Lord of The Things Typhon Operation

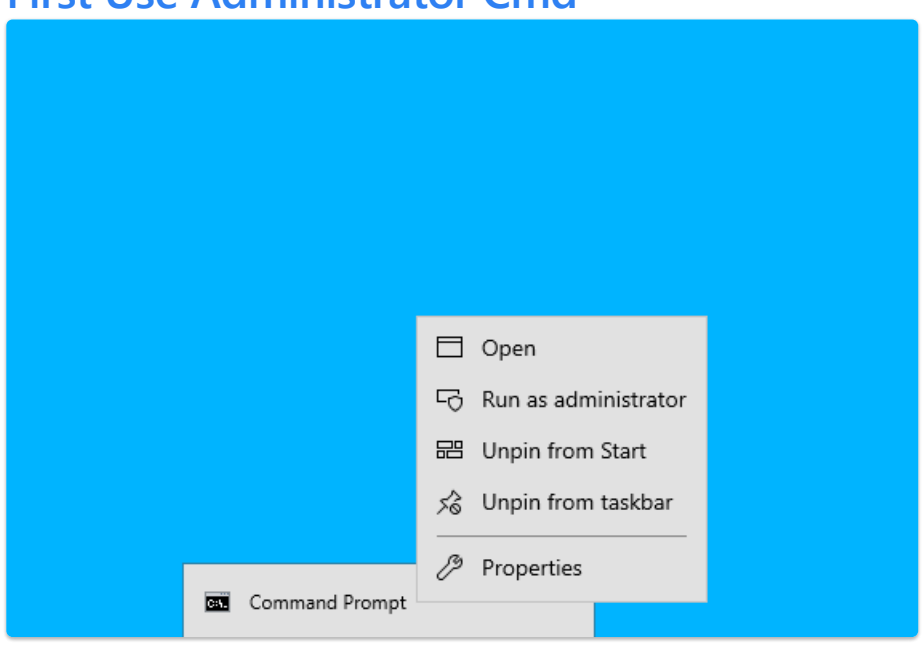
Typhon vs Zeus

- The Zeus trojan virus was first created in 2007, when hackers in Eastern Europe used it to target the United States Department of Transportation. While it's hard to say for certain who created it, the attack really took off when its malicious code became public in 2011. Since then, it has spawned dozens of variants that have kept internet security experts and law enforcement busy.
  There are two common attack vectors that open Windows computers to Zeus trojan malware attacks. Drive-by downloads require a user to visit a website that has the backdoor trojan code on it. They then download files into the user's computer without the user's knowledge. Modern browsers such as Google Chrome usually block these downloads and the sites they are found on, but hackers are constantly implementing new workarounds for this. Meanwhile, older web browsers like Internet Explorer may not block drive-by downloads at all. Zeus's other main mode of infection is through phishing attacks where users think they are downloading benign software from links in a phishing email or a post on social media.
- The myth of Typhon vs. Zeus is a dramatic and intense episode in Greek mythology, often regarded as the climax of the Titanomachy, or the war between the Olympian gods and their adversaries. This myth exemplifies the ultimate struggle for cosmic order, as Typhon, a chaotic and monstrous force, challenges Zeus, the king of the gods, for supremacy over the universe.

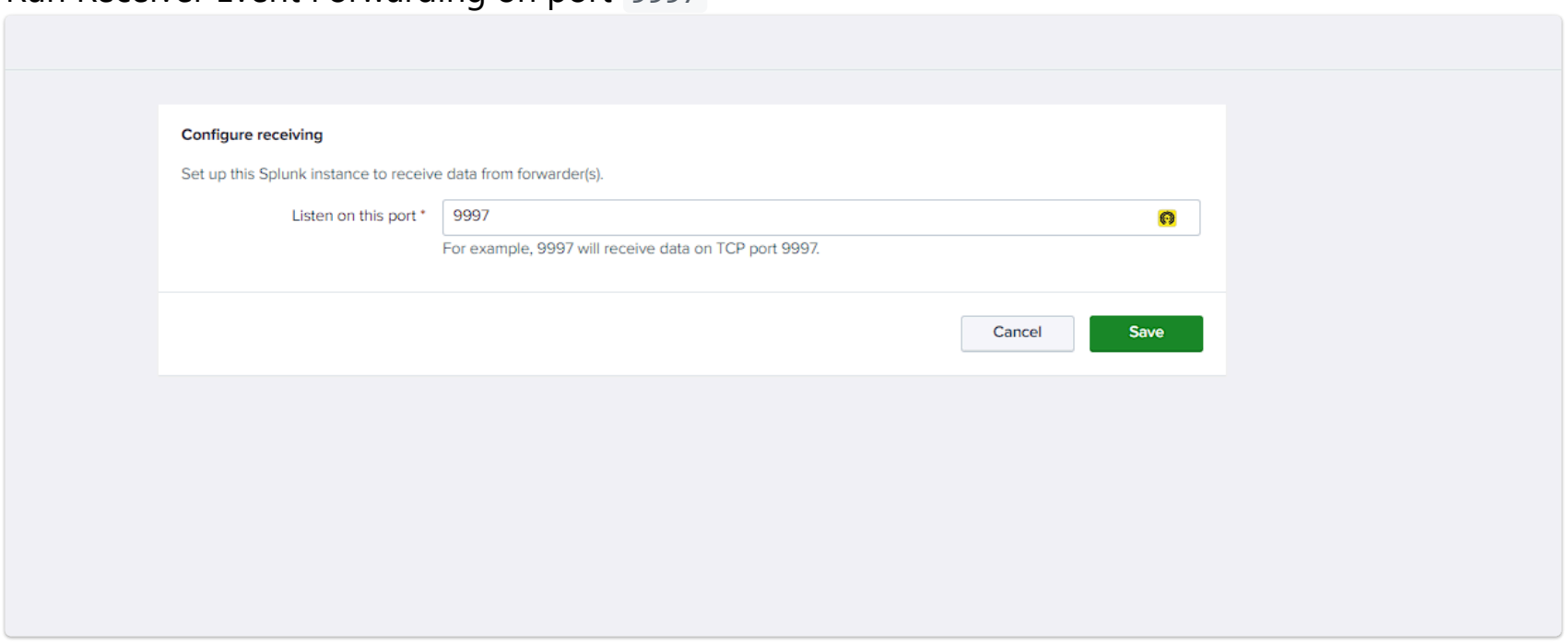
Lab Implementation

Detection Tools Installation

- First Use Administrator Cmd

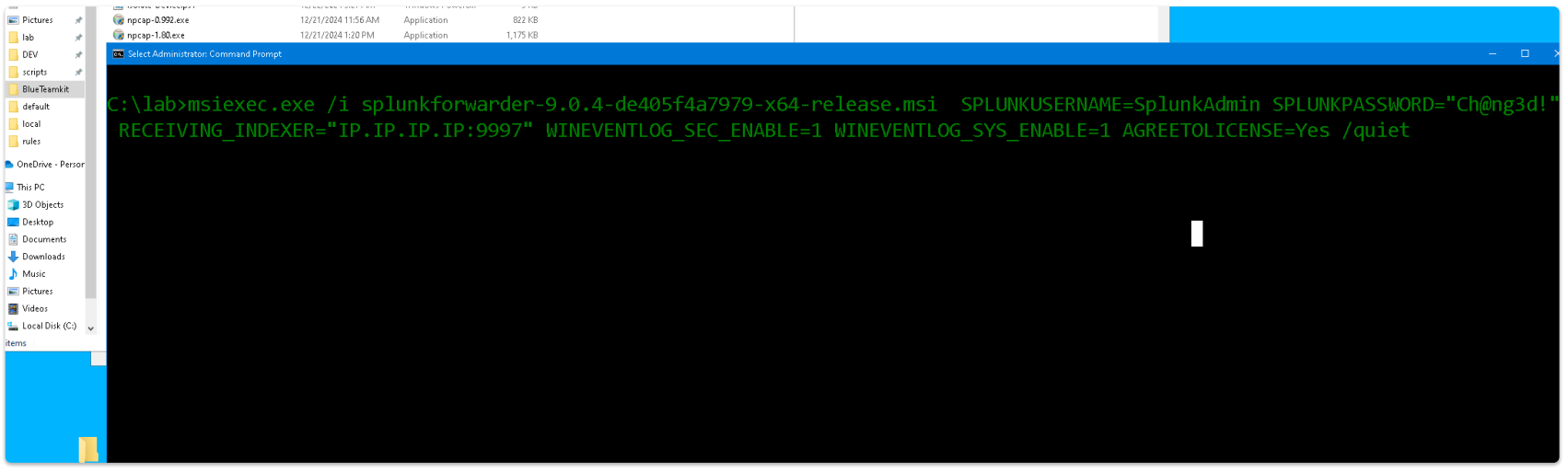


- Splunk Event Forwarder Installation
  - Create Event Receiver Port On Splunk server
  - Run Receiver Event Forwarding on port `9997`

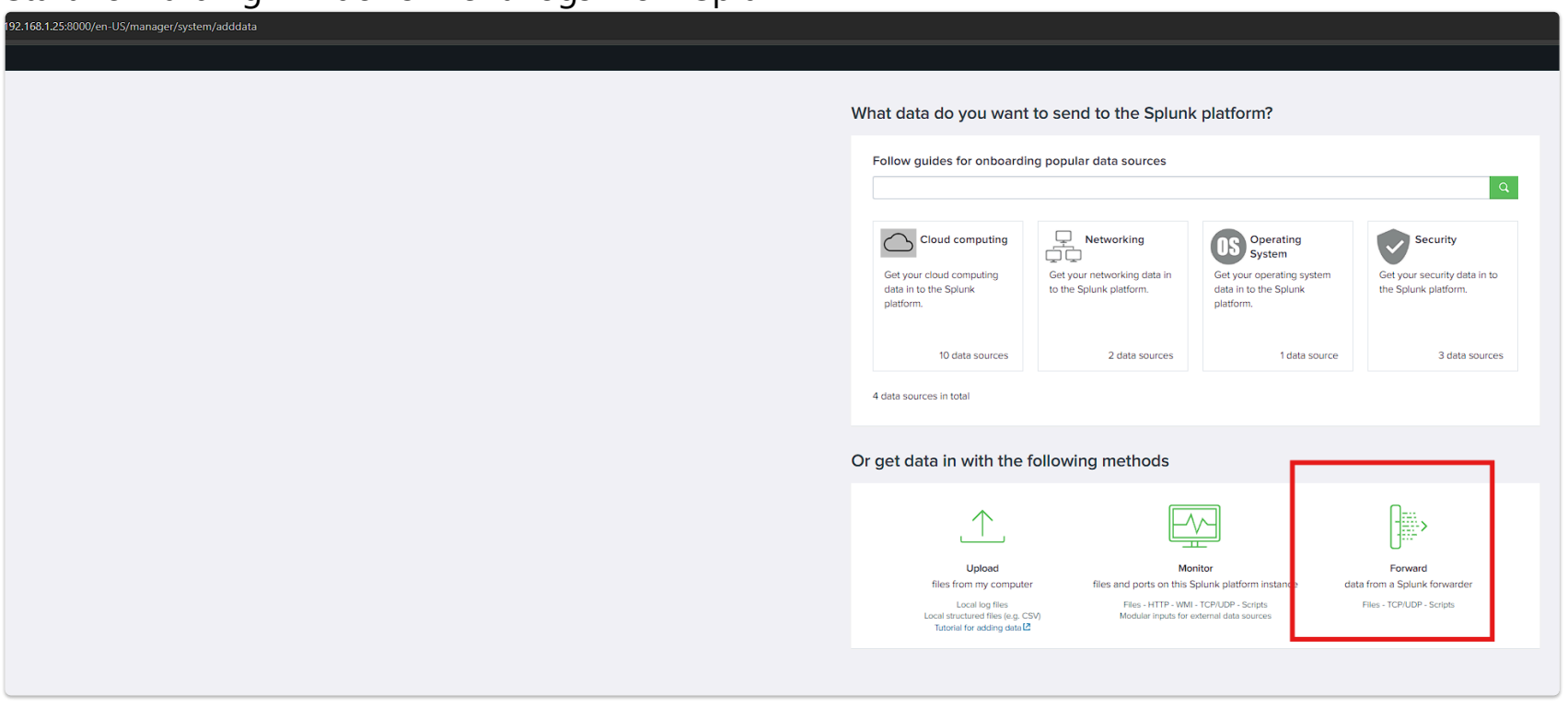


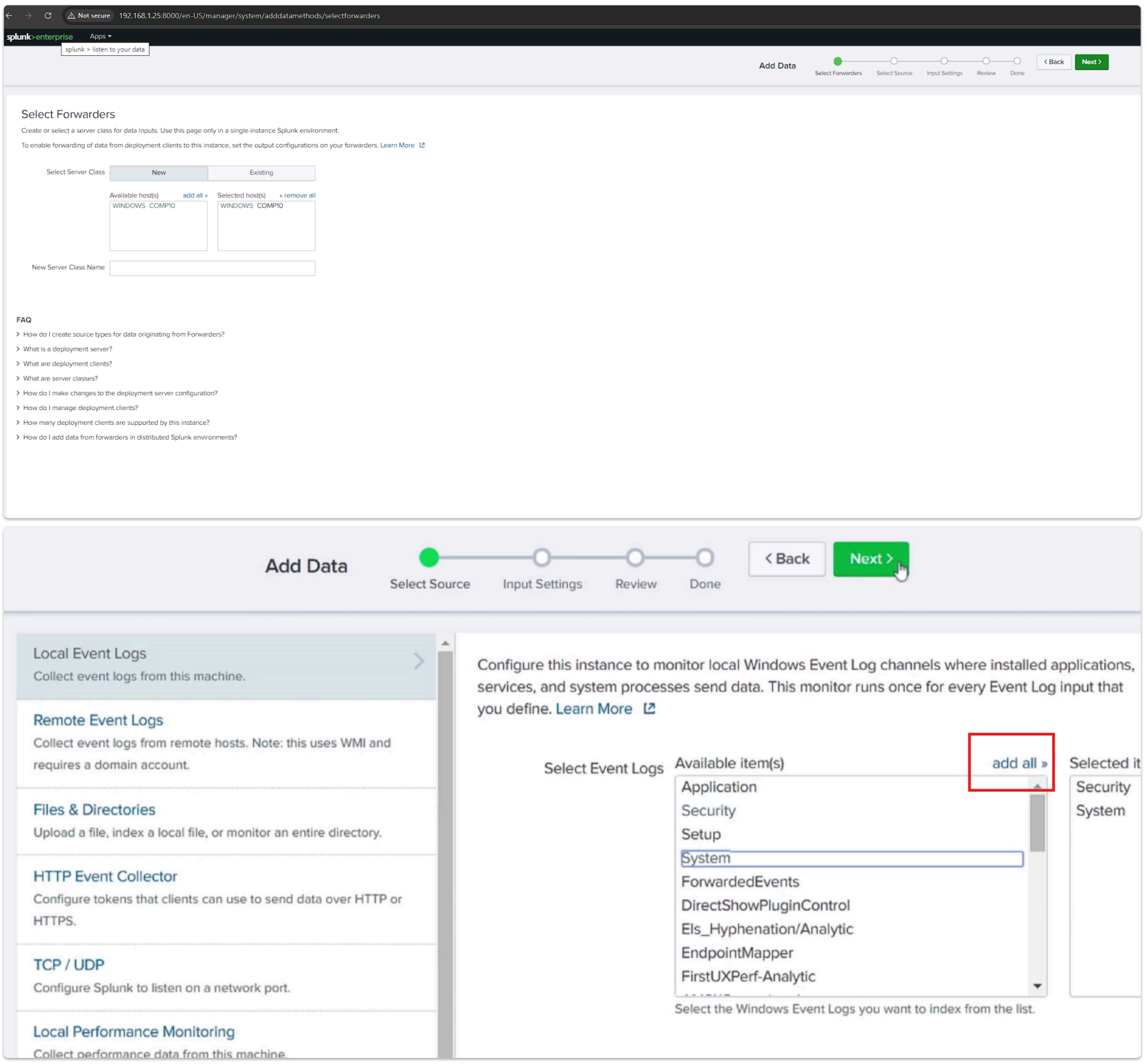
- Install & Forward Events on the Splunk server IP,Port

```
C:\lab\BlueTeamkit>msiexec.exe /i splunkforwarder-9.0.4-de405f4a7979-x64-release.msi
SPLUNKUSERNAME=SplunkAdmin SPLUNKPASSWORD=Ch@ng3d! RECEIVING_INDEXER="IP.IP.IP.IP:9997"
WINEVENTLOG_SEC_ENABLE=1 WINEVENTLOG_SYS_ENABLE=1 AGREETOLICENSE=Yes /quiet
```

