

Proactive Security

Zeus Trojan

Department: Cybersecurity

Presented by:

Walaa Ahmed (2206192)

Youstina Malak (2206199)

Seif Ahmed (2206215)

Ahmed Adel (2206194)

Introduction:

This report demonstrates the process of detecting the Zeus malware using various tools, including Suricata, Splunk, Volatility, and YARA. Each step is elaborated to explain its purpose, execution, and expected alerts.

Step 1: Setting Up the Environment

1. Kali Linux Machine:

- Install **Suricata** and **Wireshark** on the Kali Linux machine to analyze network traffic and detect malicious activities.

2. Windows 10 Machine:

- Install the Zeus malware's zip file
- Disable **Windows Defender**, **antivirus software**, and the **firewall** to prevent the automatic removal of the malicious file.

3. Network Configuration:

- Both machines must be on the same **NAT network** (192.168.111.0), ensuring they can communicate without external interference.

Purpose: This setup creates a secure, controlled environment to observe and analyze malware behavior without risking external contamination.

Step 2: Analyzing Traffic Using Wireshark

1. IP Address Identification:

- Retrieve the IP address of the Windows machine to focus network
- analysis on its traffic using ipconfig in CMD.

2. Traffic Capture:

- Start live traffic capture on the infected VM's by selecting the appropriate network interface.
- Apply a filter using the Windows machine's IP address to isolate its traffic.

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.111.145

No.	Time	Source	Destination	Protocol	Length Info
1	0 000000000	192.168.111.145	192.168.111.2	NBNS	110 Refresh NB MSEdgeWIN10<00>
2	1.514363142	192.168.111.145	192.168.111.2	NBNS	110 Refresh NB MSEdgeWIN10<00>
3	3.046704637	192.168.111.145	192.168.111.2	NBNS	110 Refresh NB MSEdgeWIN10<00>
6	17.369829983	192.168.111.145	23.12.142.221	TCP	60 50008 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
8	17.371338168	192.168.111.145	23.12.142.221	TCP	66 50009 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10	17.439859542	192.168.111.145	23.12.142.221	TCP	60 50008 → 80 [ACK] Seq=2 Ack=2 Win=65535 Len=0
12	17.444707998	192.168.111.145	23.12.142.221	TCP	60 50009 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
13	17.444708218	192.168.111.145	23.12.142.221	HTTP	235 GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z HTTP/1.1
15	20.904833361	192.168.111.145	23.12.142.221	TCP	60 50009 → 80 [RST, ACK] Seq=182 Ack=1 Win=0 Len=0
19	34.699835442	192.168.111.145	8.8.8.8	DNS	73 Standard query 0x3338 A j.maxmind.com
21	35.354736021	192.168.111.145	85.114.128.127	DNS	62 Unknown operation (13) 0xfd70[Malformed Packet]
22	35.355036931	192.168.111.145	85.114.128.127	DNS	62 Unknown operation (13) 0xfd70[Malformed Packet]
23	35.356445676	192.168.111.145	85.114.128.127	DNS	62 Unknown operation (13) 0xfd70[Malformed Packet]
24	35.367175195	192.168.111.145	85.114.128.127	DNS	62 Unknown operation (13) 0xfd70[Malformed Packet]
25	37.935452703	192.168.111.145	85.114.128.127	DNS	62 Unknown operation (13) 0xfd70[Malformed Packet]
26	39.107362644	192.168.111.145	85.114.128.127	DNS	62 Unknown operation (13) 0xfd70[Malformed Packet]
27	39.255579984	192.168.111.145	192.168.111.2	DNS	85 Standard query 0x0a0a A fpdownload.macromedia.com
29	39.500981003	192.168.111.145	23.12.142.221	TCP	66 50010 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
31	40.500981003	192.168.111.145	23.12.142.221	TCP	66 50011 → 80 [SYN, ACK] Seq=1 Win=65535 Len=0

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0, id 0 0000 00 50 56 fa 38 c8 00 0c 29 37 f0 35 08 00 45 00 PV:8...)7.5... E...
Ethernet II, Src: VMware_37:f0:35 (00:0c:29:37:f0:35), Dst: VMware_fa:38:c8 (00:50:56:fa:38:00) 0010 00 60 9a 2c 00 00 80 11 40 7c c0 a8 6f 91 c0 a8 ... , ..., @|... o...
Internet Protocol Version 4, Src: 192.168.111.145, Dst: 192.168.111.2 0020 6f 02 00 89 00 89 00 4c 1c c2 e4 de 40 00 00 01 o... L... @...
User Datagram Protocol, Src Port: 137, Dst Port: 137 0030 00 00 00 00 00 01 20 45 4e 46 44 45 46 45 45 45 E NFDEEE
NetBIOS Name Service 0040 48 45 46 46 48 45 4a 45 4f 44 42 44 41 43 41 43 HEFFHEJE ODBDACAC
0050 41 43 41 43 41 41 00 00 20 00 01 c0 0c 00 20 ACACAAA...
0060 00 01 00 04 03 00 00 06 60 00 c0 a8 6f 91 ... , ... , 0...

3. Analyzing Captured Traffic:

Observations:

1. Destination IP: 85.114.128.127 (This IP has been flagged as malicious in threat intelligence databases, commonly linked to C2 activities or malware distribution)

2. Protocol:

- DNS: The infected machine likely resolves the domain associated with this IP.
- TCP: A persistent TCP connection is observed, indicating active communication between the infected machine and the C2 server.

3. HTTP: Request with GET method and

/get/flashplayer/update/current/install_all_win_cab_64_ax_sgn.z url.

1. This HTTP request appears to download a malicious file, disguised as a legitimate Flash Player update which a common tactic used by Zeus malware to deliver updates or additional payloads to the infected machine.

4. Indicators of Compromise (IOCs): Malicious IP(85.114.128.127) Malicious

Domain(Resolved by DNS traffic) URI Pattern

(/get/flashplayer/update/current/install_all_win_cab_64_ax_sgn.z)

Step 3: Malware Detection Using Suricata

1. Custom Rule Creation:

- Create a custom Suricata rule to detect the suspicious tcp and Dns requests or other malicious traffic patterns observed in Wireshark:

```
(kali㉿kali)-[~/etc/suricata/rules]
$ cat zeus2
alert http $HOME_NET any → $EXTERNAL_NET any (msg:"Fake Flash Player Update Request"; http.uri; content:"/get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z"; http.method; content:"GET"; no
case; sid:1000001; rev:1;)

alert http $HOME_NET any → $EXTERNAL_NET any (msg:"Suspicious Flash Player"; http.user_agent; content:"Flash Player Seed/3.0"; nocase; sid:1000002; rev:1;)

alert udp any any → 85.114.128.127 any (msg:"Malicious IP detected in UDP traffic"; sid:100004; rev:1; classtype:bad-unknown; metadata:service udp; reference:url,example.com; threshold: type limit, track by_sr
c, count 1, seconds 60;)
```

- Save the rule in /etc/suricata/rules/zeus2.

Explanation of Rules:

1. HTTP Rule:

- Triggers an alert when the specified GET request is observed by Matching the specific URI string.

2. DNS Rule:

- Flags DNS queries to known malicious domains by Inspecting DNS queries for malicious indicators that Matches against a specific domain string

Purpose: These rules provide real-time alerts, enabling analysts to identify and act on Zeus-related activity.

