134.14/eu2.bin



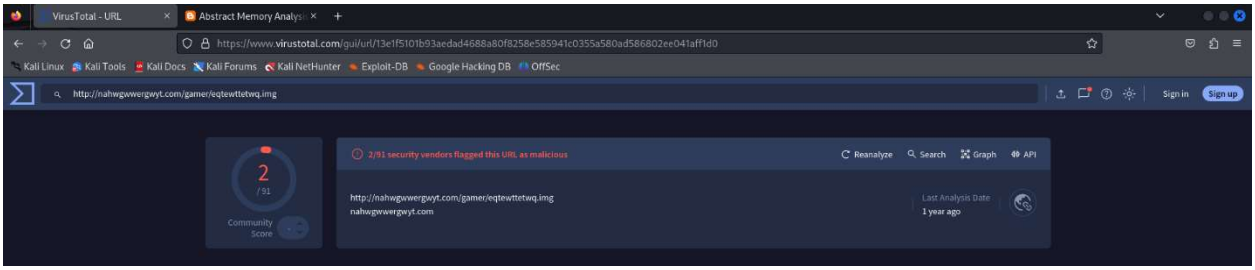
    - http://tempuri.org/$itemname$.xsd



- http://zephehooqu.ru/bin/koethood.bin

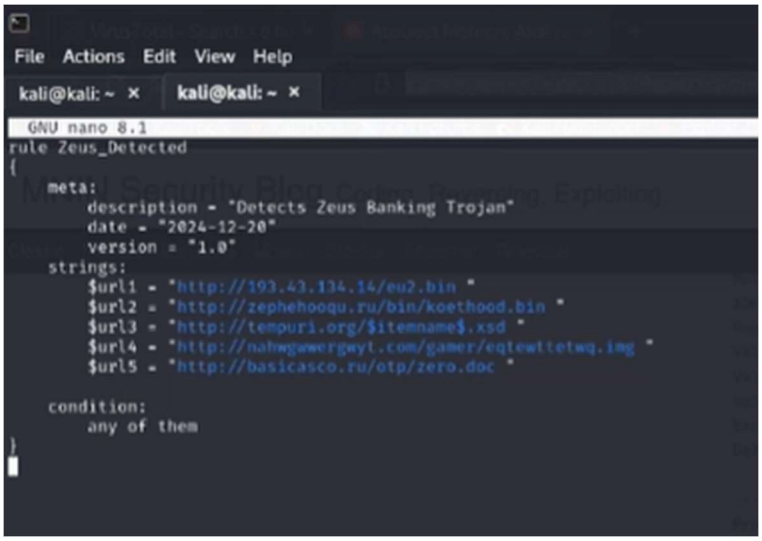


- http://nahwgwwergwyt.com/gamer/eqtewttetwq.img



- http://basicasco.ru/otp/zero.doc -> Zeus Related
  References: http://mnin.blogspot.com/2011/09/abstract-memory-analysis-zeus.html

3. Create Yara Rules



4. Test Yara Rules