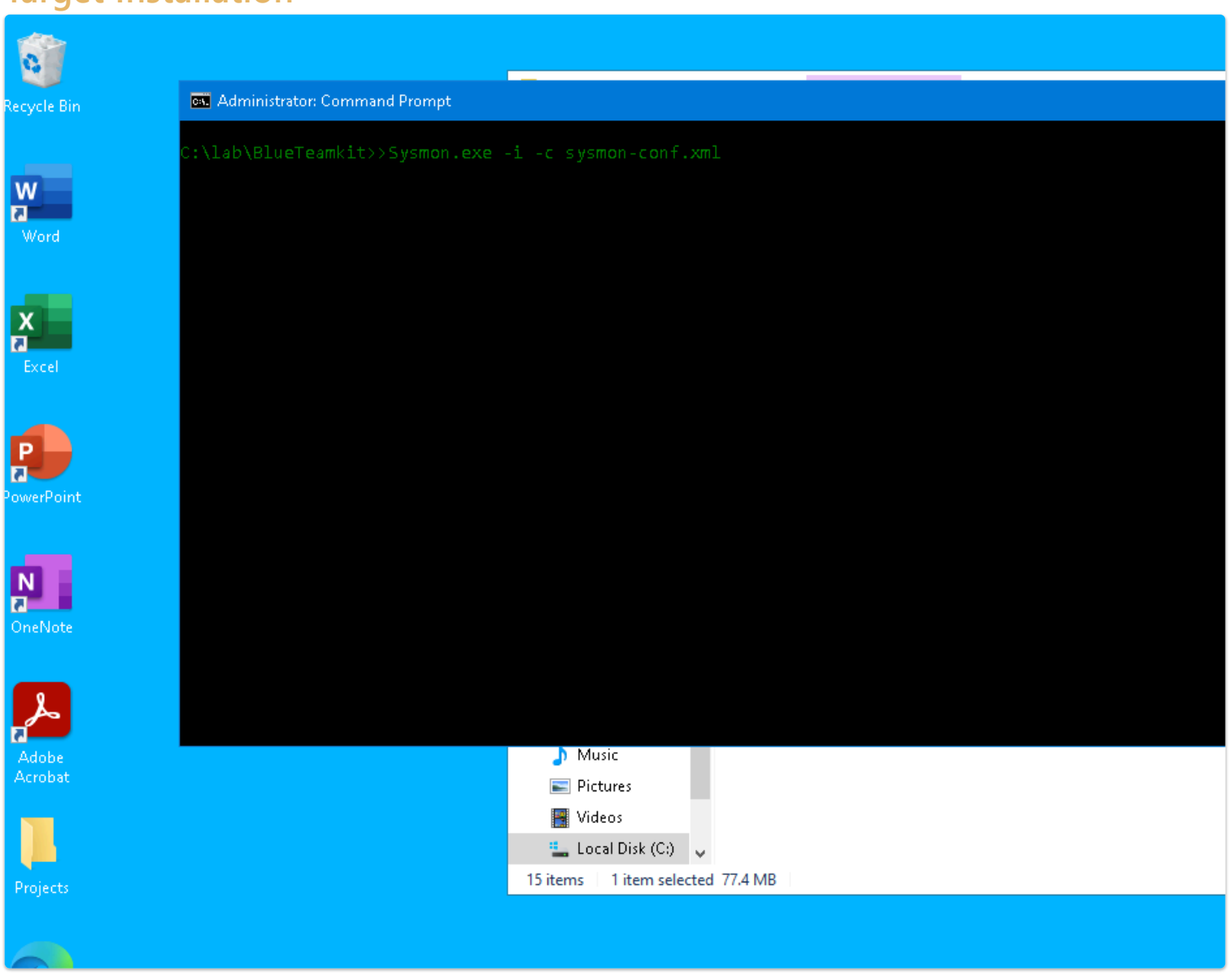


- Start Forwarding Windows Event Logs From Splunk





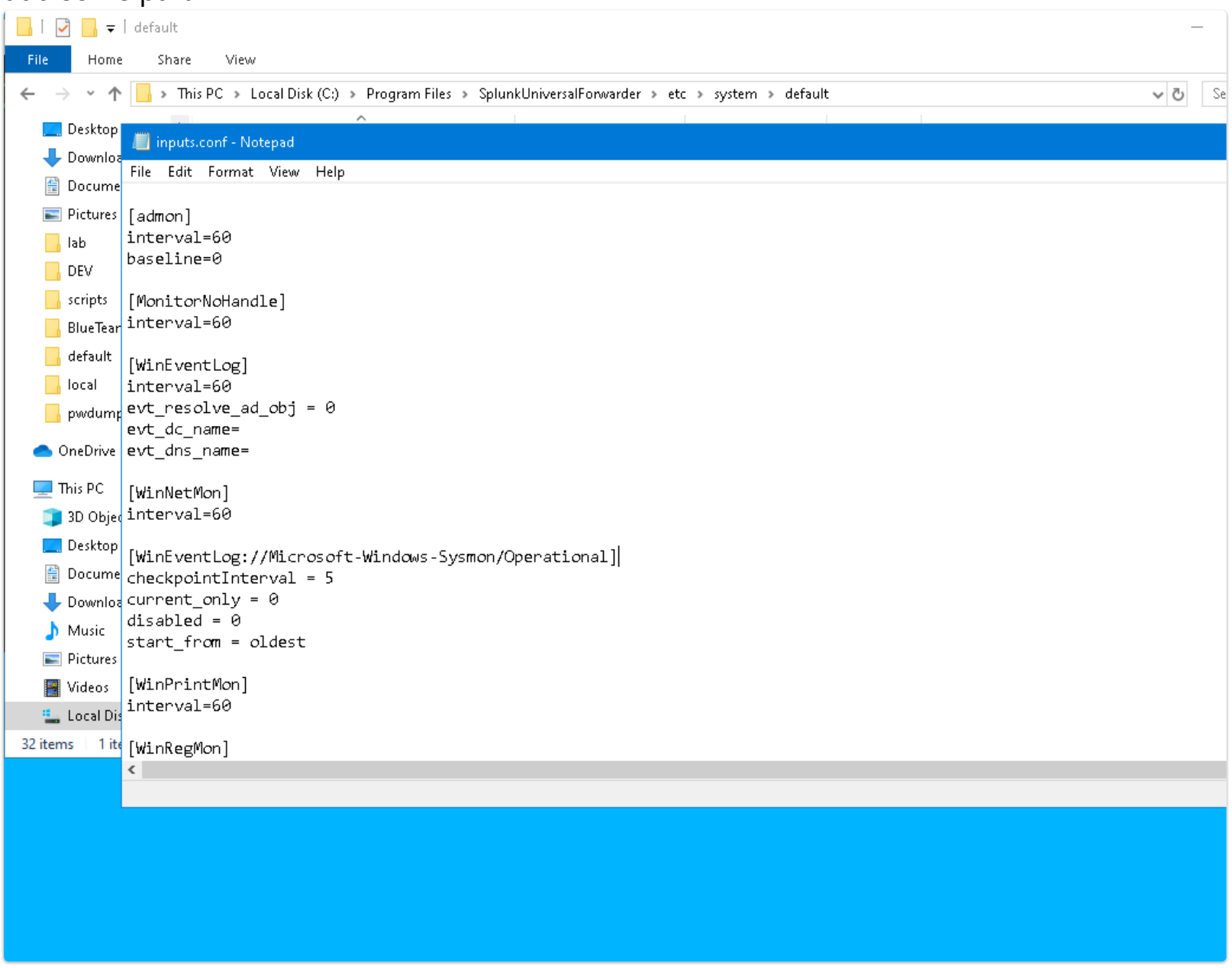
- Sysmon
  - Target Installation



  - Splunk Integration
    - Edit Inputs File

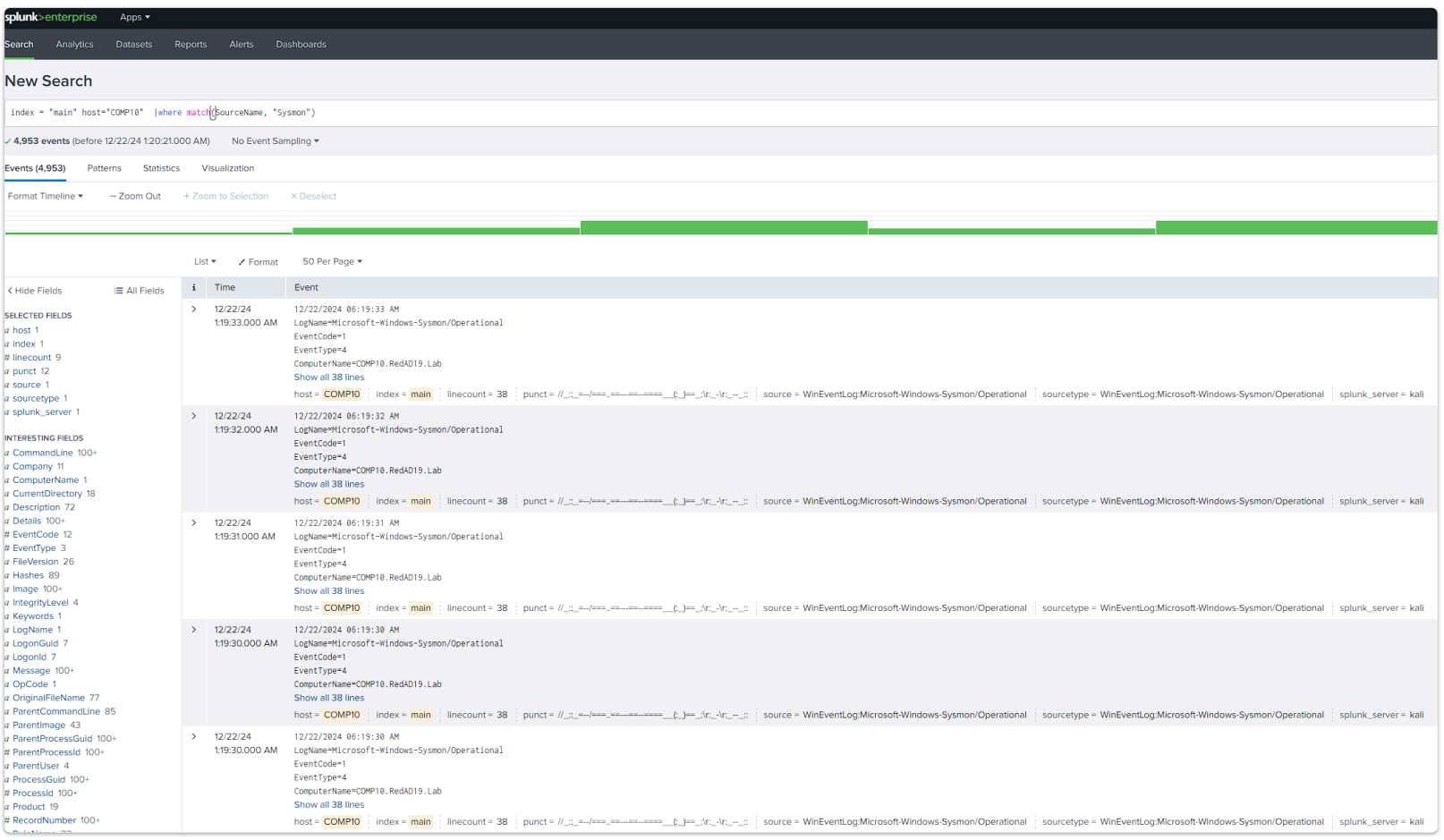
      In `C:\Program File\SplunkUniversalForwarder\etc\system\default\inputs.conf`

add some part




```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]|
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
```

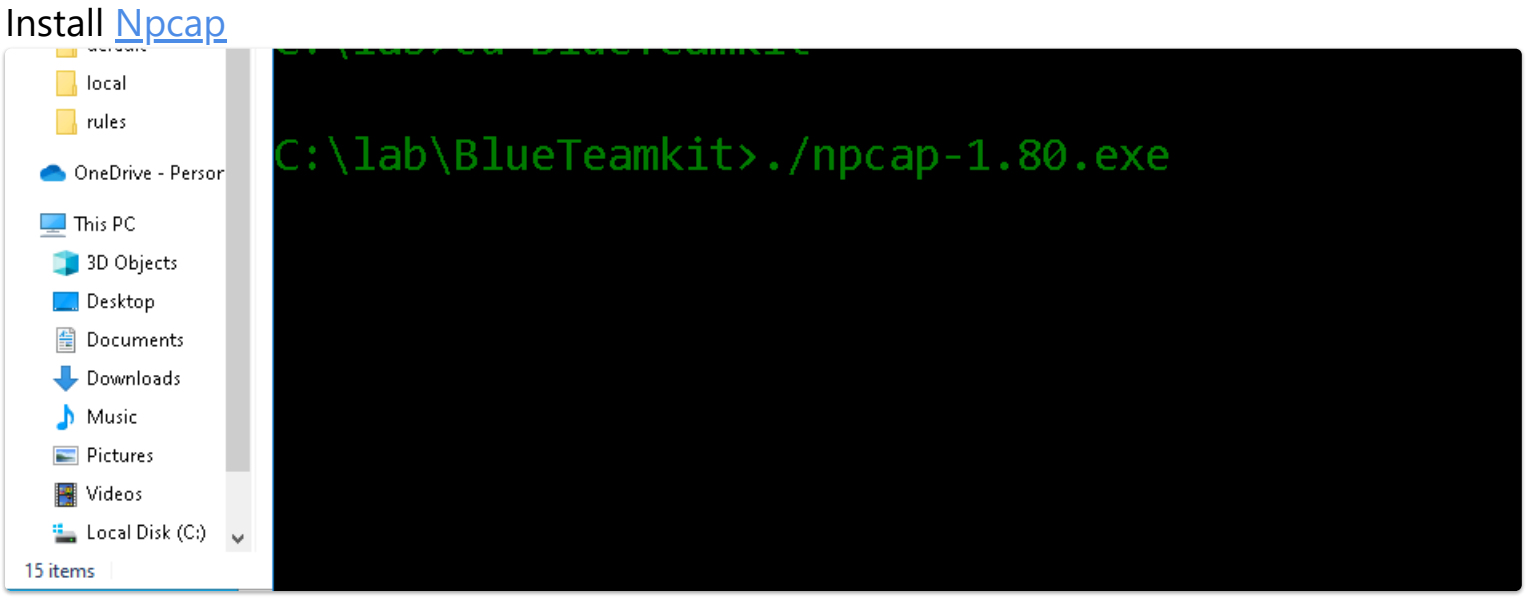
- Final Result In SEIM



- Suricata
  - Target Installation
    - File Download [suricata.exe][https://www.openinfosecfoundation.org/download/windows/Suricata-7.0.8-1-

64bit.msi]

- Install Npcap

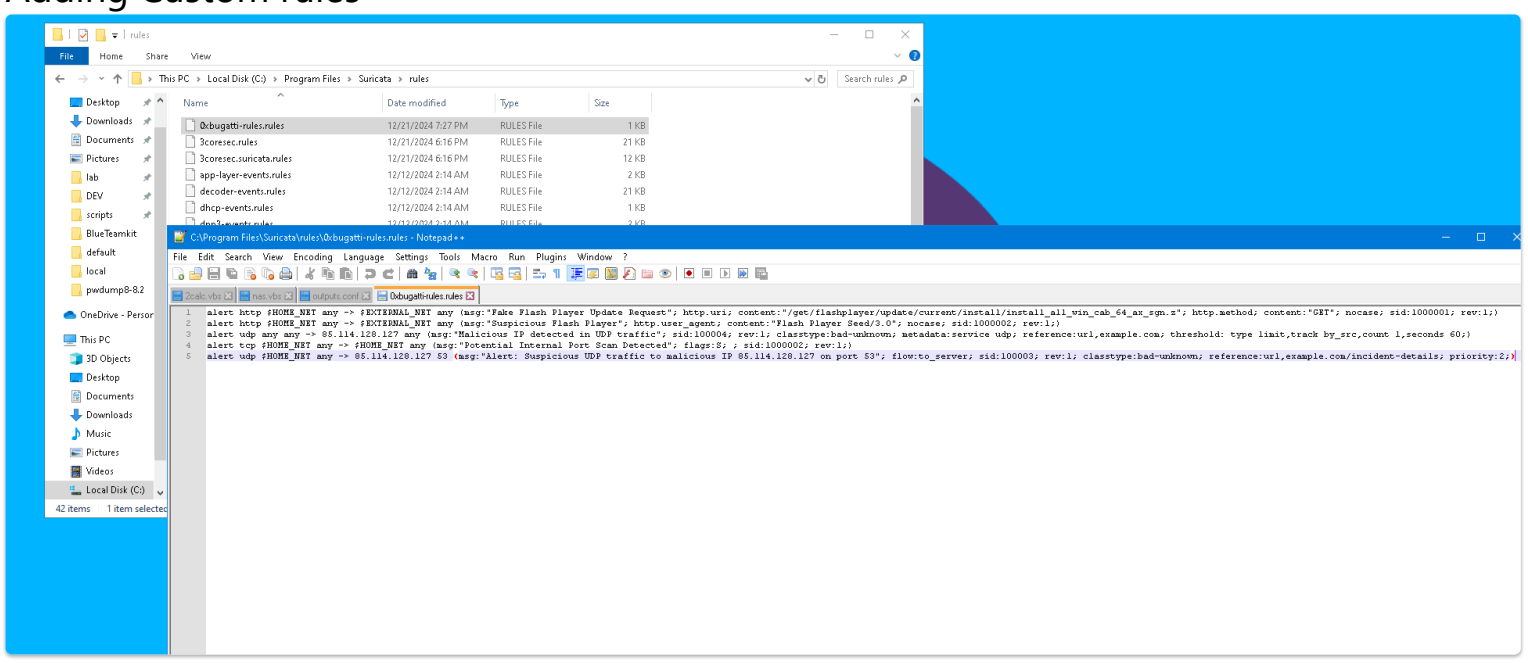


- Rule Updater Module
  - Powershell Script
  - Schedule Task command

```
$action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "-File C:\lab\\BluteamKit\Uppdate-Suricata.ps1"
$trigger = New-ScheduledTaskTrigger -Daily -At "10:00AM"
Register-ScheduledTask -TaskName "Installation of Software"  -Execute "PowerShell.exe" -Argument
```