2. Suricata Configuration:

- Edit the suricata.yaml configuration file to:

```
(kali㉿kali)-[~]
$ sudo nano /etc/suricata/suricata.yaml
```

- Define the home network as the Windows VM's IP address.

```

vars:
# more specific is better for alert accuracy and performance
address-groups:
  HOME_NET: "[192.168.111.145]"
#HOME_NET: "[192.168.111.145]"
#HOME_NET: "any"

EXTERNAL_NET: "!$HOME_NET"
#EXTERNAL_NET: "any"

HTTP_SERVERS: "$HOME_NET"
SMTP_SERVERS: "$HOME_NET"
SQL_SERVERS: "$HOME_NET"
DNS_SERVERS: "$HOME_NET"
TELNET_SERVERS: "$HOME_NET"
AIM_SERVERS: "$EXTERNAL_NET"
DC_SERVERS: "$HOME_NET"
DNP3_SERVER: "$HOME_NET"
DNP3_CLIENT: "$HOME_NET"
MODBUS_CLIENT: "$HOME_NET"

```

- Set the monitored interface to eth0.

```

# Linux high speed capture support
af-packet:
- interface: eth0
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid, AF_PACKET will load balance packets based on flow.
  cluster-id: 106
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
  # This is only supported for Linux kernel > 3.1
  # possible value are:
  # * cluster_flow: all packets of a given flow are sent to the same socket
  # * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
  # * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
  #   socket. Requires at least Linux 3.14.
  # * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.rst for
  #   more info.
  # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
  # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)

```

- Link the custom rule file in the rules-file section.

```

default-rule-path: /home/kali/Downloads/zeus
rule-files:
# - /var/lib/suricata/rules/suricata.rules
- /etc/suricata/rules/zeus2

```

- Ensure there are no syntax errors in the configuration.

```

(kali㉿kali)-[~]
$ sudo suricata -T -c /etc/suricata/suricata.yaml

Info: conf-yaml-loader: Configuration node 'types' redefined.
i: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
i: suricata: Configuration provided was successfully loaded. Exiting.

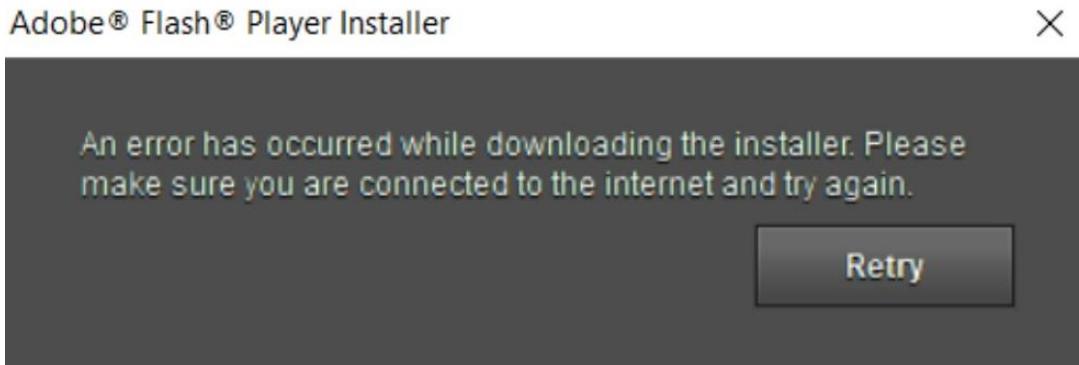
```

3. Run Suricata on the specified interface

```
(kali㉿kali)-[~/etc/suricata/rules]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
SELECTED FIELDS
Info: conf-yaml-loader: Configuration node 'types' redefined.
i: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 4 FM: 1 FR: 1   Engine started.
```

4. Running the Malware:

- Extract and execute the Zeus zip file on the Windows VM. Suricata should now detect the malware's activity.



5. Log Analysis:

- Check the fast.log file for alerts generated by Suricata:

```
(kali㉿kali)-[~]
└─$ tail -f /var/log/suricata/fast.log
12/19/2024-15:13:35.259000 [**] [1:1001001:1] Zeus Trojan: Outbound traffic to malicious IP [**] [Classification: (null)] [Priority: 3] {UDP} 192.168.111.144:62408 → 85.114.128.127:53
12/19/2024-16:06:42.802735 [**] [1:5000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:50904 → 23.12.142.221:80
12/19/2024-16:06:42.802735 [**] [1:7000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:50904 → 23.12.142.221:80
12/19/2024-16:06:46.088476 [**] [1:5000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:50904 → 23.12.142.221:80
12/19/2024-16:06:46.088476 [**] [1:7000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:50904 → 23.12.142.221:80
12/19/2024-16:06:46.088476 [**] [1:7000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:50904 → 23.12.142.221:80
12/19/2024-16:06:46.088476 [**] [1:1000004:1] Malicious IP detected in UDP traffic [**] [Classification: Potentially Bad Traffic] [Priority: 3] {UDP} 192.168.111.144:61086 → 85.114.128.127:53
12/19/2024-16:06:46.088476 [**] [1:1000004:1] Malicious IP detected in UDP traffic [**] [Classification: Potentially Bad Traffic] [Priority: 3] {UDP} 192.168.111.144:61086 → 85.114.128.127:53
12/19/2024-16:59:58.945940 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 → 23.12.142.221:80
12/19/2024-17:00:06.765445 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 → 23.12.142.221:80
12/19/2024-17:00:06.765445 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 → 23.12.142.221:80
```

Step 4: Forwarding logs :

A) Configure suricata.yaml

- The suricata.yaml configuration file was modified to enable log forwarding to both eve.json and fast.log. The eve.json file provides detailed JSON-formatted logs, while fast.log delivers concise alert summaries

```
# overridden with the -l command line parameter.
default-log-dir: /var/log/suricata/

# Global stats configuration
stats:
  enabled: yes
  # The interval field (in seconds) controls the interval at
  # which stats are updated in the log.
  interval: 8
  # Add decode events to stats.
  #decoder-events: true
  # Decoder event prefix in stats. Has been 'decoder' before, but that leads
  # to missing events in the eve.stats records. See issue #2225.
  #decoder-events-prefix: "decoder.event"
  # Add stream events as stats.
  #stream-events: false

# Plugins -- Experimental -- specify the filename for each plugin shared object
plugins:
#  - /path/to/plugin.so

# Configure the type of alert (and other) logging you would like.
outputs:
  # a line based alerts log similar to Snort's fast.log
  - fast:
      enabled: yes
      filename: fast.log
      append: yes
      filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'

  # Extensible Event Format (nicknamed EVE) event log in JSON format
  - eve-log:
      enabled: yes
      filetype: regular #regular/syslog/unix_dgram/unix_stream/redis
      filename: eve.json
      types:
        - alert
        - dns
        - http
        - tls
        - ssh
      # Enable for multi-threaded eve.json output; output files are amended with
      # an identifier, e.g., eve.9.json
```

- These logs are subsequently forwarded to the Splunk instance for centralized monitoring and analysis. This setup ensures comprehensive visibility into network and security events.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links like 'splunk>enterprise', 'Apps', 'Admin...', 'Messages' (with a notification count of 4), 'Settings', 'Activity', 'Help', and 'Open application menu'. Below the navigation is a progress bar with five steps: 'Select Source' (green dot), 'Set Source Type' (green dot), 'Input Settings' (green dot), 'Review' (green dot), and 'Done' (gray dot). To the right of the progress bar are buttons for '< Back' and 'Submit >'. The main content area is titled 'Review' and contains a table of configuration settings:

Input Type	File Monitor
Source Path	/var/log/suricata/eve.json
Continuously Monitor	Yes
Source Type	logs
App Context	launcher
Host	kali
Index	suricata200

B) Setting Up the Splunk Universal Forwarder

- The outputs.conf file was updated to direct logs to the Splunk monitoring server on the Kali machine with IP
- The inputs.conf file was configured to collect Windows Event Logs, specifically for the **Application**, **Security**, and **System** event sources:

[WinEventLog://Application]

disabled = 0

[WinEventLog://Security]

disabled = 0

[WinEventLog://System]

disabled = 0

- The configuration files are located at:

C:\Program Files\SplunkUniversalForwarder\etc\system\local

<input type="checkbox"/> inputs.conf	12/18/2024 9:09 PM	CONF File
<input type="checkbox"/> outputs.conf	12/18/2024 9:07 PM	CONF File

- The Splunk instance on Kali was configured to listen for incoming data on port 9997.

```
(kali㉿kali)-[~]
$ sudo ufw allow 9997/tcp
Licensing > Add new license
Skipping adding existing rule
Skipping adding existing rule (v6)
Add new license
(kali㉿kali)-[~]
$ sudo ufw status verbose
Status: active
To                         Action      From
--                         --          --
9997/tcp                   ALLOW IN   Anywhere
9997/tcp (v6)               ALLOW IN   Anywhere (v6)
```

Listen on this port	Status	Actions
9997	Enabled Disable	Delete

- The logs from the Windows machine successfully appeared in Splunk with sourcetype identifiers such as sourcetype="WinEventLog:System", confirming proper data ingestion.