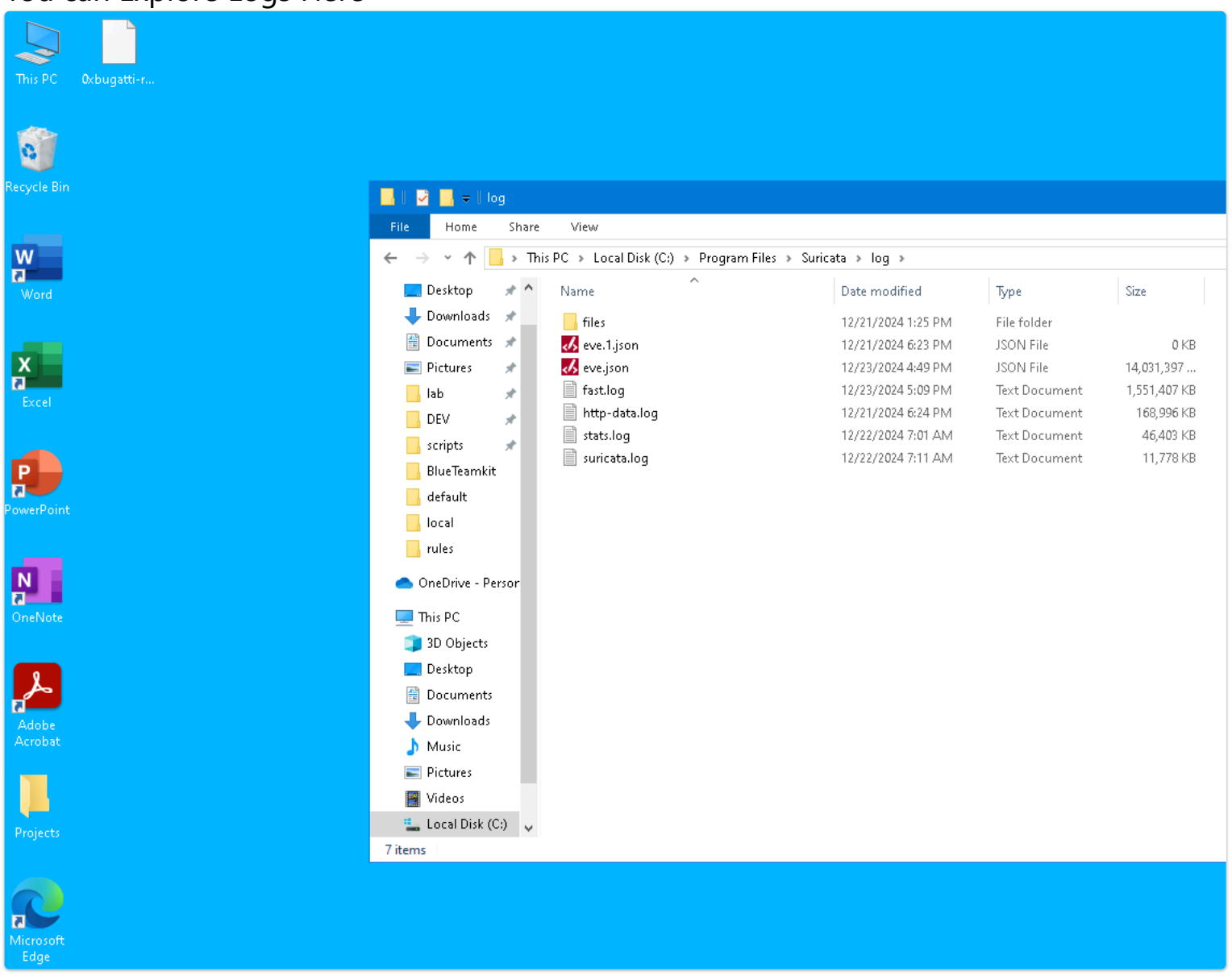
- Custom rules

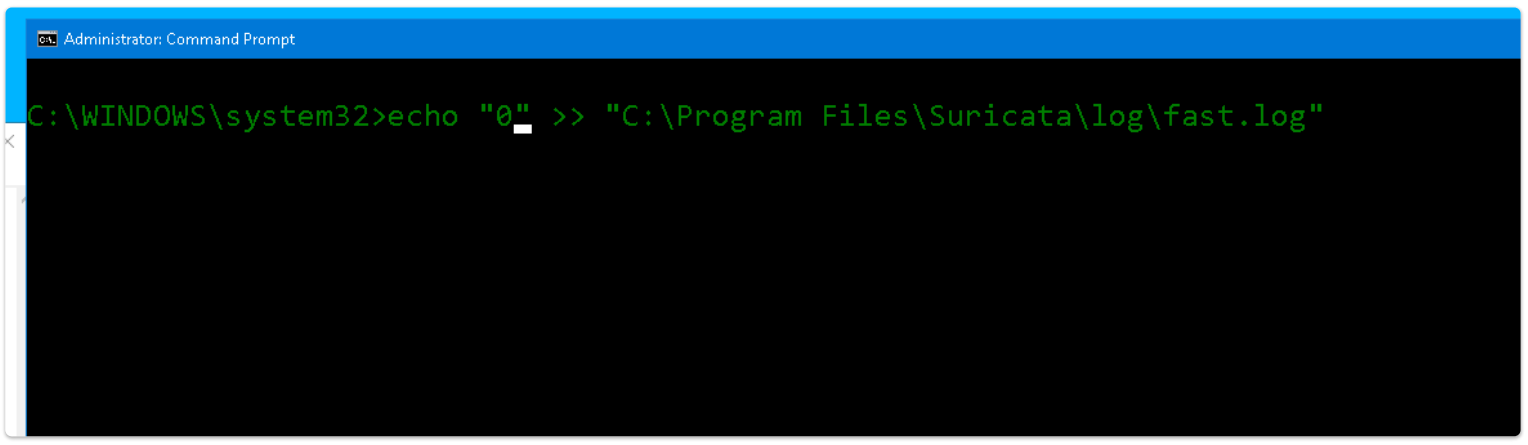
- Adding Custom rules



- Creation of alerting file

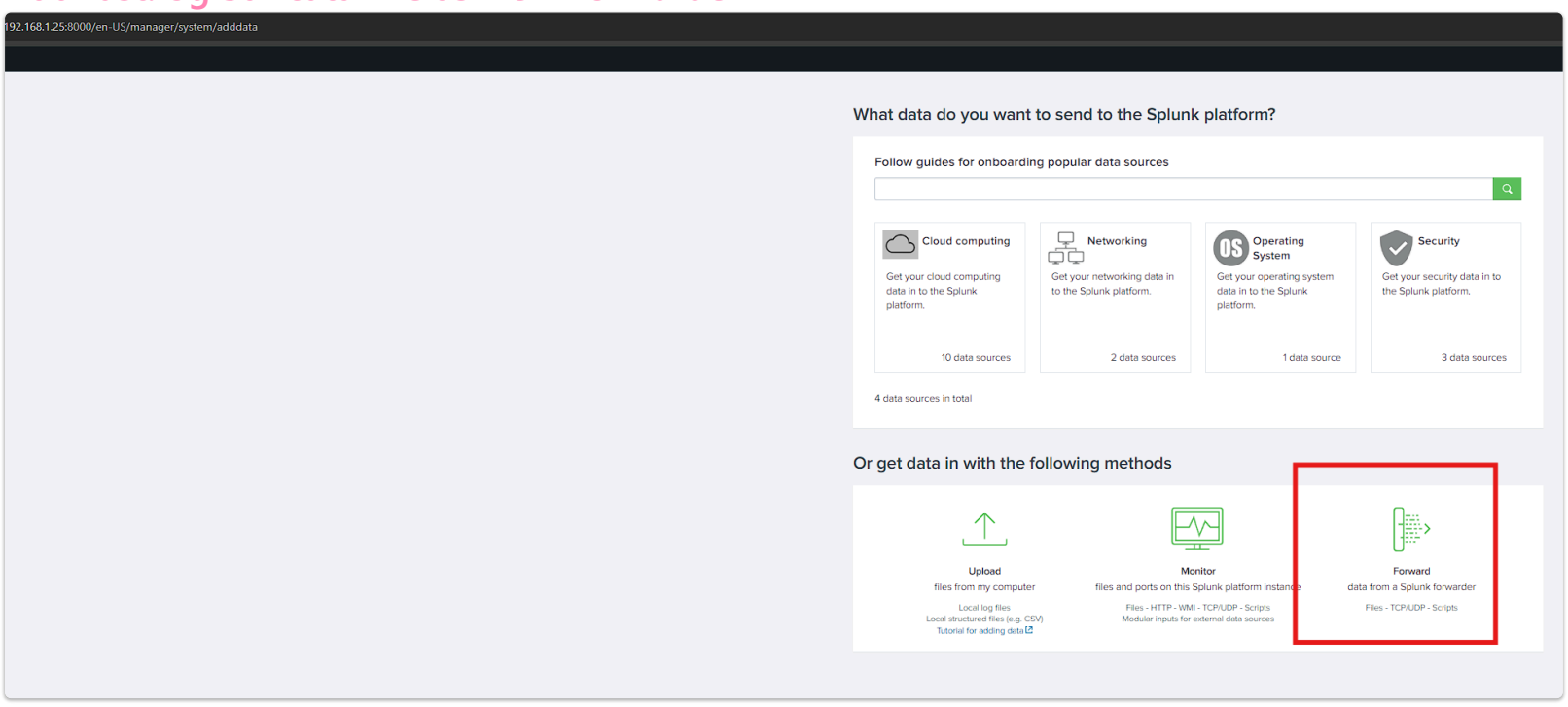
  You can Explore Logs Here

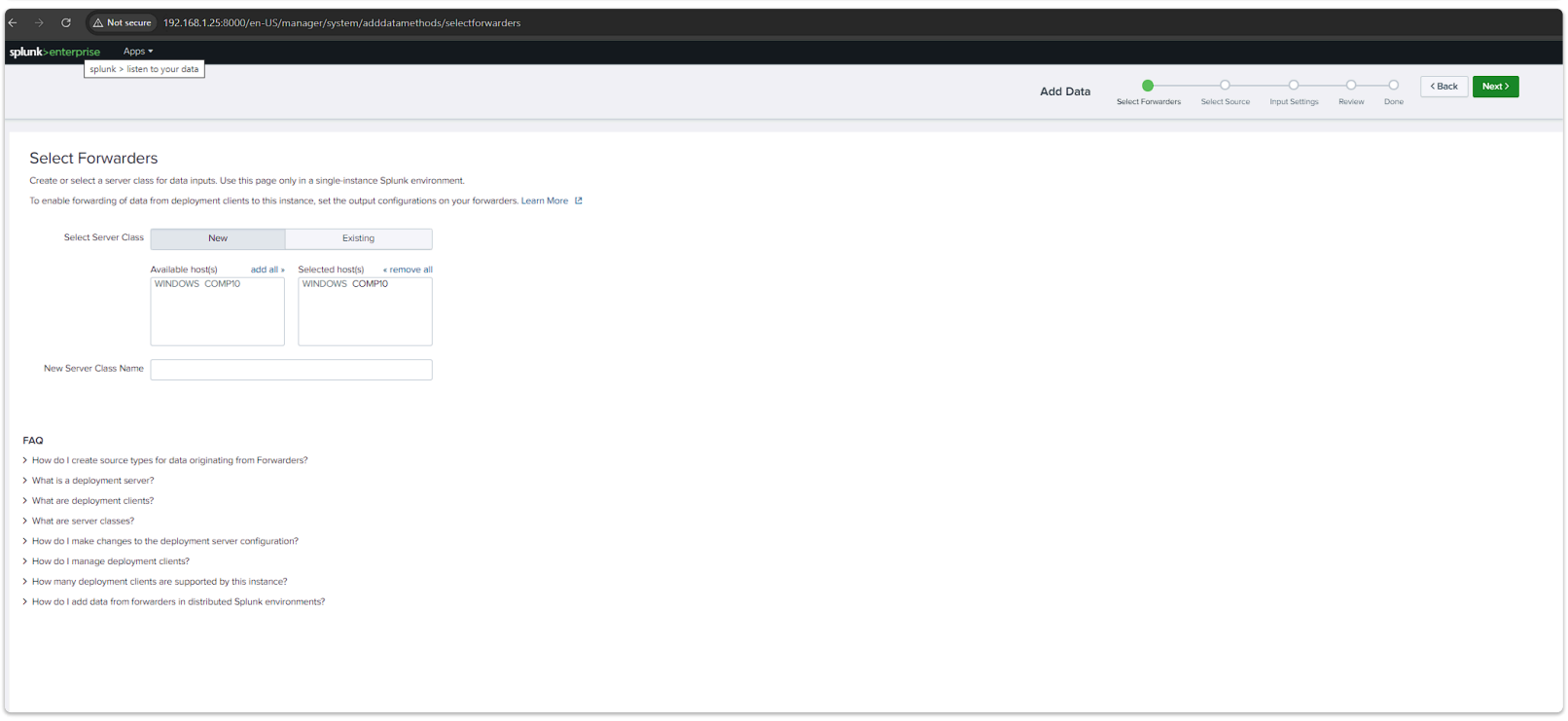


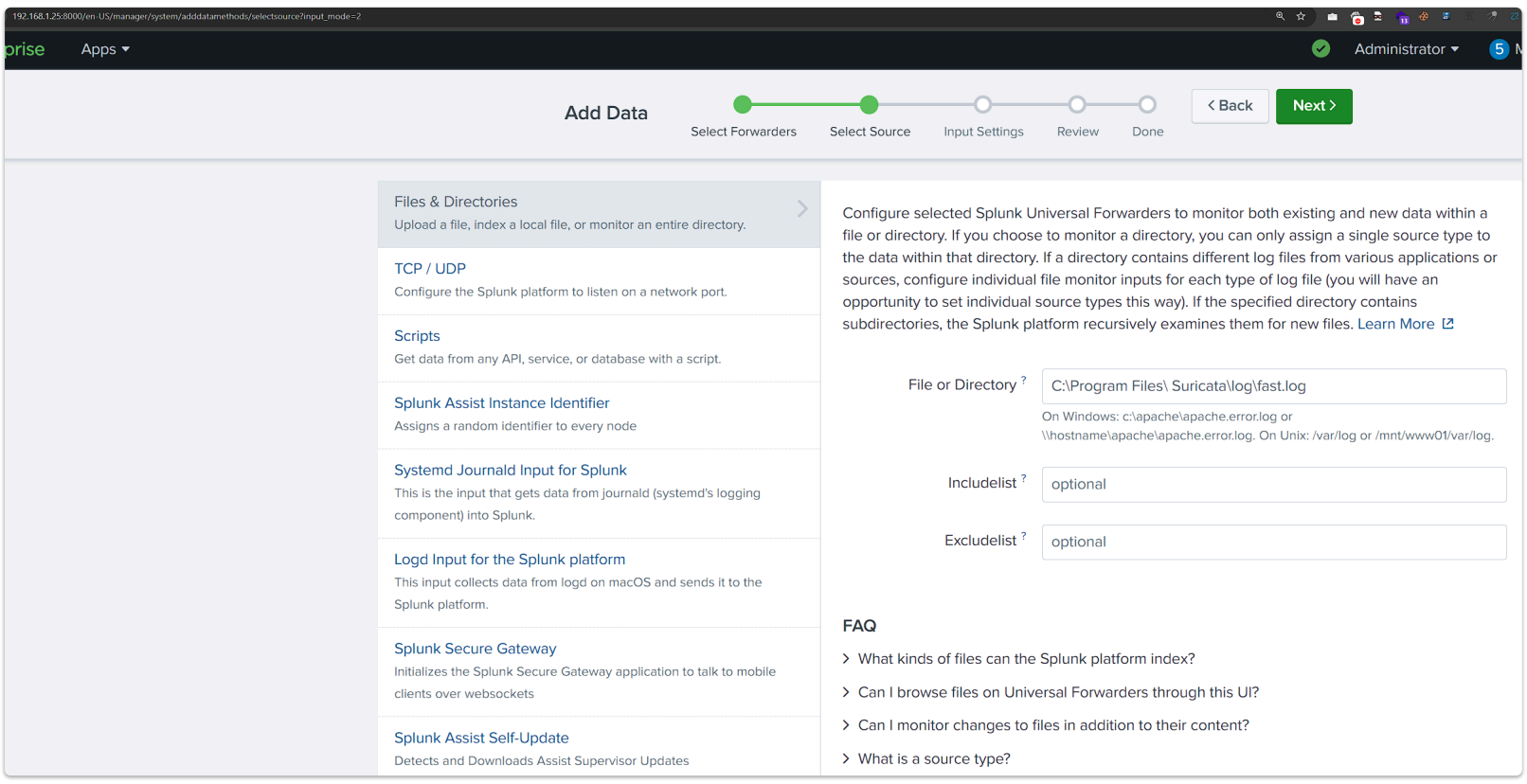


- Splunk Integration

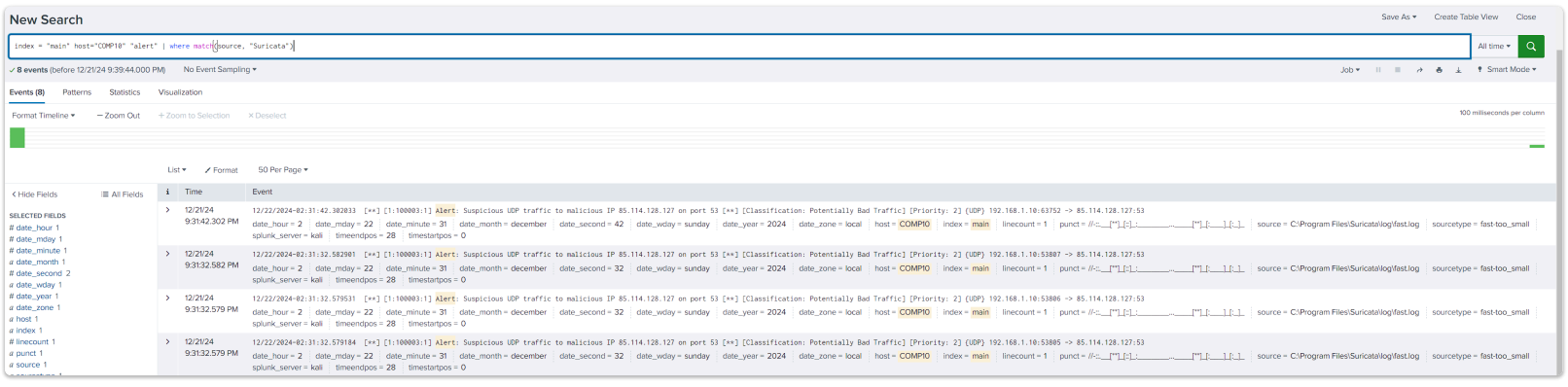
- ## Add fast.log Suricata File as New Forwarder

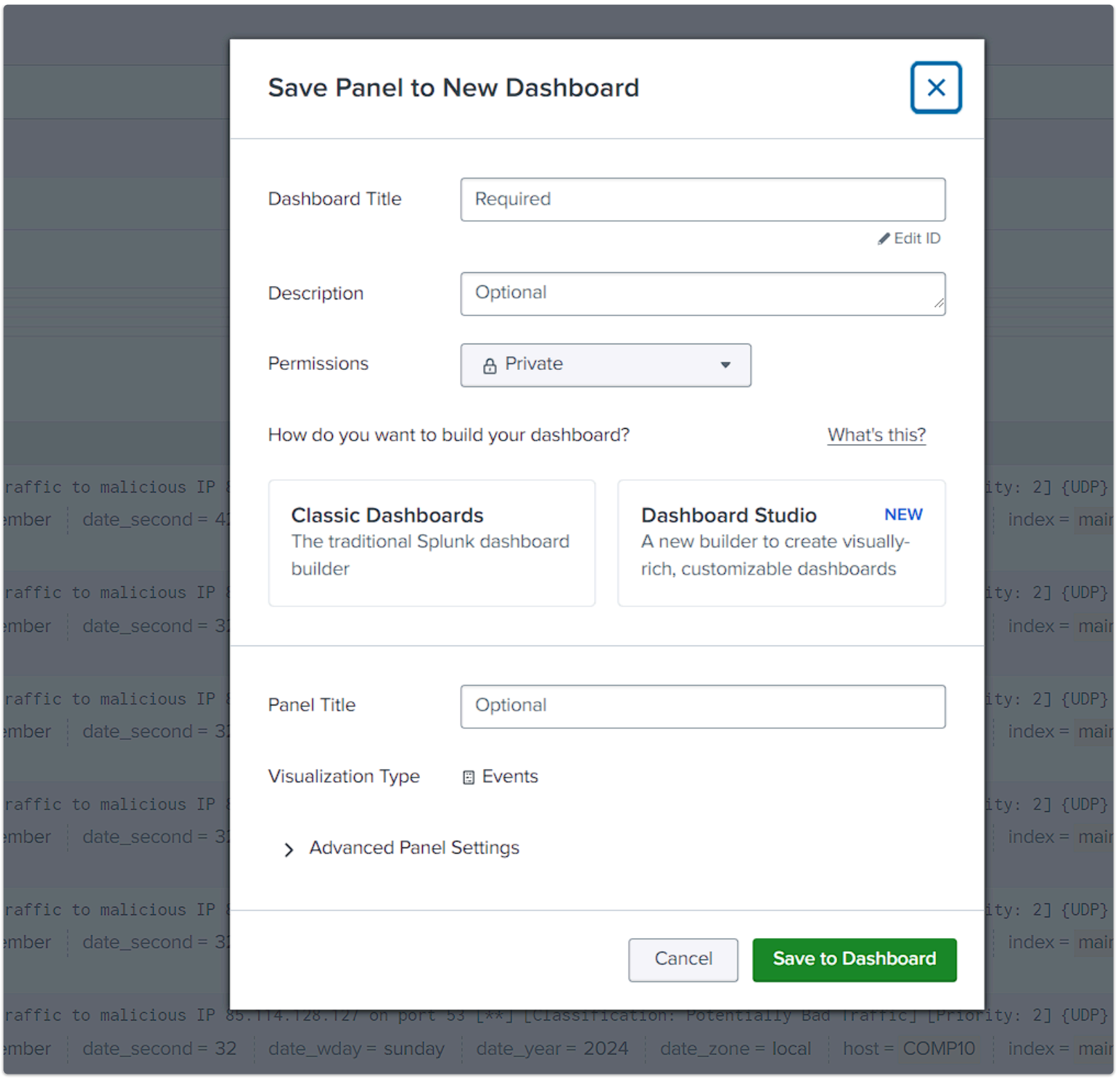


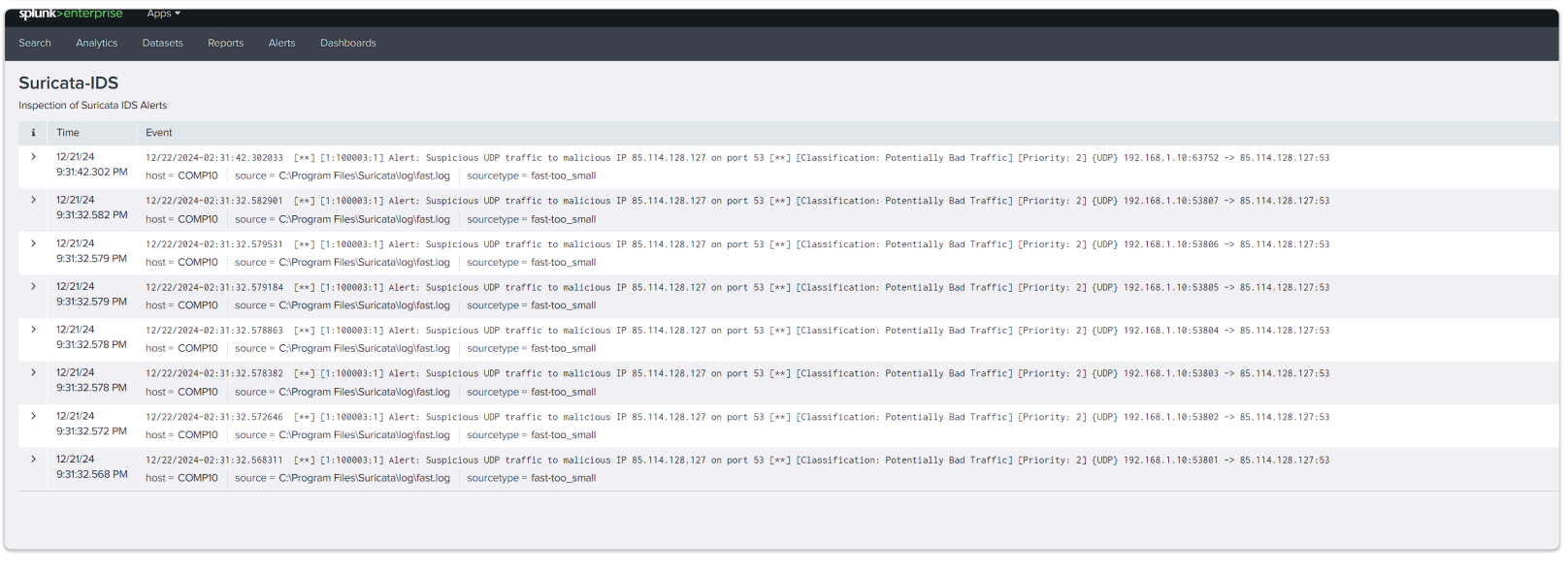




- ## Dashboard Creation



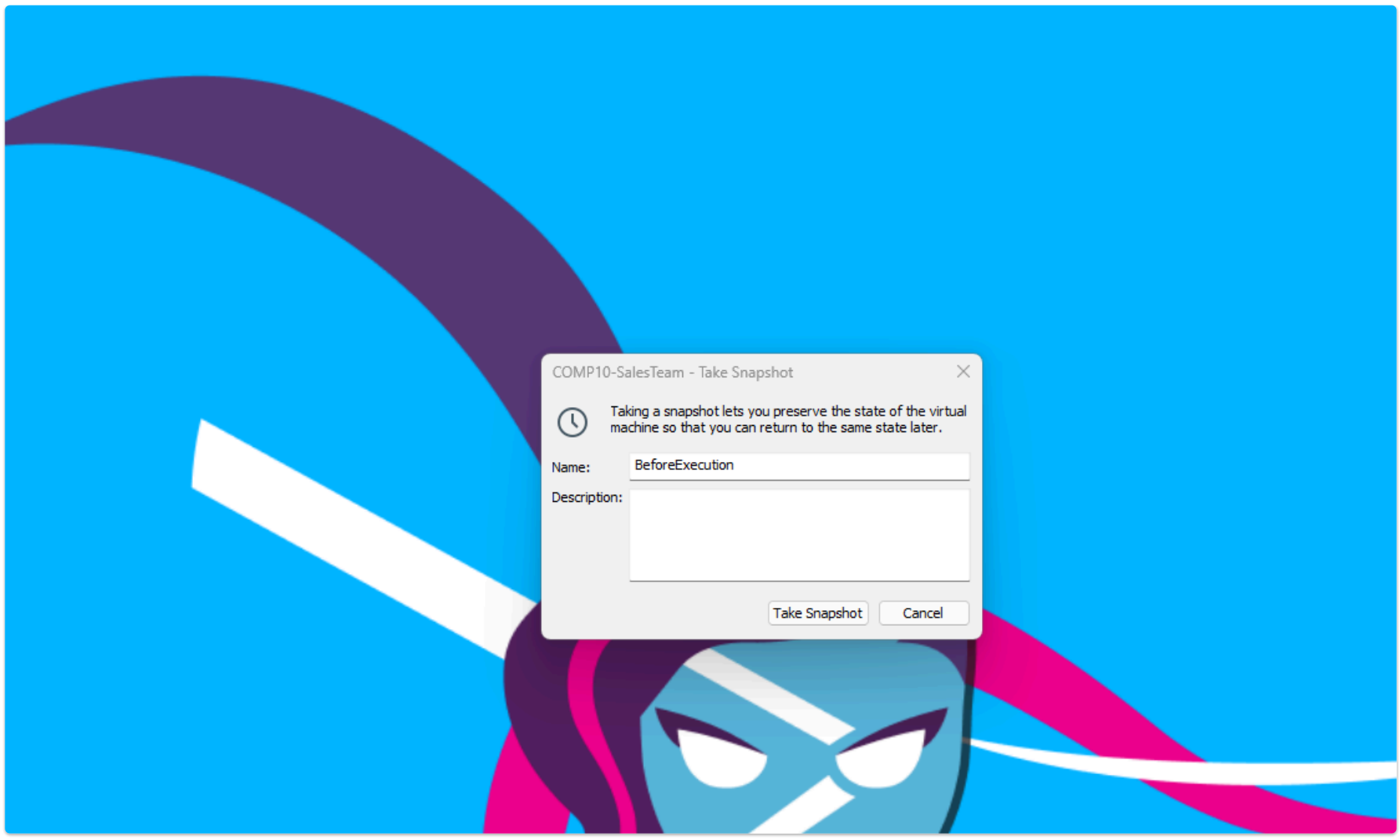




- ## Saving Daily Secure BackUp

  All is Done Now and All Detection Works

  Taking Snapshot



- Combine & Run All

Using Services

Secondary Logon	Enables starting processes un...		Manual	Local System
Secure Socket Tunneling Pr...	Provides support for the Secu...	Running	Manual	Local Service
Security Accounts Manager	The startup of this service sig...	Running	Automatic	Local System
Security Center	The WSCSVC (Windows Secur...	Running	Automatic (Delayed Start)	Local Service
Sensor Data Service	Delivers data from a variety of...		Manual (Trigger Start)	Local System
Sensor Monitoring Service	Monitors various sensors in or...		Manual (Trigger Start)	Local Service
Sensor Service	A service for sensors that man...		Manual (Trigger Start)	Local System
Server	Supports file, print, and name...	Running	Automatic (Trigger Start)	Local System
Shared PC Account Manager	Manages profiles and accoun...		Disabled	Local System
Shell Hardware Detection	Provides notifications for Aut...	Running	Automatic	Local System
Smart Card	Manages access to smart card...		Manual (Trigger Start)	Local Service
Smart Card Device Enumera...	Creates software device node...		Manual (Trigger Start)	Local System
Smart Card Removal Policy	Allows the system to be confi...		Manual	Local System
SNMP Trap	Receives trap messages gener...		Manual	Local Service
Software Protection	Enables the download, install...		Automatic (Delayed Start, Trigger Start)	Network Service
Spatial Data Service	This service is used for Spatial ...		Manual	Local Service
SplunkForwarder Service	SplunkForwarder is the remot...	Running	Automatic	Local System