Step 5: Monitoring and Observing Logs in Splunk:

A) Observing Suricata Alerts

- Analysis of Suricata alerts revealed two suspicious IP addresses originating from the victim machine. These alerts were extracted using custom Splunk searches and visualizations.

The screenshot shows a Splunk search interface titled "New Search". The search bar contains the query "index='suricata200' sourcetype='logs'". Below the search bar, it says "5 events (12/19/24 4:24:00.000 PM to 12/19/24 5:24:07.000 PM)" and "No Event Sampling". On the right, there are buttons for "Save As", "Create Table View", and "Close". The main area displays the search results with a "List" view selected. The results show five log entries, each with a timestamp, event details, and source information. The logs are as follows:

Time	Event
12/19/24 5:00:06.765 PM	12/19/2024-17:00:06.765445 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
12/19/24 5:00:06.765 PM	12/19/2024-17:00:06.765445 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
12/19/24 4:59:58.945 PM	12/19/2024-16:59:58.945940 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
12/19/24 4:59:58.945 PM	12/19/2024-16:59:58.945940 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
12/19/24 4:59:40.342 PM	12/19/2024-16:59:40.342652 [**] [1:100004:1] Malicious IP detected in UDP traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.111.144:61066 -> 85.114.128.127:53 host = kali source = /var/log/suricata/fast.log sourcetype = logs

The screenshot shows a Splunk search results table with the following data:

List	Format	20 Per Page
i	Time	Event
>	12/19/24 5:00:06.765 PM	12/19/2024-17:00:06.765445 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
>	12/19/24 5:00:06.765 PM	12/19/2024-17:00:06.765445 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
>	12/19/24 4:59:58.945 PM	12/19/2024-16:59:58.945940 [**] [1:1000002:1] Suspicious Flash Player [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
>	12/19/24 4:59:58.945 PM	12/19/2024-16:59:58.945940 [**] [1:1000001:1] Fake Flash Player Update Request [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.111.144:49766 -> 23.12.142.221:80 host = kali source = /var/log/suricata/fast.log sourcetype = logs
>	12/19/24 4:59:40.342 PM	12/19/2024-16:59:40.342652 [**] [1:100004:1] Malicious IP detected in UDP traffic [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.111.144:61066 -> 85.114.128.127:53 host = kali source = /var/log/suricata/fast.log sourcetype = logs

B) Investigating Suspicious IP Addresses

- The two identified IPs were queried in VirusTotal, revealing that one of them (85.114.128.127) is associated with DNS traffic on port 53. This activity strongly indicates that the Zeus Trojan on the victim machine is communicating with a malicious DNS server, indicative of **command-and-control (C2)** communication.

> 12/19/24 5:00:18.081 PM { [-]

```

    app_proto: failed
    dest_ip: 85.114.128.127
    dest_port: 53
    event_type: flow
    flow: { [+]
    }
    flow_id: 1930205852555330
    in_iface: eth0
    proto: UDP
    src_ip: 192.168.111.144
    src_port: 61073
    timestamp: 2024-12-19T17:00:18.081160-0500
}

```

[Show as raw text](#)

host = kali | source = /var/log/suricata/eve.json | sourcetype = logs

source="/var/log/suricata/eve.json" host="kali" index="suricata200" sourcetype="logs" dest_ip=85.114.128.127

Last 4 hours ▾ Q

1 event (12/20/24 4:15:00.000 AM to 12/20/24 8:15:32.000 AM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection ✖ Deselect 1 minute per column

Time	Event
12/20/24 4:21:58.711 AM	{ [-] alert: { [-] action: allowed category: Potentially Bad Traffic gid: 1 metadata: { [+] } rev: 1 severity: 2 signature: Malicious IP detected in UDP traffic signature_id: 100004 } app_proto: failed dest_ip: 85.114.128.127 dest_port: 53 direction: to_server event_type: alert flow: { [+] } }

Hide Fields All Fields

SELECTED FIELDS

- # host 1
- # source 1
- # sourcetype 1

INTERESTING FIELDS

- # alert.action 1
- # alert.category 1
- # alert.gid 1
- # alert.metadata.service[] 1
- # alert.rev 1
- # alert.severity 1
- # alert.signature 1
- # alert.signature_id 1
- # app_proto 1
- # date_hour 1
- # date_mday 1
- # date_minute 1

Σ http://85.114.128.127/ Sign in Sign up

1/90 security vendor flagged this URL as malicious

Rerunalyze Search Graph API

Last Analysis Date 1 year ago

Community Score 1 / 90

http://85.114.128.127/ 85.114.128.127 ip

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Fortinet	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

Do you want to automate checks?

C) Monitoring Windows Event Logs

- Comprehensive searches of Windows Event Logs were performed to detect anomalies. These logs provided critical insights into system events, security incidents, and application behavior.

The screenshot shows a log search interface with the following details:

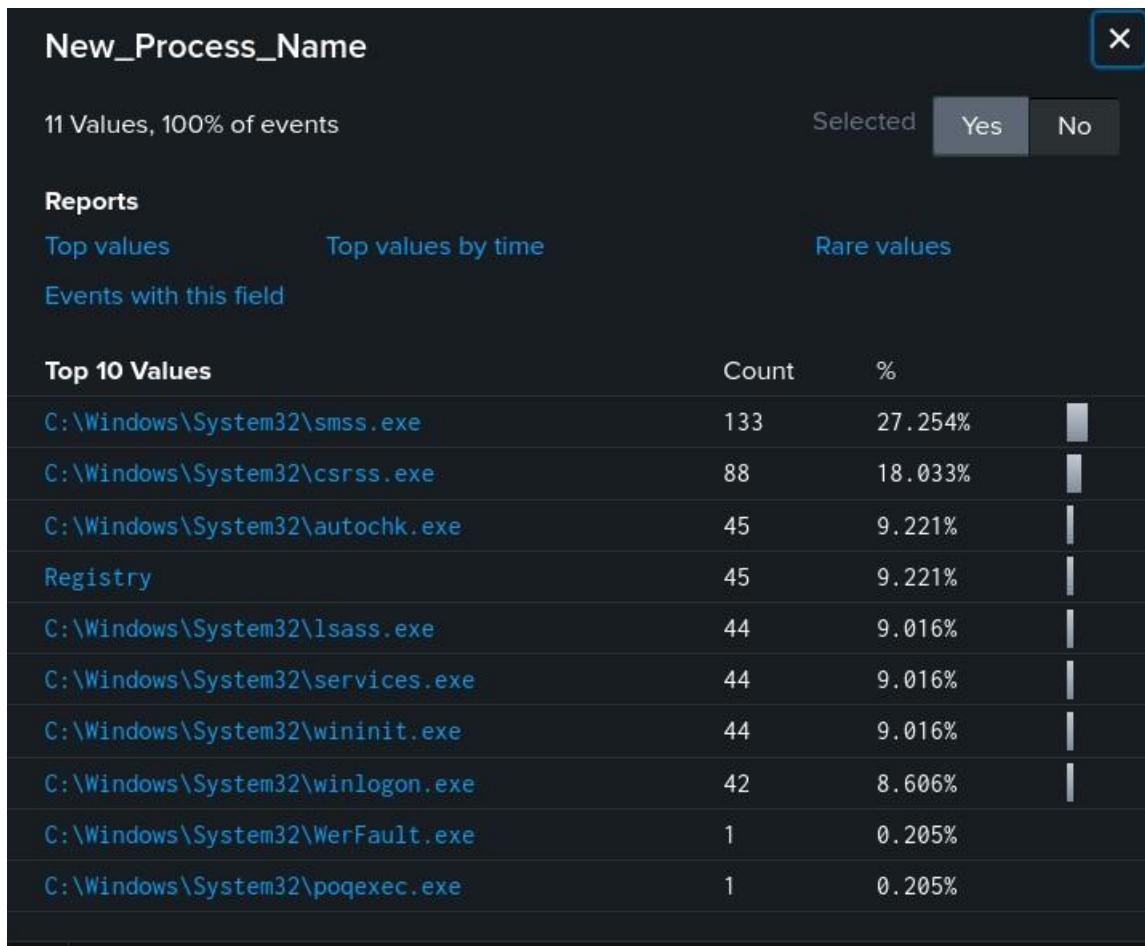
- Search Query:** source="WinEventLog:*
- Results Count:** 26,265 events (before 12/19/24 5:27:53.000 PM)
- Sampling:** No Event Sampling
- Time Range:** All time
- Buttons:** Save As, Create Table View, Close, Job, Verbose Mode

The main pane displays event logs in a table format:

S	i	Time	Event
>	12/19/24 8:39:18.000 AM	12/19/2024 05:39:18 AM	LogName=Security EventCode=4672 EventType=0 ComputerName=MSEdgeWIN10 Show all 31 lines host = MSEdgeWIN10 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/19/24 8:39:18.000 AM	12/19/2024 05:39:18 AM	LogName=Security EventCode=4624 EventType=0 ComputerName=MSEdgeWIN10 Show all 70 lines host = MSEdgeWIN10 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	12/19/24 8:38:55.000 AM	12/19/2024 05:38:55 AM	LogName=Security EventCode=4798 EventType=0 ComputerName=MSEdgeWIN10 Show all 27 lines host = MSEdgeWIN10 source = WinEventLog:Security sourcetype = WinEventLog:Security

D) Identifying New Processes:

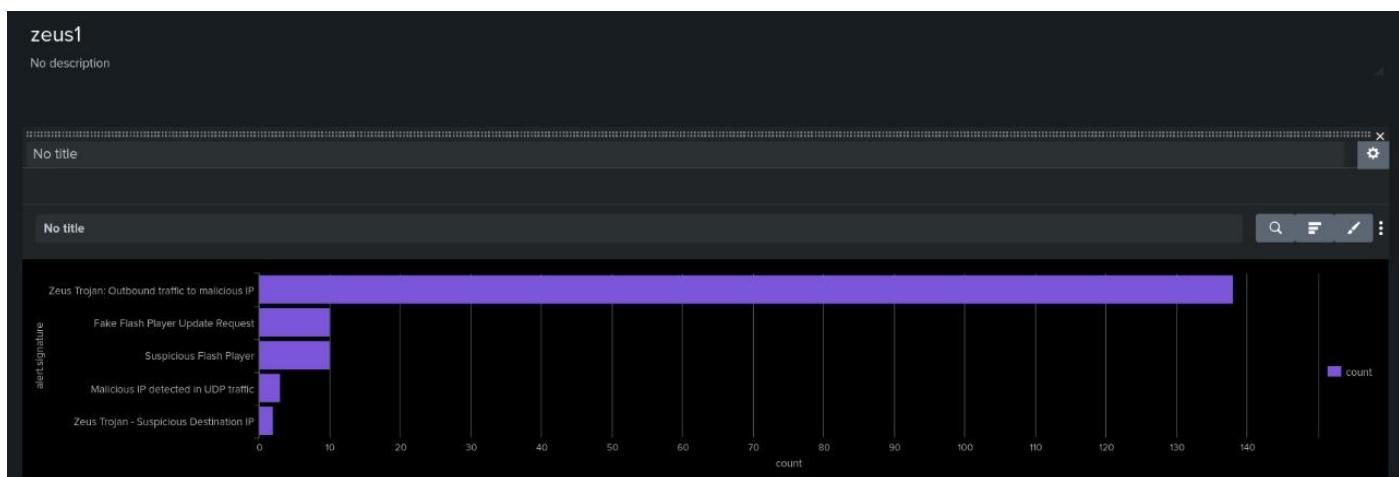
- Specific focus was given to identifying new processes spawned by the Zeus Trojan. These were detected by searching for Windows Event Log entries associated with process creation events (EventCode=4688).



E) Creating Zeus Dashboard :

A) Panel 1 : Displays the frequency of detected alerts, grouped by signature .

Query: `index=suricata200 sourcetype="logs" | stats count by alert.signature | sort -count`



B) Panel 2: Highlights IPs generating or receiving the most traffic.

Query: `index=suricata200 sourcetype="logs" | stats count by src_ip, dest_ip | sort -count`

src_ip	dest_ip	count
192.168.111.144	192.168.111.2	4949
192.168.111.129	169.254.169.254	3368
192.168.111.144	192.168.111.129	1671
192.168.111.129	192.168.111.2	788
192.168.111.144	85.114.128.127	411
fe80:0000:0000:0000:21fd:a625:1c7a:523d	ff02:0000:0000:0000:0000:0001:ff00:0001	344
192.168.111.1	224.0.0.252	339
fe80:0000:0000:0000:21fd:a625:1c7a:523d	ff02:0000:0000:0000:0000:0000:0001:0003	339
192.168.111.144	95.101.35.106	308
95.101.35.106	192.168.111.144	304

C) Panel 3: Tracks Zeus-related alerts over time.

Query: `index=suricata200 sourcetype="logs" alert.signature="Zeus" | timechart count by alert.signature`



D) Panel 4: Shows the trend of alerts over time.

Query: `index=suricata200 sourcetype="logs" | timechart count by alert.signature`

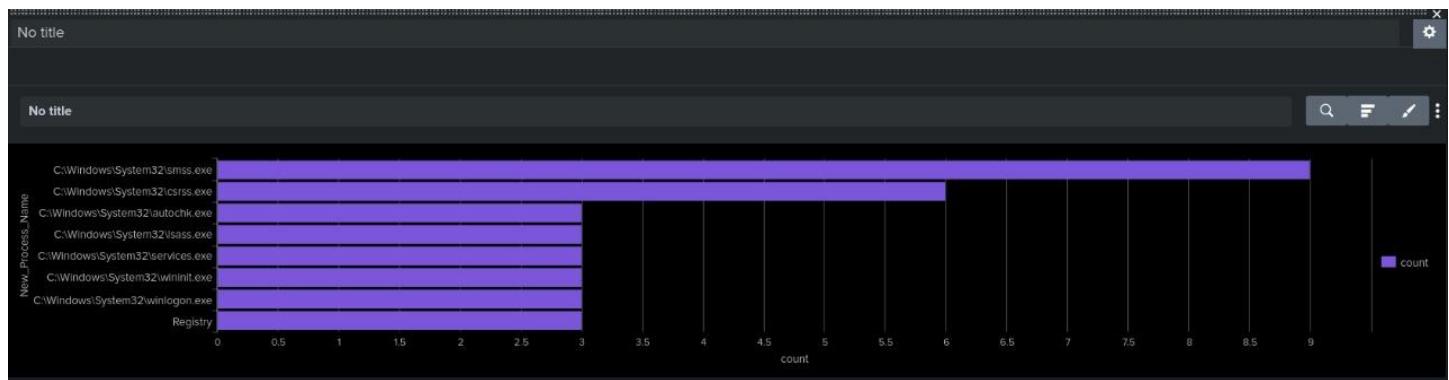


E) Panel 5 : Displays the frequency of detected processes, grouped by new_process .

Query: `sourcetype="WinEventLog:Security" EventCode=4688`

`| stats count by New_Process_Name`

`| sort-count`



Step 6: Analyzing the Memory Dump Using Volatility:

We will analyze a memory dump from a potentially compromised system using the Volatility framework. The memory image, **zeus2x4.vmem**, is analyzed to identify malicious processes and their characteristics.

The analysis will include the identification of running processes, network connections, and the extraction of executable files from memory.

1. Image Information:

First, we gather information about the memory image to determine the appropriate profile to use for analysis.

```
[seif@final] -[~/volatility]
$ python2 vol.py -f ..Downloads/zeus2x4.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
INFO    : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                      AS Layer1 : IA32PagedMemory (Kernel AS)
                      AS Layer2 : FileAddressSpace (/home/seif/Downloads/zeus2x4.vmem)
                      PAE type : No PAE
                        DTB : 0x39000L
                        KDBG : 0x8054cde0L
Number of Processors : 1
Image Type (Service Pack) : 3
          KPCR for CPU 0 : 0xffffd000L
          KUSER_SHARED_DATA : 0xffffdf0000L
Image date and time : 2010-09-09 19:56:54 UTC+0000
Image local date and time : 2010-09-09 15:56:54 -0400
```

The output suggests two possible profiles: **WinXPSP2x86** and **WinXPSP3x86**. We will use **WinXPSP2x86** for our subsequent analysis.