Spot Verifier	Verifies potential file system c...		Manual (Trigger Start)	Local System
SSDP Discovery	Discovers networked devices ...	Running	Manual	Local Service
SshdBroker	<Failed to Read Description. E...		Manual	Local System
State Repository Service	Provides required infrastructu...	Running	Manual	Local System
Still Image Acquisition Events	Launches applications associa...		Manual	Local System
Storage Service	Provides enabling services for...	Running	Manual (Trigger Start)	Local System
Storage Tiers Management	Optimizes the placement of d...		Manual	Local System
Suricata		Running	Automatic	Local System
Sync Host_dc555	This service synchronizes mail...	Running	Automatic (Delayed Start)	Local System
SysMain	Maintains and improves syste...	Running	Automatic	Local System
Sysmon64	System Monitor service	Running	Automatic	Local System
System Event Notification S...	Monitors system events and n...	Running	Automatic	Local System
System Events Broker	Coordinates execution of bac...	Running	Automatic (Trigger Start)	Local System
System Guard Runtime Mo...	Monitors and attests to the in...	Running	Automatic (Delayed Start, Trigger Start)	Local System
Task Scheduler	Enables a user to configure an...	Running	Automatic	Local System
TCP/IP NetBIOS Helper	Provides support for the NetB...	Running	Manual (Trigger Start)	Local Service

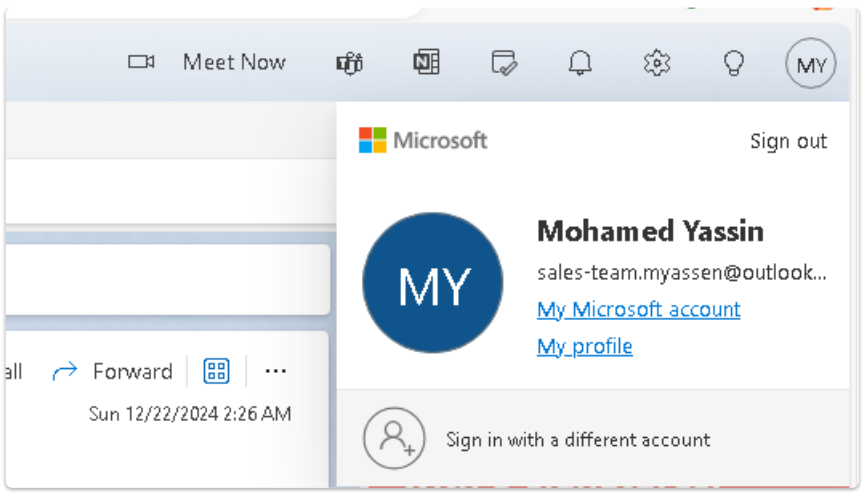
All Is Done Now Lets start Gaming

Scenario of Delivery

Outlook Phishing Mail from

From : `financial-team.maher.operationalfocus@outlook.com`

to : `sales-team.myassen@outlook.com`



MA **Maher Alaa<financial-team.maher.operationalfocus@outlook.com>**

To: You

Dear Mr. Yassen,

I hope this message finds you well. Please find attached Invoice #456789 for the web development services provided as per our agreement. Below are the key details for your reference:

Invoice Number: 456789

Invoice Date: December 22, 2024

Total Amount: $5,500.00

Due Date: January 5, 2025

Should you require any additional details or documents to process this invoice, please do not hesitate to contact me at ali.hassan@techsolutions.com or (555) 234-5678.

We sincerely appreciate your business and look forward to continuing our collaboration.

Thank you for your prompt attention to this matter.

Best regards,Ali HassanSenior ConsultantTech Solutions Ltd.

Let me know if you need further adjustments!

Please check Invoice PDF: invoice_2318362983713_823931342io.pdf.exe

Invoice Notes

- pdf extension manipulation using double extension technique
- Abusing Microsoft Collaboration Tools (OneDrive) by Hosting on it

`https://onedrive.live.com/?cid=153FC99CB596A0A2&id=153FC99CB596ADA29621s2df3d182e1c467a810bSaSbddf8f043&parld=153FC99CB596ADA2%21s3d8648ccSef34f2598d772f44d152Bae&e=OneUp`

Compromised Host Info

HostName	IP	Domain	User
COM10	192.168.1.10	RedAD19.lab	student

Incident Summery

Some Alert Hit on Suricata Customized Zeus Rules

Alerts Related to Suspicious DNS ,Http Requests Query to suspicious IP

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

Suricata-IDS

Inspection of Suricata IDS Alerts

i	Time	Event
>	12/21/24 9:31:42.302 PM	12/22/2024-02:31:42.302033 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:63752 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
>	12/21/24 9:31:32.582 PM	12/22/2024-02:31:32.582901 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:53807 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
>	12/21/24 9:31:32.579 PM	12/22/2024-02:31:32.579531 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:53806 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
>	12/21/24 9:31:32.579 PM	12/22/2024-02:31:32.579184 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:53805 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
>	12/21/24 9:31:32.578 PM	12/22/2024-02:31:32.578863 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:53804 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
>	12/21/24 9:31:32.578 PM	12/22/2024-02:31:32.578382 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:53803 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
>	12/21/24 9:31:32.572 PM	12/22/2024-02:31:32.572646 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:53802 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
>	12/21/24 9:31:32.568 PM	12/22/2024-02:31:32.568311 [**] [1:100003:1] Alert: Suspicious UDP traffic to malicious IP 85.114.128.127 on port 53 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.1.10:53801 -> 85.114.128.127:53 host = COMP10 source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small

Starting Investigation to find Initiative Process

- Using Sysmon we start Investigation on `Process Create` Event but within 40 min time range of execution
- Showed Only Image Names Executed to Ease the Process

```
index = "main" hast-"COHP10" earliest =- 4am latest =- 10m | where match(SourceName, "Sysman") | where match(Message, "Pracess Create") | rare limit-20 Inage
```

Share

v Search

```
index = "main" host="COMP10"  earliest=-40m latest=-10m   | where match(SourceName, "Sysmon")  | where match(Message, "Process Create")| rare limit=20 Image
```

✓ **197 events** (before 12/21/24 9:46:08.000 PM) No Event Sampling

Events Patterns Statistics (14) **Visualization**

Line Chart Format Trellis

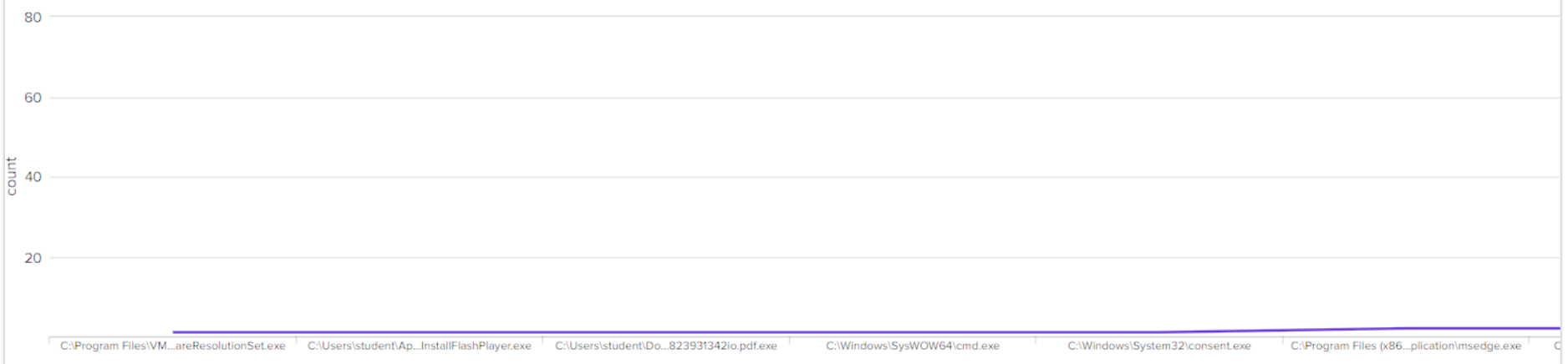
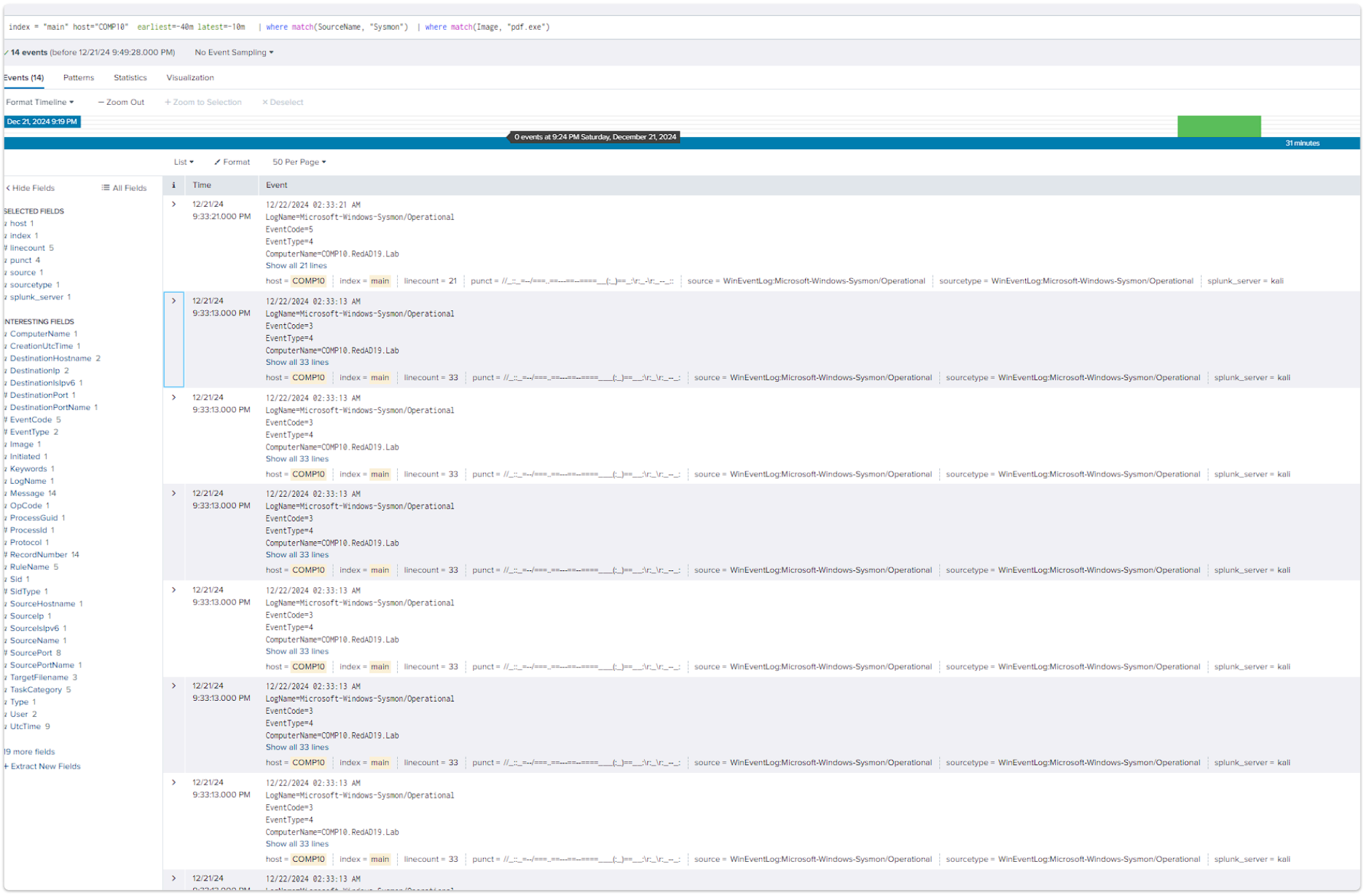


Image
C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe
C:\Users\student\AppData\Local\Temp\InstallFlashPlayer.exe
C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\System32\consent.exe
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
C:\Windows\SysWOW64\WerFault.exe
C:\Windows\System32\svchost.exe
C:\Program Files (x86)\Google\GoogleUpdater\132.0.6833.0\updater.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-admon.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe

- We Found Some Suspicious process using **double extension naming technique** which is IOA
  `C:\Users\student\Downloads\invoce_2318362983713_8239313421o.pdf.exe`
- tracking all events for that process

index = "main" host="COMP10" earliest =- 40m latest =- 10m |
match(Sourcellane, "Sysmon") | where match(Image, "pdf.exe")
```




# Investigation Findings

## Network Investigation
```

- Observed DNS Connection to IP `85.114.128.127` from

splunk>enterprise Apps ▾ | Administrator ▾ | 5 Messages ▾ | Settings ▾ | Activity ▾ | Help ▾ | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards | Search & Reporting

New Search

Save As ▾ | Create Table View | Close

```
index="main" host="COMP10"  | where match(SourceName, "Sysmon")  | where match(Image,"pdf.exe")  | where match(TaskCategory,"Network connection detected") | table  TaskCategory,Protocol, host, ComputerName, Image, SourceIp, SourcePort,
    DestinationIp, DestinationPort
```

Last 3 days

✓ **16 events** (12/20/24 3:36:54.000 PM to 12/23/24 3:36:54.000 PM) | No Event Sampling ▾ | Job ▾ | Smart Mode ▾

Events | Patterns | **Statistics (16)** | Visualization

20 Per Page ▾ | Format | Preview ▾

TaskCategory	Protocol	host	ComputerName	Image	SourceIp	SourcePort	DestinationIp	DestinationPort	EventCount
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53800	8.8.8.8	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53800	8.8.8.8	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53807	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53806	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53805	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53804	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53803	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53802	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53801	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53807	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53806	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53805	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53804	85.114.128.127	53	
Network connection detected (rule: NetworkConnect)	udp	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	192.168.1.10	53803	85.114.128.127	53	

- Search IP on ThreatIntel

AbuseIPDB » *85.114.128.127*

Check an IP Address, Domain Name, or Subnet
e.g. **51.158.252.96**, **microsoft.com**, or **5.188.10.0/24**

85.114.128.127 CHECK

85.114.128.127 was not found in our database

ISP	fast IT Colocation
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	srv11028.dus4.fastwebserver.de
Domain Name	wiit.cloud
Country	Germany
City	Munich, Bavaria

REPORT 85.114.128.127 | WHOIS 85.114.128.127

SPONSOR

AWS Marketplace Learn how to architect observable systems with free guides and top tools for AWS monitoring.

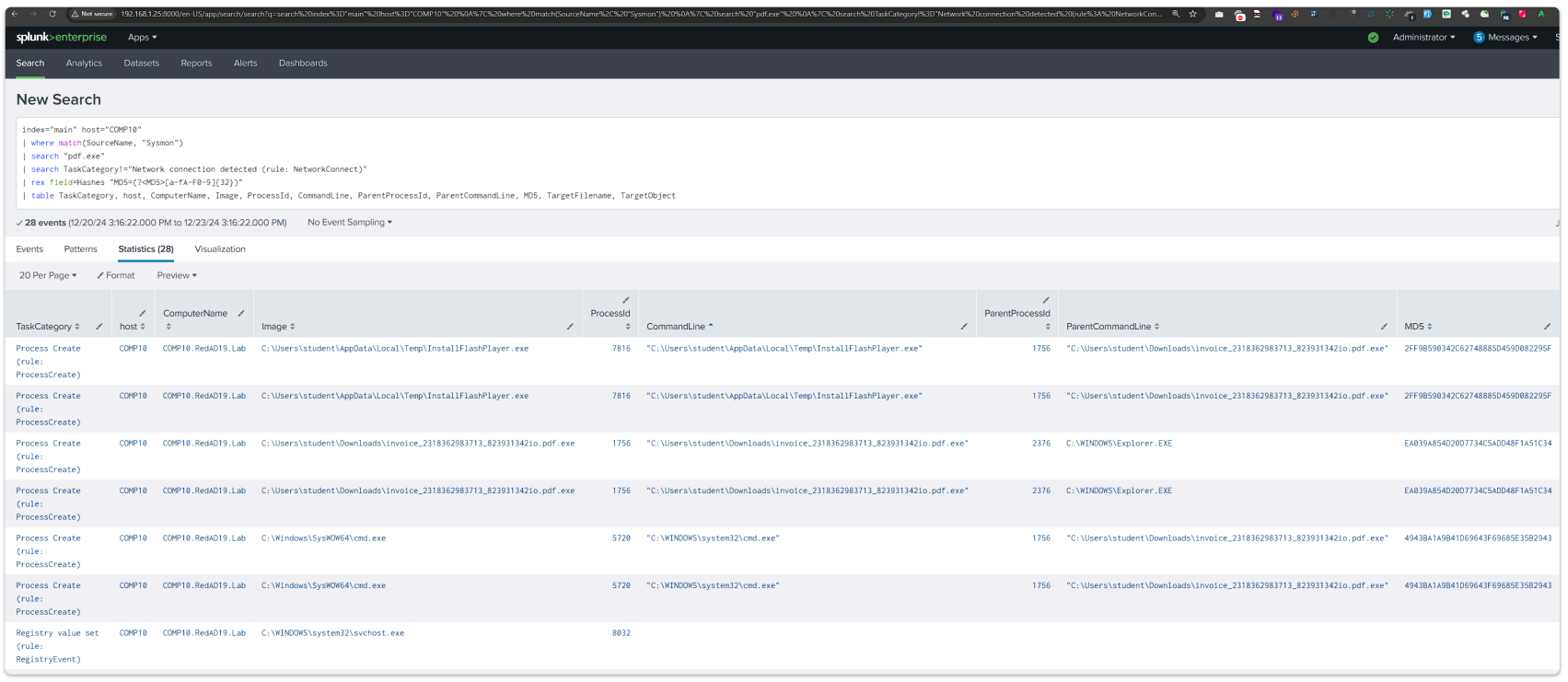
IP Abuse Reports for **85.114.128.127**:

This IP address has not been reported. File Report

Endpoint Investigation

- **Processes Information**
  - SEIM Query

```
index="main" host="COMP10"
| where match(SourceName, "Sysmon")
| search "pdf.exe"
| search TaskCategory!="Network connection detected (rule: NetworkConnect)"
| rex field=Hashes "MD5=(?<MD5>[a-fA-F0-9]{32})"
| table TaskCategory, host, ComputerName, Image, ProcessId, CommandLine,
ParentProcessId, ParentCommandLine, MD5, TargetFilename, TargetObject
```



- Processes Tree

`explorer.exe>invoice_2318362983713_8239313421o.pdf.exe >cmd.exe,InstallFlashPalyer.exe`

invoice_2318362983713_823931342io.pdf.exe

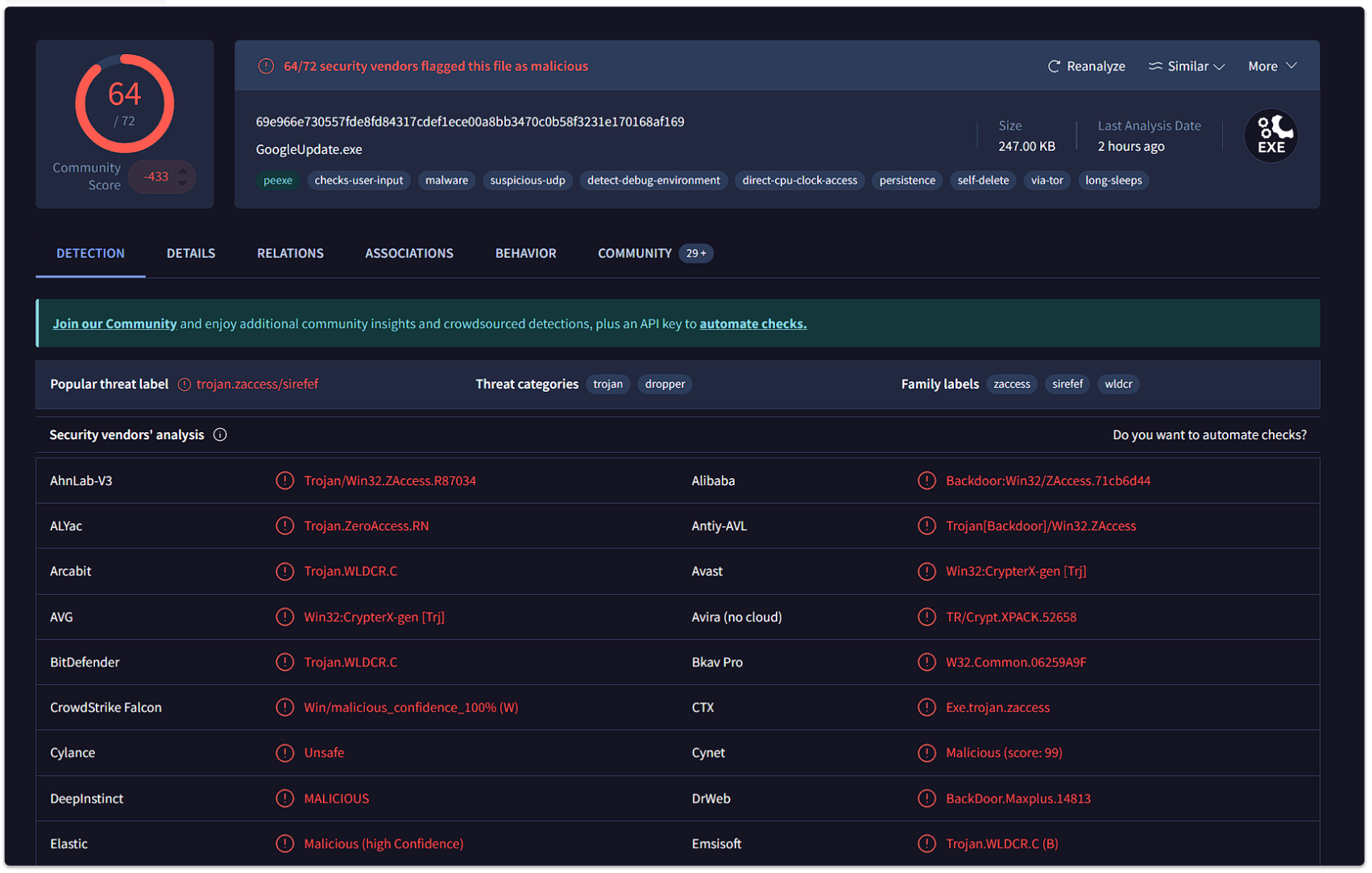
`Process ID` : 1756

`Parent Process` C:\Windows\explorer.exe

`Parent ID` 2376

`File Path` C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe

`File Hash` : EA039A854D20D7734C5ADD48F1A51C34



InstallFlashPalyer.exe

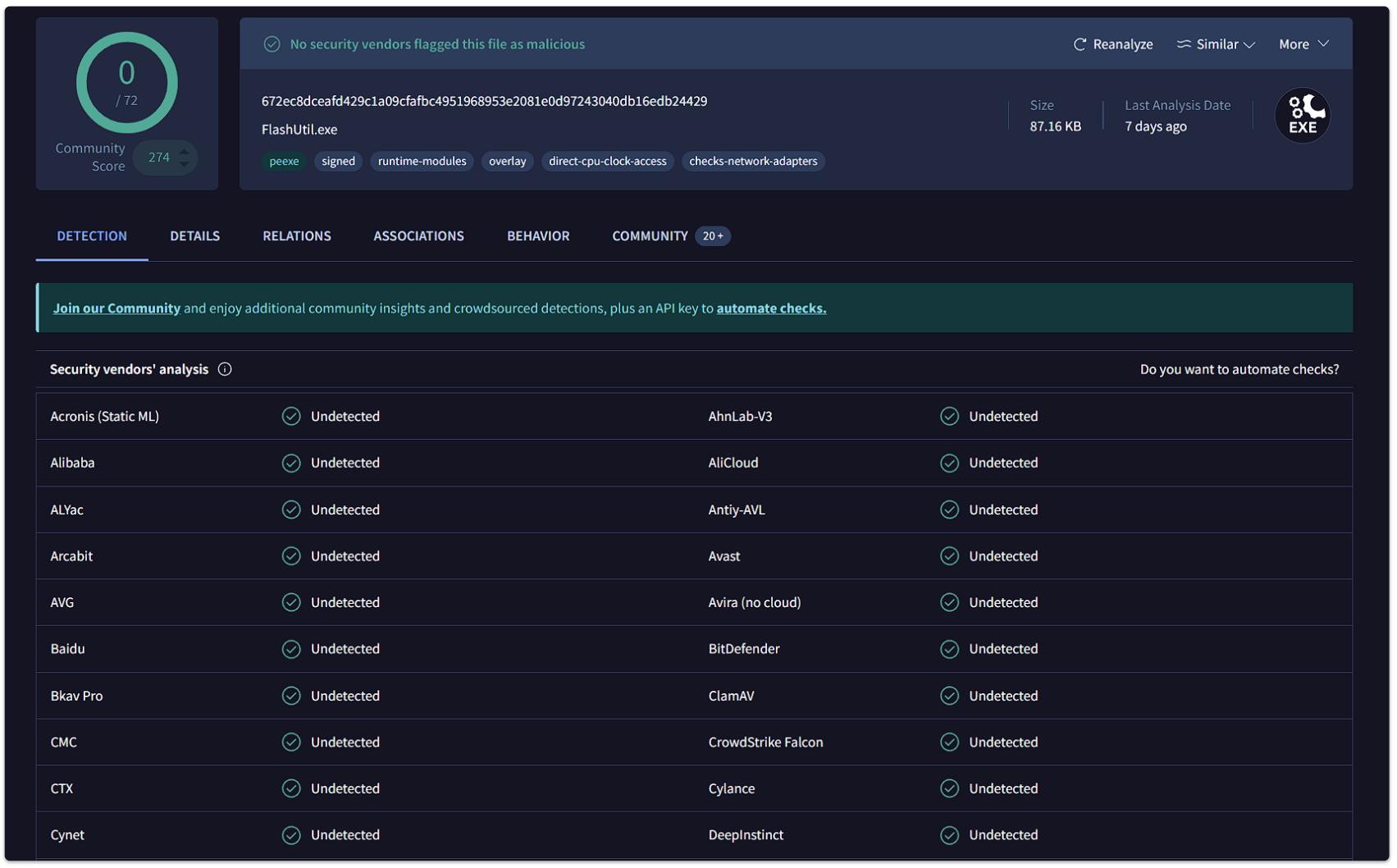
`Process ID 7` 7816

`Parent Process` C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe

`Parent ID` 1756

`File Path` C:\Users\student\AppData\Local\Temp\InstallFlashPlayer.exe

`File Hash` : 2FF9B590342C62748885D459D082295F



`Reputation`

- **Process Activities**
  - Created Files

```
index="main" host="COMP10"
| where match(SourceName, "Sysmon")
| search "pdf.exe"
| search TaskCategory!="Network connection detected (rule: NetworkConnect)"
| rex field=Hashes "MD5=(?<MD5>[a-fA-F0-9]{32})"
| table TaskCategory, host, ComputerName,Image,ProcessId,TargetFilename,TargetObject,MD5
```

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

```
index="main" host="COMP10"
| where match(SourceName, "Sysmon")
| search "pdf.exe"
| search TaskCategory!="Network connection detected (rule: NetworkConnect)"
| rex field=Hashes "MD5=(?<MD5>[a-fA-F0-9]{32})"
| table TaskCategory, host, ComputerName,Image,ProcessId,TargetFilename,TargetObject,MD5
```

✓ **28 events** (12/20/24 3:21:16.000 PM to 12/23/24 3:21:16.000 PM) No Event Sampling

Events Patterns **Statistics (28)** Visualization

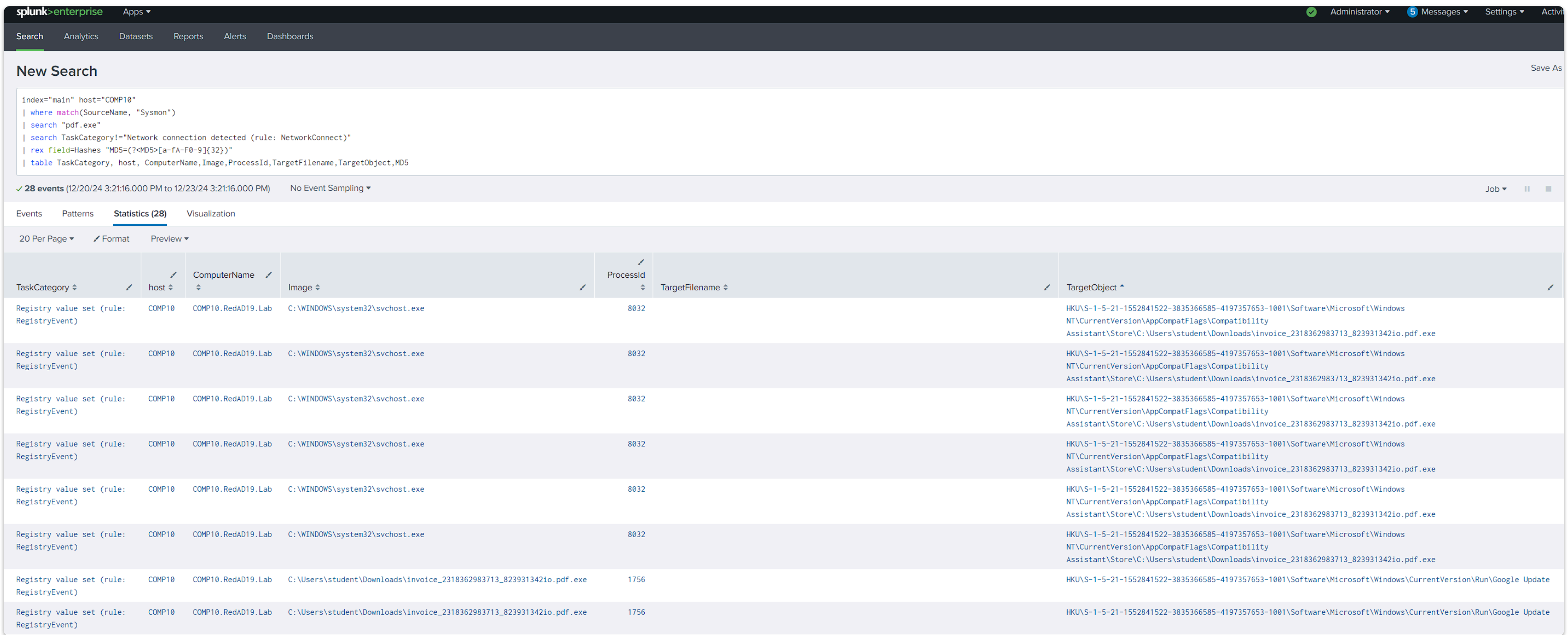
20 Per Page Format Preview

TaskCategory	host	ComputerName	Image	ProcessId	TargetFilename
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	1756	C:\Users\student\AppData\Local\Google\Desktop\Install\{3be6f3ea-f161-fd6c-0169-b17b29e868a5}\❤⚡»»\🗋☠~\exe.etadpUelgooG\{5a868e92b71b-9610-c6df-161f-ae3f6eb3}\🐍
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	1756	C:\Users\student\AppData\Local\Google\Desktop\Install\{3be6f3ea-f161-fd6c-0169-b17b29e868a5}\❤⚡»»\🗋☠~\exe.etadpUelgooG\{5a868e92b71b-9610-c6df-161f-ae3f6eb3}\🐍
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	1756	C:\Users\student\AppData\Local\Temp\InstallFlashPlayer.exe
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	1756	C:\Users\student\AppData\Local\Temp\InstallFlashPlayer.exe
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	1756	C:\Users\student\AppData\Local\Temp\msimg32.dll
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe	1756	C:\Users\student\AppData\Local\Temp\msimg32.dll
File creation time changed (rule: FileCreateTime)	COMP10	COMP10.RedAD19.Lab	C:\WINDOWS\Explorer.EXE	2376	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\WINDOWS\Explorer.EXE	2376	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe
File creation time changed (rule: FileCreateTime)	COMP10	COMP10.RedAD19.Lab	C:\WINDOWS\Explorer.EXE	2376	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe
File created (rule: FileCreate)	COMP10	COMP10.RedAD19.Lab	C:\WINDOWS\Explorer.EXE	2376	C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe

  - Created Regs

```
index="main" host="COMP10"
| where match(SourceName, "Sysmon")
| search "pdf.exe"
| search TaskCategory!="Network connection detected (rule: NetworkConnect)"
```

```
| rex field=Hashes "MD5=(?<MD5>[a-fA-F0-9]{32})"
| table TaskCategory, host, ComputerName,Image,ProcessId,TargetFilename,TargetObject,MD5
```



> *Created Files*

Process invoice_2318362983713_823931342io.pdf
Process ID : 1756
`C:\Users\student\AppData\Local\Google\Desktop\Install\{3be6f3ea-f161-fd6c-0169-b17b29e868a5}\❤$»»\Ɖ☠~\|xe.etadpUelgooG\{5a868e92b71b-9610-c6df-161f-ae3f6eb3}\ئسن`

`C:\Users\student\AppData\Local\Temp\InstallFlashPlayer.exe`
`C:\Users\student\AppData\Local\Temp\msimg32.dll`

> *Created Registries*

Process svchost.exe
Process ID : 8032
`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store\C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe`

`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store\C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe`
`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store\C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe`
`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store\C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe`
`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store\C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe`
`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store\C:\Users\student\Downloads\invoice_2318362983713_823931342io.pdf.exe`
Process invoice_2318362983713_823931342io.pdf.exe
Process ID : 1756
`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\Windows\CurrentVersion\Run\Google Update`
`HKU\S-1-5-21-1552841522-3835366585-4197357653-1001\Software\Microsoft\Windows\CurrentVersion\Run\Google Update`

Analysis Highlights

- Very Low Amount of Traffic successful no reverse shell
- Downloads\ location means File Downloaded By the User
- explorer.exe parent means Executed By User
- Registries Created by svchost.exe IOA of Process Injection

TTP Time Line

Tactic	Technique	Procedure/Activity	Detection Methods	Mitigation Actions
Reconnaissance	Abuse MS Collaboration Tools	Phishing email with a malicious file attachment hosted via OneDrive.	Not Detected	- Implement advanced email filtering. - Train users on identifying phishing emails.
Delivery	Spearphishing Attachment	Malicious file (`xxxpdf.exe`) disguised as a legitimate document.	Not Detected	- Use endpoint protection solutions that block known malware. - Educate users to avoid unknown files.
Execution	User Execution	User executes the malicious file, initiating the payload.	- Monitor for new process creation from unusual file paths. using Sysmon logs, Splunk).	- Restrict execution of non-whitelisted files. - Limit privileges of user accounts.
Command and Control (C2)	Malicious DNS Requests	Malware queries external malicious domains for communication.	- Suricata Integration DNS logs	- Implement DNS filtering solutions. - Block access to known malicious domains.
Execution	Ingress Tool Transfer-Dropping Executable File	Malware downloads additional payloads or scripts.	Not Detected	- Block access to non-approved repositories. - Implement network-based intrusion prevention.
Defense Evasion	Process Injection	Injects into `svchost.exe` to evade detection and blend into legitimate activity.	- Monitor for unusual memory usage or thread injections in `svchost.exe`.using Sysmon logs, Splunk).	- Enable Credential Guard and modern Windows protections. - Investigate anomalies in high-privileged processes.
Discovery	- Query Registry -System Information Discovery		Not Detecetd	Anomalous Behavior Detection and Analysis Application Whitelisting Privileged Account Management
Persistence	Registry Modification	Malware establishes persistence by creating or modifying registry keys.	- Registry monitoring for unusual changes (e.g., Sysmon logs, Splunk).	- Regularly audit registry keys. - Use tools to lock down

Tactic	Technique	Procedure/Activity	Detection Methods	Mitigation Actions
				critical registry paths.