2. Process Listing:

Next, we list all running processes in the memory image to identify any suspicious activity.

```
python2 vol.py -f ..../Downloads/zeus2x4.vmem --profile WinXPSP2x86 pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0x823c8a00	System	4	0	57	671	——	0	
0x82292da0	smss.exe	596	4	3	19	——	0	2010-09-02 12:25:18 UTC+0000
0x821f2978	csrss.exe	668	596	14	471	0	0	2010-09-02 12:25:21 UTC+0000
0x822c09f8	winlogon.exe	692	596	21	588	0	0	2010-09-02 12:25:22 UTC+0000
0x821a5da0	services.exe	744	692	15	279	0	0	2010-09-02 12:25:22 UTC+0000
0x822c8798	lsass.exe	756	692	24	437	0	0	2010-09-02 12:25:22 UTC+0000
0x82150b90	svchost.exe	912	744	20	202	0	0	2010-09-02 12:25:22 UTC+0000
0x822c8bf8	svchost.exe	992	744	10	277	0	0	2010-09-02 12:25:22 UTC+0000
0x82151da0	svchost.exe	1084	744	58	1327	0	0	2010-09-02 12:25:22 UTC+0000
0x821521b0	svchost.exe	1140	744	6	81	0	0	2010-09-02 12:25:22 UTC+0000
0x8214f488	svchost.exe	1192	744	13	175	0	0	2010-09-02 12:25:23 UTC+0000
0x8221e278	iscsieve.exe	1436	744	6	78	0	0	2010-09-02 12:25:24 UTC+0000
0x82095500	spoolsv.exe	1616	744	13	140	0	0	2010-09-02 12:25:24 UTC+0000
0x821b2020	explorer.exe	1752	1720	22	520	0	0	2010-09-02 12:25:25 UTC+0000
0x822b96c0	SharedIntApp.ex	1900	1752	3	75	0	0	2010-09-02 12:25:25 UTC+0000
0x820ee580	prl_cc.exe	1908	1752	14	133	0	0	2010-09-02 12:25:25 UTC+0000
0x8212ada0	jusched.exe	1936	1752	1	43	0	0	2010-09-02 12:25:26 UTC+0000
0x82129370	svchost.exe	364	744	4	88	0	0	2010-09-02 12:25:33 UTC+0000
0x82089558	jqs.exe	472	744	5	146	0	0	2010-09-02 12:25:33 UTC+0000
0x8208abf0	sqlservr.exe	488	744	25	306	0	0	2010-09-02 12:25:33 UTC+0000
0x82077da0	coherence.exe	572	744	4	51	0	0	2010-09-02 12:25:36 UTC+0000
0x82189530	prl_tools_servi	436	744	3	78	0	0	2010-09-02 12:25:36 UTC+0000
0x82086798	prl_tools.exe	632	436	9	107	0	0	2010-09-02 12:25:36 UTC+0000
0x821aa7e8	sqlwriter.exe	660	744	4	84	0	0	2010-09-02 12:25:36 UTC+0000
0x8213dda0	wscntfy.exe	2180	1084	3	48	0	0	2010-09-02 12:25:41 UTC+0000
0x81e8a368	alg.exe	2588	744	6	107	0	0	2010-09-02 12:25:44 UTC+0000
0x8205dda0	wuauctl.exe	940	1084	4	126	0	0	2010-09-02 12:26:40 UTC+0000
0x82001ad0	ImmunityDebugge	2972	1752	2	87	0	0	2010-09-08 19:14:36 UTC+0000
0x8207bda0	nifek_locked.ex	2204	2972	2	38	0	0	2010-09-08 19:14:36 UTC+0000
0x82282380	ImmunityDebugge	1932	1752	2	86	0	0	2010-09-08 19:23:02 UTC+0000
0x8223c020	vaelh.exe	952	1932	2	40	0	0	2010-09-08 19:23:02 UTC+0000
0x81ffb6d8	ImmunityDebugge	3788	1752	2	103	0	0	2010-09-08 22:39:40 UTC+0000
0x8219e5c8	anaxu.exe	3508	3788	2	54	0	0	2010-09-08 22:39:40 UTC+0000
0x81ebab2f8	wuauctl.exe	3984	1084	8	325	0	0	2010-09-09 19:52:45 UTC+0000
0x82066478	ImmunityDebugge	2404	1752	2	85	0	0	2010-09-09 19:56:19 UTC+0000
0x81f4bb28	b98679df6defbb3	3772	2404	1	46	0	0	2010-09-09 19:56:19 UTC+0000
0x81e87da0	ihah.exe	3276	3772	1	45	0	0	2010-09-09 19:56:32 UTC+0000
0x82311648	rundll32.exe	3768	1084	1	53	0	0	2010-09-09 19:56:33 UTC+0000

including **ImmunityDebugge**, **explorer.exe**, and others. Notably, we see processes with unusual names or those that are not typically found on a clean system, such as **ihah.exe** and **b98679df6defbb3**.

3. Process Tree:

To understand the parent-child relationships between processes, we can visualize the process tree.

```
(seif㉿final)-[~/volatility]
└─$ python2 vol.py -f .../Downloads/zeus2x4.vmem --profile WinXPSP2x86 pstrace
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
Name          Pid  PPid  Thds  Hnds  Time
-----  -----
0x821b2020:explorer.exe           1752  1720    22   520 2010-09-02 12:25:25 UTC+0000
. 0x82282380:ImmunityDebugge      1932  1752     2    86 2010-09-08 19:23:02 UTC+0000
.. 0x8223c020:vaelh.exe          952   1932     2    40 2010-09-08 19:23:02 UTC+0000
. 0x8212ada0:jusched.exe         1936  1752     1    43 2010-09-02 12:25:26 UTC+0000
. 0x82001ad0:ImmunityDebugge      2972  1752     2    87 2010-09-08 19:14:36 UTC+0000
.. 0x8207bda0:nife_k_locked.ex  2204   2972     2    38 2010-09-08 19:14:36 UTC+0000
. 0x81ffb6d8:ImmunityDebugge      3788  1752     2   103 2010-09-08 22:39:40 UTC+0000
.. 0x8219e5c8:anaxu.exe          3508   3788     2    54 2010-09-08 22:39:40 UTC+0000
. 0x820ee580:prl_cc.exe          1908  1752    14   133 2010-09-02 12:25:25 UTC+0000
. 0x82066478:ImmunityDebugge      2404  1752     2    85 2010-09-09 19:56:19 UTC+0000
.. 0x81f4bb28:b98679df6defbb3  3772   2404     1    46 2010-09-09 19:56:19 UTC+0000
... 0x81e87da0:ihah.exe          3276   3772     1    45 2010-09-09 19:56:32 UTC+0000
. 0x822b96c0:SharedIntApp.ex     1900  1752     3    75 2010-09-02 12:25:25 UTC+0000
```

The process tree reveals that ImmunityDebugge is a parent process to several other processes, including ihah.exe. This could indicate that ImmunityDebugge is being used as a debugger for malicious activities.

4. Network Connection:

Next, we check for any active network connections that may indicate communication with a command and control (C2) server.

```
(seif㉿final)-[~/volatility]
$ python2 vol.py -f .../Downloads/zeus2x4.vmem --profile WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)

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
```

```
(seif㉿final)-[~/volatility]
$ python2 vol.py -f .../Downloads/zeus2x4.vmem --profile WinXPSP2x86 connections
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)

Offset(V) Local Address           Remote Address         Pid
0x822ace08 10.211.55.5:1432    193.43.134.14:80   1752
```

The output shows several connections, including ip 193.43.134.14 with PID 1752 which is the PPID for the ImmunityDebugge .

5. Dumping Malicious Processes:

To analyze the contents of the suspicious processes, we can dump their executable files from memory.

```
(seif@final)-[~/volatility]
$ python2 vol.py -f .../Downloads/zeus2x4.vmem --profile WinXPSP2x86 procdump -p 2404 -D procdump
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
Process(V) ImageBase Name Result
0x82066478 0x00400000 ImmunityDebugge OK: executable.2404.exe
```

This command dumps the executable of the process with PID 2404 (identified as ImmunityDebugge). We repeat this for other suspicious processes:

- b98679df6defbb3

```
(seif@final)-[~/volatility]
$ python2 vol.py -f .../Downloads/zeus2x4.vmem --profile WinXPSP2x86 procdump -p 3772 -D procdump
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
Process(V) ImageBase Name Result
0x81f4bb28 0x00400000 b98679df6defbb3 OK: executable.3772.exe
```

- ihah.exe

```
(seif@final)-[~/volatility]
$ python2 vol.py -f ..../Downloads/zeus2x4.vmem --profile WinXPSP2x86 procdump -p 3276 -D procdump
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
Process(V) ImageBase Name Result
0x81e87da0 0x00400000 ihah.exe OK: executable.3276.exe
```

6. Analyzing Dumped Executables

After dumping the executables, we can calculate their SHA256 hashes to verify their integrity and check against known malware databases.

```
[seif@final] - [~/volatility]
$ sha256sum procdump/executable.2404.exe
66b6e5898e8ceed70e3e3e09c1c399cb51c5fbee4029a8aa5323de6bb0d506cc  procdump/executable.2404.exe

[seif@final] - [~/volatility]
$ sha256sum procdump/executable.3772.exe
9374b90433d9e2369258413997f3b84d2db0c51b8fd0d7e050458e780a141407  procdump/executable.3772.exe

[seif@final] - [~/volatility]
$ sha256sum procdump/executable.3276.exe
c4b88f8e160f9eb145bb9e12e5122fa539a83b772e93929efb8846c8e1171eed  procdump/executable.3276.exe
```

The hashes can be used to search for known malware signatures on VirusTotal.

- **ImmunityDebugge**

2 / 71 security vendors flagged this file as malicious

66b6e5898e8ceed70e3e09c1c399cb51c5fbee4029a8aa5323de6bb0d506cc
ImmDbg
peexe

Community Score: 2 / 71

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis				Do you want to automate checks?
Bkav Pro	W32.AIDetectMalware	Trapmine	Suspicious_low.mt.score	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected	
Alibaba	Undetected	ALYac	Undetected	
Antiy-AVL	Undetected	Arcabit	Undetected	
Avast	Undetected	AVG	Undetected	
Avira (no cloud)	Undetected	Baidu	Undetected	
BitDefender	Undetected	BitDefenderTheta	Undetected	
ClamAV	Undetected	CMC	Undetected	
CrowdStrike Falcon	Undetected	Cybereason	Undetected	

- **b98679df6defbb3**

58 / 73 security vendors flagged this file as malicious

9374b90433d9e2369258413997f3b84d2db0c51b8fd0d7e050458e780a141407
executable.3772.exe
peexe

Community Score: 1 / 73

DETECTION DETAILS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis				Do you want to automate checks?
Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Heur.Dreidel.lqW@wSEdjyh	
AegisLab	Trojan.Win32.Generic.41c	AhnLab-V3	Spyware/Win32.Zbot.R1109	
Alibaba	TrojanPSW:Win32.Generic.9463b213	ALYac	Gen:Heur.Dreidel.lqW@wSEdjyh	
Antiy-AVL	Trojan/Win32.AGeneric	Arcabit	Trojan.Dreidel.E27A3C	
Avast	SF:Crypt-BT [Trj]	AVG	SF:Crypt-BT [Trj]	
Avira (no cloud)	TR/Spy.Gen	BitDefender	Gen:Heur.Dreidel.lqW@wSEdjyh	
BitDefenderTheta	AI-Packer.C2IA06951E	Comodo	Malware@#1gmtrwjzbzr	
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.c136b4	
Cylance	Unsafe	Cyren	W32/Zbot.BR.genElderado	
DrWeb	BackDoor.Qbot.234	eGambit	Unsafe.AI_Score_85%	

- **ihah.exe**

51 / 64 security vendors flagged this file as malicious

c4b88f8e160f9eb145bb9e12e5122fa539a83b772e93929efb8846c8e1171eed
executable.3276.exe
peexe

Community Score: -80 / 64

DETECTION DETAILS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis				Do you want to automate checks?
Ad-Aware	Gen:Variant.Symmi.12682	AegisLab	Trojan.W32.Generic	
AhnLab-V3	Spyware/Win32.Zbot.R1109	ALYac	Gen:Variant.Symmi.12682	
Antiy-AVL	Trojan/Win32.AGeneric	Arcabit	Trojan.Symmi.D318A	
Avast	SF:Crypt-BT [Trj]	AVG	SF:Crypt-BT [Trj]	
Avira (no cloud)	TR/Spy.Gen	AVware	Trojan.Win32.GenericIBT	
Baidu	Win32.Trojan.WisdomEyes.16070401.950...	BitDefender	Gen:Variant.Symmi.12682	
ClamAV	Win.Malware.QBot.1530	Comodo	UnclassifiedMalware	
CrowdStrike Falcon	Malicious_confidence_100% (D)	Cylance	Unsafe	
Cyren	W32/Zbot.BR.genElderado	DrWeb	BackDoor.Qbot.234	
Emsisoft	Gen:Variant.Symmi.12682 (B)	Endgame	Malicious (High Confidence)	

7. Memory Analysis for Malicious Code:

To further analyze the memory for injected code or other malicious artifacts, we can use the malfind plugin.

- **ImmunityDebugge**

```
└─(seif㉿final)-[~/volatility]
$ python2 vol.py -f ~/Downloads/zeus2x4.vmem --profile WinXPSP2x86 malfind -p 2404
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug      : For best results please install distorm3
Process: ImmunityDebugge Pid: 2404 Address: 0x2340000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000002340000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x00000000002340010  b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00  ..@.....
0x00000000002340020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x00000000002340030  00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00  .....

Process: ImmunityDebugge Pid: 2404 Address: 0x32d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x000000000032d0000  b8 35 00 00 00 e9 a9 d1 63 79 68 6c 02 00 00 e9  .5.....cyhl....
0x000000000032d0010  b4 63 64 79 8b ff 55 8b ec e9 7c 11 54 79 8b ff  .cdy..U...|.Ty..
0x000000000032d0020  55 8b ec e9 01 32 f4 73 8b ff 55 8b ec e9 7c 60  U....2.s..U...|`.
0x000000000032d0030  ef 73 8b ff 55 8b ec e9 ca e9 ef 73 8b ff 55 8b  .s..U.....s..U.
```

- b98679df6defbb3

```
(seif㉿final)-[~/volatility]
└─$ python2 vol.py -f ~/Downloads/zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3772
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug : For best results please install distorm3
Process: b98679df6defbb3 Pid: 3772 Address: 0x380000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 36, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000380000 90 90 90 90 5a 89 e5 83 ec 14 8b 5d 00 83 eb 05 ....Z.....]....
0x0000000000380010 be 0b 88 01 00 29 f3 89 1c 24 b9 84 44 02 00 01 ....) ...$..D ...
0x0000000000380020 d9 8b 09 89 4c 24 0c b9 74 43 02 00 01 d9 8b 09 ....L$..tC.....
0x0000000000380030 89 4c 24 10 57 be 00 10 00 00 01 de b9 0b 78 01 .L$.W.....x.

Process: b98679df6defbb3 Pid: 3772 Address: 0x9a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000009a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x00000000009a0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
0x00000000009a0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x00000000009a0030 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 ......

Process: b98679df6defbb3 Pid: 3772 Address: 0xa30000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000a30000 b8 35 00 00 00 e9 a9 d1 ed 7b 68 6c 02 00 00 e9 .5.....{hl....
0x0000000000a30010 b4 63 ee 7b 8b ff 55 8b ec e9 7c 11 de 7b 8b ff .c.{ ..U... | ..{ ..
0x0000000000a30020 55 8b ec e9 01 32 7e 76 8b ff 55 8b ec e9 7c 60 U....2~v..U... |` ..
0x0000000000a30030 79 76 8b ff 55 8b ec e9 ca e9 79 76 8b ff 55 8b yv..U....yv..U.
```

- ihah.exe

```
└─(seif㉿final)─[~/volatility]
└─$ python2 vol.py -f ~/Downloads/zeus2x4.vmem --profile WinXPSP2x86 malfind -p 3276
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
WARNING : volatility.debug      : For best results please install distorm3
Process: ihah.exe Pid: 3276 Address: 0x380000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 37, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00000000000380000 90 90 90 90 5a 89 e5 83 ec 14 8b 5d 00 83 eb 05 .Z....].
0x00000000000380010 be 94 c2 00 00 29 f3 89 1c 24 b9 98 41 02 00 01 ..$..A...
0x00000000000380020 d9 8b 09 89 4c 24 0c b9 30 46 02 00 01 d9 8b 09 ..L$..0F...
0x00000000000380030 89 4c 24 10 57 be 00 10 00 00 01 de b9 94 b2 00 .L$.W.....
.

Process: ihah.exe Pid: 3276 Address: 0x3f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x000000000003f0000 b8 35 00 00 00 e9 a9 d1 51 7c 68 6c 02 00 00 e9 .5.....Q|hl...
0x000000000003f0010 b4 63 52 7c 8b ff 55 8b ec e9 7c 11 42 7c 8b ff .cR|..U...|.B|..
0x000000000003f0020 55 8b ec e9 01 32 e2 76 8b ff 55 8b ec e9 7c 60 U...2.v..U...|.
0x000000000003f0030 dd 76 8b ff 55 8b ec e9 ca e9 dd 76 8b ff 55 8b .v..U.....v..U.

Process: ihah.exe Pid: 3276 Address: 0x9a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 52, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x000000000009a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x000000000009a0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.
0x000000000009a0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x000000000009a0030 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 00 .....
```

The output shows suspicious memory regions associated with the process, including executable code that may not be part of the original executable.

- We can see that this process has MZ header and protection of PAGE_EXECUTE_READWRITE, which means that this memory region is marked as executable, and it can also be both read from and written to.
- This is unusual and suspicious because it allows an attacker to execute code from that memory region and also modify its content dynamically.
- In legit scenarios, memory regions won't be executable and writable at the same time.

Step 7: Detect Zeus with YARA Signatures:

First Create a Yara Rule file:

```
1 rule ZeusBanking_Detection {
2     meta:
3         author="Seif Ahmed"
4         description="A detection rule against ZuesBankingVersion_26Nov2013"
5     strings:
6         $file_name="invoice_2318362983713_823931342io.pdf.exe" ascii
7         // Suspected name of functions and DLL functionalities.
8         $function_name_KERNEL32_CreateFileA="CellrotoCrudUntohighCols" ascii
9         // PE Magic Byte.
10        $PE_magic_byte = "MZ"
11        // Hex String Function name.
12        $hex_string = {43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72}
13    condition:
14        $PE_magic_byte at 0 and $file_name
15        and $function_name_KERNEL32_CreateFileA
16        or $hex_string
17 }
```

Strings Section:

This section defines strings or patterns the rule looks for:

➤ \$file_name:

Detects a suspicious file name: "invoice_2318362983713_823931342io.pdf.exe".

- The ascii modifier ensures it's interpreted as plain text.
- The filename appears like a phishing or malicious document disguised as a PDF but is actually an executable (.exe).

➤ \$function_name:

- Matches a specific function name: "CellrotoCrudUntohighCols".
- This is likely a unique name associated with the Zeus Banking malware, possibly part of its internal code.

➤ \$PE_magic_byte:

- Matches the magic bytes { 4D 5A }, which represent "MZ" in hexadecimal.
- These bytes indicate the start of a Portable Executable (PE) file, common in Windows executables.
- The at 0 condition ensures this pattern is at the very beginning of the file, as expected in a valid PE file.

➤ \$hex_string:

- Matches a specific binary pattern in hexadecimal: { 43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72 }.
- This corresponds to the ASCII string "CameValeWauler".
- This might be a unique or uncommon string embedded in the malware for identification or functionality.

Condition Section:

The condition section specifies the logic for triggering the rule. This is the decision-making part of the rule.

➤ \$PE_magic_byte at 0:

- Ensures the file starts with MZ, confirming it is a Windows executable.

➤ \$file_name and \$function_name: Both must be present for a match.

➤ or \$hex_string: The hex string can trigger the rule on its own, without the file name or function name.

The overall logic:

- If the file is a valid PE file (MZ at the start), And if:

A known malicious file name (\$file_name) is present and a specific function name (\$function_name) is found, OR a unique binary pattern (\$hex_string) is present, Then the rule matches.

This setup ensures the rule is specific to the malware while still flexible enough to catch variations.

Second Detect the Malware with Yara:

```
(seif@final)-[~]
└─$ yara rules.yara ./Downloads/test/invoice_2318362983713_823931342io.pdf.exe -s -w -p 32
ZeusBanking_Detection ./Downloads/test/invoice_2318362983713_823931342io.pdf.exe
0x3176c:$function_name: CellrotoCrudUntohighCols
0x0:$PE_magic_byte: 4D 5A
0x31716:$hex_string: 43 61 6D 65 56 61 6C 65 57 61 75 6C 65 72
```

Additional Step Create a Yara Rule with YarGen:

First create a Yara Rule to the ZeusBankingVersion_26Nov2013:

```
/*
YARA Rule Set
Author: yarGen Rule Generator
Date: 2024-12-20
Identifier: test
Reference: https://github.com/Neo23x0/yarGen
*/
/* Rule Set */

rule ZeusBankingVersion_26Nov2013 {
meta:
    description = "test - file ZeusBankingVersion_26Nov2013.zip"
    author = "yarGen Rule Generator"
    reference = "https://github.com/Neo23x0/yarGen"
    date = "2024-12-20"
    hash1 = "4644b5fb10fb84c0d47bec4b5a48d5e60165e8ae2130fcac5c055633aaad73162"
strings:
    $s1 = "invoice_2318362983713_823931342io.pdf.exe" fullword ascii
    $s2 = "invoice_2318362983713_823931342io.pdf.exePK" fullword ascii
    $s4 = "\0THBep!" fullword ascii
    $s5 = "OWVjY6S" fullword ascii
    $s6 = "oBPD\0=" fullword ascii
    $s7 = ".tjb,\`" fullword ascii
    $s8 = "IlBU,\\" fullword ascii
    $s9 = "asRt#U!" fullword ascii
    $s10 = "iYqK/e^" fullword ascii
    $s11 = "KL)'tNrIIA_wAn" fullword ascii
    $s12 = "lXxgM\0O" fullword ascii
    $s13 = "vtaMp?p" fullword ascii
    $s14 = "PMzrbuX" fullword ascii
    $s15 = "InYv?8" fullword ascii
    $s16 = "\\\vVuW" fullword ascii
    $s17 = "UofQk3" fullword ascii
    $s18 = "2G]zoh" fullword ascii
    $s19 = "G[IfNy#" fullword ascii
    $s20 = "!+d+1_" fullword ascii
condition:
    uint16(0) = 0x4b50 and filesize < 500KB and
    8 of them
}
```

Strings Section:

This section defines patterns (strings) the rule searches for in a file. Each \$sN variable represents a specific pattern:

- Strings like \$s1 and \$s2 are filenames or parts of filenames (invoice_2318362983713_823931342io.pdf.exe).
- Other strings, such as \$s3 to \$s20, are ASCII sequences potentially indicating unique or suspicious content (e.g., malicious code or markers of the Zeus malware).

Condition Section:

The condition determines whether the rule triggers. The conditions for this rule are:

- uint16(0) == 0x4b50: Checks if the file's first two bytes are 0x4b50, which indicates a ZIP file.
- filesize < 500KB: Ensures the file size is less than 500 KB.
- 8 of them: At least 8 of the defined strings must match for the rule to trigger.

This rule is tailored to detect ZIP files with specific malicious content associated with the Zeus malware.

Detect it with Yara:

```
└─(seif@Final)─[~/yarGen]
$ yara -y argen_rules.yar .. /Downloads/test/ZeusBankingVersion_26Nov2013.zip -s -w -p 32
ZeusBankingVersion_26Nov2013 .. /Downloads/test/ZeusBankingVersion_26Nov2013.zip
0x1e:$s1: invoice_2318362983713_823931342io.pdf.exe
0x2acab:$s2: invoice_2318362983713_823931342io.pdf.exePK
0x28c4b:$s3: E1U1r!.
0x4d91:$s4: @THBep!
0x15d4d:$s5: OWVjY6S
0x5213:$s6: oBPD@=
0x14eb4:$s7: .tjb,
0xcab8:$s8: ILBU,
0xb260:$s9: asRt#U!
0x855b:$s10: ivqK'e^
0x10ee8:$s11: KL)'tNrIIA_wAn
0x12904:$s12: lXxgM00
0x1e6b5:$s13: vtaMp?p
0x17a63:$s14: PMzrbuX
0x162c8:$s15: InYuZ8
0x1577:$s16: \vVuW
0x2058f:$s17: UofQk3
0xea35:$s18: 2G]zoh
0x10dc6:$s19: G[IfNy#
0xa46f:$s20: !+d+1_
```

Second create a Yara Rule to the invoice_2318362983713_823931342io_pdf:

```
rule invoice_2318362983713_823931342io_pdf {
    meta:
        description = "test - file invoice_2318362983713_823931342io.pdf.exe"
        author = "yarGen Rule Generator"
        reference = "https://github.com/Neo23x0/yarGen"
        date = "2024-12-20"
    hash1 = "69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169"
    strings:
        $s1 = "ejDmZK1d5htD0UB[gZTHJvrlLtaTBbsBS18pEuDJBuMks{0H0zRNleRt2kh8S:QPqP/2v2JFYWjpubc,vQKhJvYCDzsyJKTWY,B6xyzRzzHY6Ezu44u6U6L0L[dhqVMn" ascii
        $s2 = "corect.com" fullword ascii
        $s3 = "USER32.GetShellWindow" fullword ascii
        $s4 = "KERNEL32.GetThreadPriority" fullword ascii
        $s5 = "KERNEL32.SystemTimeToFileTime" fullword ascii
        $s6 = "USER32.GetKeyNameTextA" fullword ascii
        $s7 = "KERNEL32.CreateIoCompletionPort" fullword ascii
        $s8 = "KERNEL32.GetShortPathNameA" fullword ascii
        $s9 = "KERNEL32.GetWindowsDirectoryA" fullword ascii
        $s10 = "KERNEL32.GetStartupInfoW" fullword ascii
        $s11 = "kqKDSPX2HCYOP/CYRnfftI[QZT8NB8Tafn,Jg2Ko[0X+i1o0KnPp4ubEZniy2Q:OfQpxex4frsHQLes46ehHemEMxU9LPw{6VUKMC06p0w6cLW395ZdQdqxqDI6UQu7W" ascii
        $s12 = "9tc34Lsgj7KsJmvD1Nx5NewhlynXj97U7020IsjnaNv0Vglp5FzexmnW7uVRnovysoxu0sKAIn0NYuxRcwu81fYFOEugVLBVJ+3jUAL/w2{hHzhK9lepr0kc:ehsEO" ascii
        $s13 = "IKe397ub8Cxt0Fc4rpl7t{DViecb2T7YM1yKaiMRMyCfs8Q:m[+PtURL3Myem6ZTR6kTSYjeph4xg1wlgrno+H@p81Wmn78yBOY76uEWgJRFJUWBsYj9UhYSyka,41W" ascii
        $s14 = "Dumpcotsavo" fullword ascii
        $s15 = "<requestedExecutionLevel level='asInvoker' uiAccess='false' />" fullword ascii
        $s16 = "USER32.GetUpdateRgn" fullword ascii
        $s17 = "gi4HzEwf0b9TQHjtEo0Xk3TgcahTZe3sGWE0g5iVBZz3WW7wkiNIMrnH0ZuSagxOTBaU93fuzD4BD7yiAU9MT6yUdT+fdoMjVp00LOGZZVdXpV7cfpzMrUnxewB5eYr" ascii
        $s18 = "USER32.GetMonitorInfoW" fullword ascii
        $s19 = "jqixZmpZIU8V590xs8,5xbUM7YgXcpsjiizfRlhaQhH/pYXXG8LJqjhVsKft34K01rJG9KCGjT,brQiWn/xuwTW3xm,CyP60F936QWqfEhEgN1gM830g0trTb6hbP7ir" ascii
        $s20 = "fvifbs4KEyDcEPd9ma,m2mhSNAXYsZEbzZc10duQCS6p8uEip/hwoawNRzsRy6G5JFiyRhp/pLoGOKTt68dv6Hz:ofAI7V17o8lZxQpqKq51M3U,Nsk0Fy1rZViDPKI" ascii
    condition:
        uint16(0) = 0x5a4d and filesize < 700KB and
        8 of them
}
```

Strings Section:

- \$s1: A long ASCII sequence, likely representing encoded or obfuscated data.
- \$s2: References corect.com, which may be associated with malicious infrastructure.
- \$s3 to \$s10: Function names from Windows APIs, suggesting this file interacts with the operating system, potentially for malicious purposes.
- \$s15: A line from a manifest file indicating a requested execution level, showing the program's privileges.
- \$s14: "Dumpcotsavo" is likely a specific string marker.
- \$s11, \$s12, \$s13, \$s17, \$s19, \$s20: Long ASCII sequences indicating additional suspicious patterns.

Condition Section:

- `uint16(0) == 0x5a4d`: Checks if the file starts with 0x5a4d, indicating a Windows executable (PE file).
- `filesize < 700KB`: Ensures the file size is less than 700 KB.
- `8 of them`: At least 8 of the defined strings must match for the rule to trigger.

This rule is focused on detecting executable files related to a suspicious invoice filename with patterns of malicious behavior.

Detect it with Yara:

```
└─(seif㉿final)-[~/yarGen]
└─$ yara yargen_rules.yar .../Downloads/test/invoice_2318362983713_823931342io.pdf.exe -s -w -p 32
invoice_2318362983713_823931342io_pdf .../Downloads/test/invoice_2318362983713_823931342io.pdf.exe
0x15f36:$s1: ejDmZKid5htD0UB[gZTHJvrlTaTBBsBS18pEuDJBuMks{0H0zRNleRt2kh8S:QPqP/2v2JFYWjpubc,vQKhJvYCDZsyJKTWY,B6xyzRzzHY6Ezu44u6U6LOL[dhqVMn
0x311f6:$s2: corect.com
0x31a49:$s3: USER32.GetShellWindow
0x31d13:$s4: KERNEL32.GetThreadPriority
0x319e2:$s5: KERNEL32.SystemTimeToFileTime
0x319a7:$s6: USER32.GetKeyNameTextA
0x31ada:$s7: KERNEL32.CreateIoCompletionPort
0x31b13:$s8: KERNEL32.GetShortPathNameA
0x31939:$s9: KERNEL32.GetWindowsDirectoryA
0x31be1:$s10: KERNEL32.GetStartupInfoW
0x271a8:$s11: kqKDSPX2HCYOP/CYRnfftI[QZT{BN8Tafn,Jg2Ko[0X+i1o0knPp4ubEZniy2Q:OfQpxex4frsHQLes46ehHemEMxU9LPw{6VUKMC06p0w6cLW395ZdQdqxqDI6UQu7W
0x1ae26:$s12: 9tc34LSgjt7ksJmvD1NxNewhlynXj97U7020IsjnaNv0Vglp5FzexmnW7uVRnovysoxu0sKAIn0NYuxRcwu81fYOeEugVLBVJ+3jUAl/w2{hZhK9Lepr0kc:ehsE0
0x2dae8:$s13: IKe397ub8Cxt0FKc4rpl7t{DViecb2T7YM1yKaiMRmyCfs8Q:m[+PtURL3Myem6ZTR6kTSYjeph4xg1wlgrno+H0p81Wmn78yBOY76uEWgJRFJUWBsYj9UhYSyka,41W
0x3180c:$s14: Dumpcotsavo
0x3c461:$s15: <requestedExecutionLevel level='asInvoker' uiAccess="false" />
0x31fa1:$s16: USER32.GetUpdateRgn
0x309b7:$s17: gi4HzEwf0b9TQHjtEo0Xk3TgcahTZe3sCGwE0g5iVBZz3WW7wkiNIMrnH0ZuSagxOTBaU93fuzD4BD7yiAU9MT6yUdT+fdoMjVp00l0GZZVdXPV7cfpzMrUnxewB5eYr
0x31dbb:$s18: USER32.GetMonitorInfoW
0x222bc:$s19: jqiXzmPzIU8V590Xs8,5xbUM7YgXcpsjiizfRlhaQhH/pYXxG8LJqjhVskFt34KolaJG9KCGjT,brQrWn/xuwTW3xm,CyP60F936QWqfEhEgN1gM830g0trTb6hbP7ir
0x23d08:$s20: fvifsB4KEyDcEPd9ma,mZmhSNAXYsZEBZcl0dUQCS6p8uEip/hwoawNRzsRy6G5JFIyRhp/pLoGOKTt68dv6HMz:ofAI7VI7o8lZxQpqKq51M3U,Nsk0Fy1rZViPKI
```