Incident & Response Process

Preparation (Done)

This step involves setting up processes, tools, and resources to ensure an organization can effectively respond to incidents.

- Develop and document an Incident Response Plan (IRP).
- Establish an Incident Response Team (IRT) with defined roles and responsibilities.
- Deploy and configure security tools like SIEMs, EDRs, and firewalls.
- Train staff with cybersecurity awareness and conduct regular incident response drills (e.g., tabletop exercises).
- Maintain an updated inventory of critical assets and their associated risks.
- Develop playbooks for common attack scenarios (e.g., phishing, ransomware, data breaches).

Identification (Done)

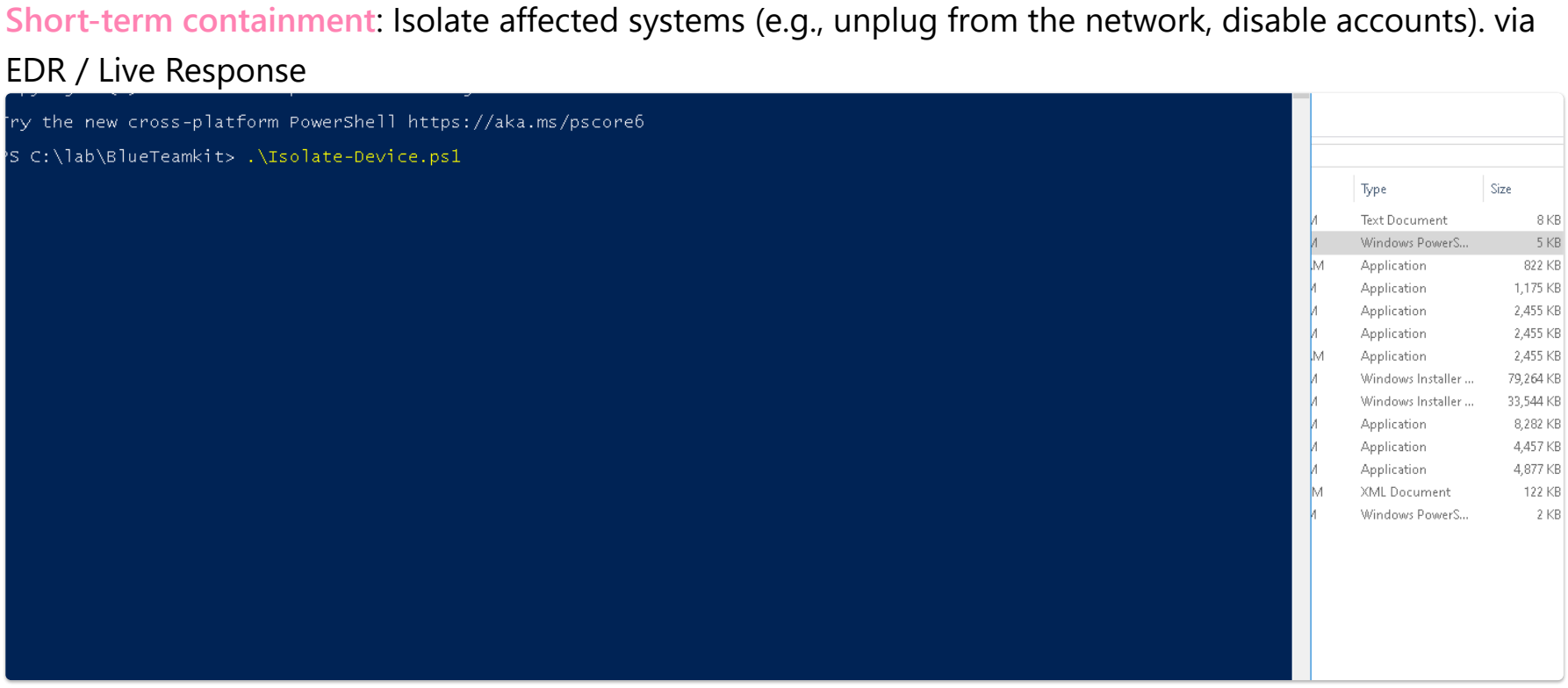
In this phase, we detect and confirm potential security incidents by analyzing alerts, logs, and behaviors.

- Monitor systems and networks using tools like SIEM, IDS/IPS, and endpoint security tools.
- Analyze alerts and anomalies to confirm if an incident is occurring.
- Gather forensic data, including logs, system snapshots, and network traffic.
- Classify and prioritize the incident based on its severity, impact, and type (e.g., phishing, ransomware).

Containment

This step focuses on stopping the spread of the attack and limiting its damage.

- Short-term containment: Isolate affected systems (e.g., unplug from the network, disable accounts). via EDR / Live Response



- Long-term containment: Set up temporary solutions, such as deploying new firewalls or network segments.
- Block malicious domains, IPs, and email addresses in firewalls or DNS settings.
  Here We Don't Need Logging Utils such sysmon,suricata
  We Need Action Utils

Instead of NDR,IPS Will Use Windows Firewall Rules
`New-NetFirewallRule -DisplayName "Block Outbound Traffic to $ip" -Direction Outbound -RemoteAddress "85.114.128.127" -Action Block -Protocol Any

```
New-NetFirewallRule -DisplayName "Block Inbound Traffic from $ip" -Direction Inbound -RemoteAddress "85.114.128.127" -Action Block -Protocol Any
```

Instead of EDR Will Use WindowsAV Rules

```
Add-MpPreference -ThreatIDDefaultAction_Actions 2 -ThreatIDDefaultAction_Ids EA039A854D20D7734C5ADD48F1A51C34
```

- Implement patches or workarounds to prevent further exploitation.
- Preserve evidence for further investigation (e.g., disk images, memory dumps).

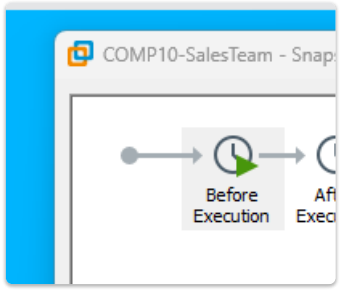
Eradication

In this phase, you remove the threat from your environment to prevent further compromise.

- Identify and remove malware, backdoors, or malicious files.
- Patch exploited vulnerabilities in systems, software, or configurations.
- Scan systems thoroughly to ensure no remnants of the attack remain.
- Harden systems and networks against similar attacks in the future.

Recovery

The goal of this step is to restore normal operations while ensuring the environment is secure.



- Rebuild or restore affected systems from clean backups.
- Verify that all systems are functioning properly and securely.
- Monitor systems closely for any signs of lingering threats.
- Gradually reintroduce affected systems to the network.

Incident Analysis (Digital Forensics)

Short Malware Analysis Hands-On

| For Emulation will Use Public tools

Static Malware Analysis

File Information

- `Name :` invoice_2318362983713_823931342io.pdf.exe
- `Hash` : 69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
- Reputation 64/72
- Signature : Not Signed

History

Creation Time	**2013-11-25 10:32:03 UTC**
First Seen In The Wild	2019-07-10 23:59:42 UTC
First Submission	2013-11-25 17:21:04 UTC

PE Info

Magic	**PE32 executable (GUI) Intel 80386, for MS Windows**
File type	Win32 EXE
TrID	Win32 Executable MS Visual C++ (generic) (47.3%
Target Machine	Intel 386 or later processors and compatible processors

Dropped Files

Scanned Date	Detections	File Type	Name	SHA-256
2022-07-02	51 / 68	Win32 DLL	`desktop.ini`	`00e3d0987b2edd740f1dcbbfb5a`
2020-09-23	59 / 70	Win32 DLL	`1x32.dll`	`315387a3e83aae9a667b82635b2`
-	-	-	-	`68ba25c6623b40c2a9cd9fbbcdc`
2024-12-24	64 / 72	Win32 EXE	`invoice_2318362983713_823931342io.pdf.exe`	`69e966e730557fde8fd84317cde`
2024-05-23	50 / 74	Win32 DLL	`x64.dll`	`8c803f3de87cf264f09ae57b4eb`
-	-	-	-	`92d89ba74874f506a644576a358`
-	-	-	-	`a1b513a59a9a2ebf8cbf91f580b`

Executable Sections

Section Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
`.text`	4096	46449	46592	6.71	`679fbf23d7317d8207d350b532908f0a`
`.data`	53248	75953	76288	6.13	`73fdae90c1738941b6afec633c45972e`
`.itext`	131072	2125	2560	4.82	`7f89ad170ffea80a9c7304edf9c7f32c`
`.pdata`	135168	97470	97792	6.77	`a8448d1b94e56bc8f80ed852445884c1`
`.rsrc`	233472	22770	23040	6.14	`b3af18982aee2e1b39915237800c877e`
`.reloc`	258048	5612	5632	6.44	`37469a130e838cd467ff44551f2a43fb`

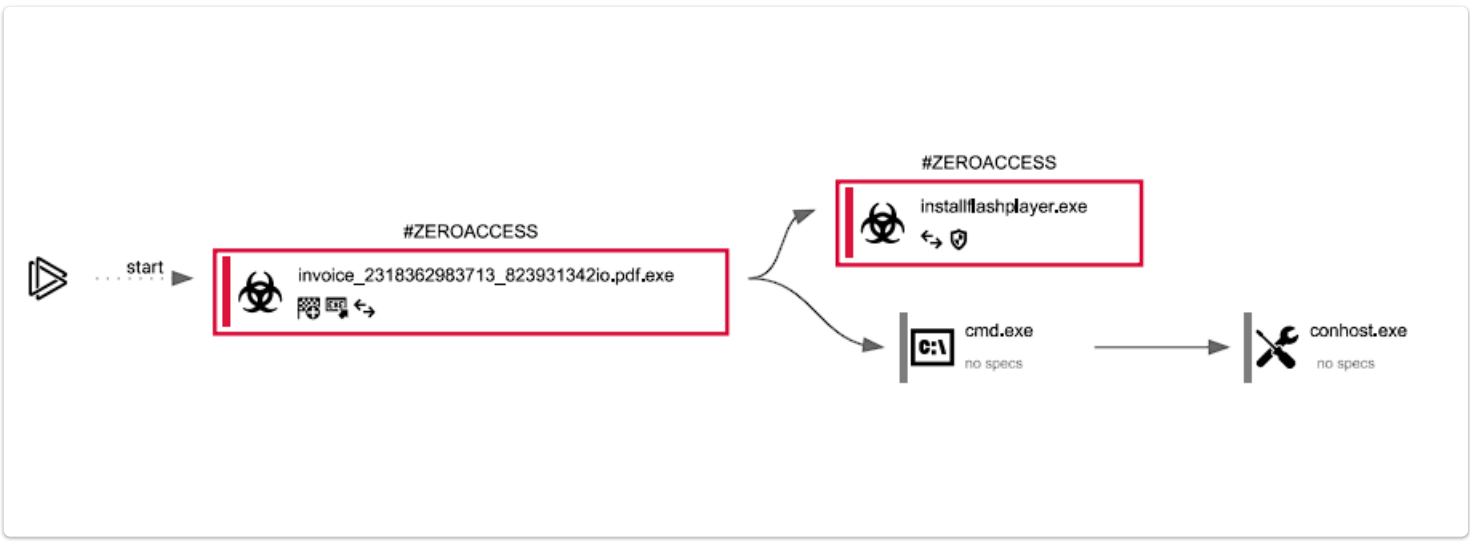
IAT Highlights

DLL	Malicious Potential Imported APIs
`SHLWAPI.dll`	PathCombineW, PathIsPrefixA, PathIsRelativeA, PathIsRootW, PathIsSameRootA, PathIsUNCServerA, PathMatchSpecW, PathRelativePathToW
`KERNEL32.dll`	CreateFileMappingA, GetCurrentThread, FreeLibrary, GetCompressedFileSizeA
`USER32.dll`	GetAsyncKeyState, SetLastErrorEx, SwapMouseButton, AllowSetForegroundWindow

1. SHLWAPI.dll:
    - Functions like `PathCombineW`, `PathIsPrefixA`, and `PathIsRelativeA` can be used for path manipulation, potentially targeting sensitive directories.
    - Functions such as `PathIsUNCServerA` and `PathMatchSpecW` may help attackers find and abuse network shares.
2. KERNEL32.dll:
    - `CreateFileMappingA` can facilitate inter-process memory access, which attackers might use for injecting or sharing payloads.
    - `FreeLibrary` and `GetCurrentThread` can manipulate thread contexts or remove modules dynamically.
3. USER32.dll:
    - Functions like `GetAsyncKeyState` can capture keystrokes.
    - `SwapMouseButton` and `AllowSetForegroundWindow` can be used to manipulate the UI for phishing or evasion.

Dynamic Malware Analysis

Process



Process Activities

PID	CMD	Path	Indicators	Parent process
6404	"C:\Users\admin\AppData\Local\Temp\invoice_2318362983713_823931342io.pdf.exe"	C:\Users\admin\AppData\Local\Temp\invoice_2318362983713_823931342io.pdf.exe		explorer.exe

- Process Added to Sturup
- Network Connection
- Executable File Dropped

6812	"C:\Users\admin\AppData\Local\Temp\InstallFlashPlayer.exe"	C:\Users\admin\AppData\Local\Temp\InstallFlashPlayer.exe		invoice_2318362983713_823931342io.pdf.exe

Information

User:	admin	Company:	Adobe Systems, Inc.
Integrity Level:	HIGH	Description:	Adobe® Flash® Player Installer/Uninstaller 11.0 r1
Version:	11,0,1,152		

- Integrity Level Elevation

- Network Connection

Registry activity

Total events	Read events	Write events	Delete events
1 749	1 739	10	0

Modification events

(PID) Process: (6404) invoice_2318362983713_823931342io.pdf.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: write Name: Google Update
Value: "C:\Users\admin\AppData\Local\Google\Desktop\Install\{81b8c3da-9d80-cef9-7346-aaa39584b477}\♥⚡»\Q※ᵔ\< "exe.etadpUelgooG\{774b48593aaa-6437-9fec-08d9-ad3c8b18}\c~ڹ

(PID) Process: (6404) invoice_2318362983713_823931342io.pdf.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write Name: SlowContextMenuEntries
Value: 6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E232827701000001140200000000000C000000000000000468D0000006078A409B011A54DAFA526D86198A7803901000062B06A59D2B415429F74E9109B0A815348010000

(PID) Process: (6404) invoice_2318362983713_823931342io.pdf.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write Name: SlowContextMenuEntries
Value: 6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E232827701000060B81DB4E48ED2119906E49FADC173CACB0000006078A409B011A54DAFA526D86198A7803901000062B06A59D2B415429F74E9109B0A815348010000

(PID) Process: (6404) invoice_2318362983713_823931342io.pdf.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\OneDrive\Accounts
Operation: write Name: LastUpdate
Value: F0A76A6700000000

(PID) Process: (6404) invoice_2318362983713_823931342io.pdf.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write Name: SlowContextMenuEntries
Value: 6024B221EA3A6910A2DC08002B30309D23020000BD0E0C47735D584D9CEDE91E22E232827701000060B81DB4E48ED2119906E49FADC173CACB0000006078A409B011A54DAFA526D86198A7803901000062B06A59D2B415429F74E9109B0A815348010000

(PID) Process: (6812) InstallFlashPlayer.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write Name: CachePrefix
Value:

(PID) Process: (6812) InstallFlashPlayer.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write Name: CachePrefix
Value: Cookie:

Files activity

Executable files	Suspicious files	Text files	Unknown types
3	1	0	0

Dropped files

PID	Process	Filename	Type
6404	invoice_2318362983713_823931342io.pdf.exe	C:\Users\admin\AppData\Local\Google\Desktop\Install\{81b8c3da-9d80-cef9-7346-aaa39584b477}\♥⚡»\Q※ᵔ\-9fec-08d9-ad3c8b18}\c~ڹ@\{774b48593aaa-6437 MD5: C33450B09B7CF790FAE4F870FA1BA7BD SHA256: 9A3060B9FFF6231716104D37D0C5AC91B53949FF318E38C79EE6AA1368D4BC67	binary
6404	invoice_2318362983713_823931342io.pdf.exe	C:\Users\admin\AppData\Local\Google\Desktop\Install\{81b8c3da-9d80-cef9-7346-aaa39584b477}\♥⚡»\Q※ᵔ\-9fec-08d9-ad3c8b18}\c~ڹexe.etadpUelgooG\{774b48593aaa-6437 MD5: EA039A854D20D7734C5ADD48F1A51C34 SHA256: 69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169	executable
6404	invoice_2318362983713_823931342io.pdf.exe	C:\Users\admin\AppData\Local\Temp\InstallFlashPlayer.exe MD5: 2FF9B590342C62748885D459D082295F SHA256: 672EC8DCEAFD429C1A09CFAFBC4951968953E2081E0D97243040DB16EDB24429	executable
6404	invoice_2318362983713_823931342io.pdf.exe	C:\Users\admin\AppData\Local\Temp\msimg32.dll MD5: E051308C2F0C1B280514C99AABD36E34 SHA256: DDF7CCAB32E8C0EE6294DF2591EFAC632C27C61D073B86B97DE62311F9379212	executable

Process Connection

5064	SearchApp.exe	104.126.37.163:443	www.bing.com	Akamai International B.V.	DE	whitelisted
5732	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
–	–	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
6404	invoice_2318362983713_823931342io.pdf.exe	85.114.128.127:53	–	–	–	malicious
1076	svchost.exe	184.28.89.167:443	go.microsoft.com	AKAMAI-AS	US	whitelisted
1176	svchost.exe	40.126.32.134:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1176	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
6812	InstallFlashPlayer.exe	85.114.128.127:53	–	–	–	malicious
6812	InstallFlashPlayer.exe	104.102.58.45:80	fpdownload.macromedia.com	AKAMAI-AS	DE	whitelisted
4712	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4712	MoUsoCoreWorker.exe	2.16.164.120:80	crl.microsoft.com	Akamai International B.V.	NL	whitelisted
4712	MoUsoCoreWorker.exe	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
936	SIHClient.exe	52.149.20.212:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
936	SIHClient.exe	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
936	SIHClient.exe	40.69.42.241:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6504	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6504	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
6504	backgroundTaskHost.exe	20.199.58.43:443	fd.api.iris.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
4712	MoUsoCoreWorker.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
3976	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
5732	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted

Network DNS Requests

DNS requests

Domain	IP	Reputation
google.com	142.250.74.206	whitelisted
www.bing.com	104.126.37.163 104.126.37.179 104.126.37.177 104.126.37.130 104.126.37.136 104.126.37.171 104.126.37.178 104.126.37.129 104.126.37.123	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
j.maxmind.com	–	shared
go.microsoft.com	184.28.89.167	whitelisted
login.live.com	40.126.32.134 40.126.32.140 20.190.160.14 40.126.32.74 20.190.160.22 40.126.32.133 40.126.32.72 20.190.160.17	whitelisted
fpdownload.macromedia.com	104.102.58.45	whitelisted
settings-win.data.microsoft.com	40.127.240.158 20.73.194.208 51.104.136.2	whitelisted
crl.microsoft.com	2.16.164.120 2.16.164.49	whitelisted
www.microsoft.com	88.221.169.152	whitelisted
slscr.update.microsoft.com	52.149.20.212	whitelisted
fe3cr.delivery.mp.microsoft.com	40.69.42.241	whitelisted
arc.msn.com	20.223.35.26	whitelisted
fd.api.iris.microsoft.com	20.199.58.43	whitelisted

Network HTTP Requests

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6812	InstallFlashPlayer.exe	GET	404	104.102.58.45:80	http://fpdownload.macromedia.com/get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z	unknown	–	–	whitelisted
–	–	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxduNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	–	–	whitelisted
1176	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
4712	MoUsoCoreWorker.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
4712	MoUsoCoreWorker.exe	GET	200	2.16.164.120:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
936	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
936	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted
6504	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAUZZSZEml49Gjh0j13P68w%3D	unknown	–	–	whitelisted

Short Endpoint Forensics Hands-On

Here We Will not Deepdive on All Forensics Lifecycle
Just will Capture some Hints of Memory Forensics for demonstration

Memory Forensics

After Dumping memory

Using Volatility

Installation

```
pip install volatility3
```

Deep Dive in OS Information

Windows Image Info

```
sudo vol -f  zeus2x4.vmem windows.info
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$  sudo vol -f zeus2x4.vmem windows.info
Volatility 3 Framework 2.8.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly proce
ed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0x804d7000
DTB     0x39000
Symbols file:///usr/local/lib/python3.12/dist-packages/volatility3/symbols/windows/ntoskrnl.pdb/1B2D0DFE2FB942758D615C901BE04692-2.json.xz
Is64Bit False
IsPAE   False
layer_name      0 WindowsIntel
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x8054cde0
NTBuildLab      2600.xpsp_sp3_gdr.090804-1435
CSDVersion      3
KdVersionBlock  0x8054cdb8
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2010-09-09 19:56:54+00:00
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Tue Aug  4 15:14:34 2009
```

Listing All Assigned Security Privileges

```
sudo vol -f zeus2x4.vmem   windows.privileges.Privs
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$ sudo vol -f zeus2x4.vmem    windows.privileges.Privs
Volatility 3 Framework 2.8.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to c
ed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Value   Privilege       Attributes      Description

4       System  7       SeTcbPrivilege  Present,Enabled,Default Act as part of the operating system
4       System  2       SeCreateTokenPrivilege  Present Create a token object
4       System  9       SeTakeOwnershipPrivilege        Present Take ownership of files/objects
4       System  15      SeCreatePagefilePrivilege       Present,Enabled,Default Create a pagefile
4       System  4       SeLockMemoryPrivilege   Present,Enabled,Default Lock pages in memory
4       System  3       SeAssignPrimaryTokenPrivilege   Present Replace a process-level token
4       System  5       SeIncreaseQuotaPrivilege        Present Increase quotas
4       System  14      SeIncreaseBasePriorityPrivilege Present,Enabled,Default Increase scheduling priority
4       System  16      SeCreatePermanentPrivilege      Present,Enabled,Default Create permanent shared objects
4       System  20      SeDebugPrivilege        Present,Enabled,Default Debug programs
4       System  21      SeAuditPrivilege        Present,Enabled,Default Generate security audits
4       System  8       SeSecurityPrivilege     Present Manage auditing and security log
4       System  22      SeSystemEnvironmentPrivilege    Present Edit firmware environment values
4       System  23      SeChangeNotifyPrivilege Present,Enabled,Default Receive notifications of changes to files or directories
4       System  17      SeBackupPrivilege       Present Backup files and directories
4       System  18      SeRestorePrivilege      Present Restore files and directories
4       System  19      SeShutdownPrivilege     Present Shut down the system
4       System  10      SeLoadDriverPrivilege   Present Load and unload device drivers
4       System  13      SeProfileSingleProcessPrivilege Present,Enabled,Default Profile a single process
4       System  12      SeSystemtimePrivilege   Present Change the system time
4       System  25      SeUndockPrivilege       Present Remove computer from docking station
4       System  28      SeManageVolumePrivilege Present Manage the files on a volume
4       System  29      SeImpersonatePrivilege  Present,Enabled,Default Impersonate a client after authentication
4       System  30      SeCreateGlobalPrivilege Present,Enabled,Default Create global objects
596     smss.exe        7       SeTcbPrivilege  Present,Enabled,Default Act as part of the operating system
```

Listing All Created Files

```
sudo vol -f zeus2x4.vmem    windows.filescan.FileScan
```

```
┌──(kali㉿kali)-[~/Zeus/pdump]
└─$ vol -f ../zeus2x4.vmem -o /home/kali/Zeus/pdump  windows.filescan
Volatility 3 Framework 2.8.0
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. These should be placed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
Offset  Name

0x1e7c0d8       \WINDOWS\system32\drivers\tcpip6.sys
0x1e80278       \Program Files\IDA\procs\nec850.w32
0x1e80318       \Program Files\IDA\loaders\qnx.ldw
0x1e803b0       \Program Files\IDA\loaders\pilot.ldw
0x1e809b0       \WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
0x1e80a48       \WINDOWS\system32
0x1e80cd0       \WINDOWS\system32\oleaut32.dll
0x1e80e10       \WINDOWS\system32\ntdll.dll
0x1e80f28       \Program Files\IDA\procs\avr.w32
0x1e81028       \Program Files\IDA\plugins\findcrypt.plw
0x1e81228       \Program Files\IDA\ida.wll
0x1e81340       \WINDOWS\system32\clusapi.dll
0x1e814b8       \WINDOWS\system32\shlwapi.dll
0x1e815c8       \Documents and Settings\Administrator\Application Data\Obyt\ihah.exe
0x1e81a68       \WINDOWS\system32\crypt32.dll
0x1e81c10       \Program Files\IDA\ids\win\wininet.ids
0x1e81d88       \WINDOWS\pchealth\helpctr\DataColl\CollectedData_415.xml
0x1e822e8       \Program Files\Immunity Inc\Immunity Debugger\OllyDump.dll
0x1e82380       \Program Files\Immunity Inc\Immunity Debugger\Cmdline.dll
0x1e82e78       \WINDOWS\explorer.exe
0x1e84d18       \WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
0x1e85228       \Endpoint
0x1e85920       \WINDOWS\WindowsUpdate.log
0x1e861b8       \WINDOWS\system32\mpr.dll
0x1e86368       \boot.ini
0x1e86430       \Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlaccess.dll
0x1e866f8       \WINDOWS\system32\advapi32.dll
0x1e871b8       \WINDOWS\system32\msi.dll
0x1e87b40       \lsass
0x1e89360       \Documents and Settings\Administrator\Desktop\FileInsight.lnk
0x1e8be60       \Documents and Settings\All Users\Desktop\PDFCreator.lnk
0x1e8bef8       \Documents and Settings\All Users\Desktop\FlexHEX.lnk
0x1e8d2b8       \$Directory
0x1e8dd38       \WINDOWS\Installer\8b5f80.msi
0x1e8ddd0       \net\NtControlPipe16
0x1eaa268       \$Directory
0x1eaa670       \$Directory
0x1eabb90       \WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
0x1eabd28       \WINDOWS\system32\cscript.exe
0x1eabdc0       \WINDOWS\system32\jscript.dll
0x1eac4d8       \WINDOWS\system32\user32.dll
0x1ead338       \WINDOWS\system32\mfcsubs.dll
0x1ead8e0       \WINDOWS\inf\unregmp2.exe
```

Listing All loaded Dlls

```
sudo vol -f zeus2x4.vmem    windows.dlllist.DllList
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$ sudo vol -f zeus2x4.vmem    windows.dlllist.DllList
Volatility 3 Framework 2.8.0
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. These should be placed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Base    Size    Name    Path    LoadTime        File output

596     smss.exe        0x48580000      0xf000  smss.exe        \SystemRoot\System32\smss.exe   N/A     Disabled
596     smss.exe        0x7c900000      0xb2000 -       -       N/A     Disabled
668     csrss.exe       0x4a680000      0x5000  csrss.exe       \??\C:\WINDOWS\system32\csrss.exe       N/A     Disabled
668     csrss.exe       0x7c900000      0xb2000 -       -       N/A     Disabled
668     csrss.exe       0x75b40000      0xb000  CSRSRV.dll      C:\WINDOWS\system32\CSRSRV.dll  N/A     Disabled
668     csrss.exe       0x75b50000      0x10000 basesrv.dll     C:\WINDOWS\system32\basesrv.dll N/A     Disabled
668     csrss.exe       0x75b60000      0x4b000 winsrv.dll      C:\WINDOWS\system32\winsrv.dll  N/A     Disabled
668     csrss.exe       0x77f10000      0x49000 GDI32.dll       C:\WINDOWS\system32\GDI32.dll   N/A     Disabled
668     csrss.exe       0x7c800000      0xf6000 KERNEL32.dll    C:\WINDOWS\system32\KERNEL32.dll        N/A     Disabled
668     csrss.exe       0x7e410000      0x91000 USER32.dll      C:\WINDOWS\system32\USER32.dll  N/A     Disabled
668     csrss.exe       0x7e720000      0xb0000 sxs.dll C:\WINDOWS\system32\sxs.dll      N/A     Disabled
668     csrss.exe       0x77dd0000      0x9b000 ADVAPI32.dll    C:\WINDOWS\system32\ADVAPI32.dll        N/A     Disabled
668     csrss.exe       0x77e70000      0x92000 RPCRT4.dll      C:\WINDOWS\system32\RPCRT4.dll  N/A     Disabled
668     csrss.exe       0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll N/A     Disabled
692     winlogon.exe    0x1000000       0x81000 winlogon.exe    \??\C:\WINDOWS\system32\winlogon.exe    N/A     Disabled
692     winlogon.exe    0x7c900000      0xb2000 -       -       N/A     Disabled
692     winlogon.exe    0x7c800000      0xf6000 kernel32.dll    C:\WINDOWS\system32\kernel32.dll        N/A     Disabled
692     winlogon.exe    0x77dd0000      0x9b000 ADVAPI32.dll    C:\WINDOWS\system32\ADVAPI32.dll        N/A     Disabled
692     winlogon.exe    0x77e70000      0x92000 RPCRT4.dll      C:\WINDOWS\system32\RPCRT4.dll  N/A     Disabled
692     winlogon.exe    0x77fe0000      0x11000 Secur32.dll     C:\WINDOWS\system32\Secur32.dll N/A     Disabled
692     winlogon.exe    0x776c0000      0x12000 AUTHZ.dll       C:\WINDOWS\system32\AUTHZ.dll   N/A     Disabled
```

Listing all Running Services

```
sudo vol -f zeus2x4.vmem    windows.svcscan.SvcScan
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$ sudo vol -f zeus2x4.vmem    windows.svcscan.SvcScan
Volatility 3 Framework 2.8.0
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. These should be placed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
Offset  Order   PID     Start   State   Type    Name    Display Binary  Binary (Registry)       Dll

0x381e90        1       N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   Abiosdsk        Abiosdsk        N/A     -       -
0x381f20        2       N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   abp480n5        abp480n5        N/A     -       -
0x381fb0        3       N/A     SERVICE_DEMAND_START    SERVICE_RUNNING SERVICE_KERNEL_DRIVER   ac97intc        Intel(r) 82801 Audio Driver Install S
ervice (WDM)    \Driver\ac97intc        -       -
0x382040        4       N/A     SERVICE_BOOT_START      SERVICE_RUNNING SERVICE_KERNEL_DRIVER   ACPI    Microsoft ACPI Driver   \Driver\ACPI    -   -
0x3820c8        5       N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   ACPIEC  ACPIEC  N/A     -       -
0x382158        6       N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   adpu160m        adpu160m        N/A     -       -
0x3821e8        7       N/A     SERVICE_DEMAND_START    SERVICE_STOPPED SERVICE_KERNEL_DRIVER   aec     Microsoft Kernel Acoustic Echo Canceller    N
/A      -       -
0x382270        8       N/A     SERVICE_SYSTEM_START    SERVICE_RUNNING SERVICE_KERNEL_DRIVER   AFD     AFD     \Driver\AFD     -       -
0x3822f8        9       N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   Aha154x Aha154x N/A     -       -
0x382388        10      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   aic78u2 aic78u2 N/A     -       -
0x382418        11      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   aic78xx aic78xx N/A     -       -
0x3824a8        12      N/A     SERVICE_DEMAND_START    SERVICE_STOPPED SERVICE_KERNEL_DRIVER   akshasp Aladdin HASP Key        N/A     -       -
0x382538        13      N/A     SERVICE_DEMAND_START    SERVICE_STOPPED SERVICE_KERNEL_DRIVER   aksusb  Aladdin USB Key N/A     -       -
0x3825c8        14      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_WIN32_SHARE_PROCESS     Alerter Alerter N/A     -       -
0x382658        15      2588    SERVICE_DEMAND_START    SERVICE_RUNNING SERVICE_WIN32_OWN_PROCESS       ALG     Application Layer Gateway Service   C
:\WINDOWS\System32\alg.exe      -       -
0x3826e0        16      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   AliIde  AliIde  N/A     -       -
0x382770        17      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   amsint  amsint  N/A     -       -
0x382800        18      N/A     SERVICE_DEMAND_START    SERVICE_STOPPED SERVICE_WIN32_SHARE_PROCESS     AppMgmt Application Management  N/A     -   -
0x382890        19      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   asc     asc     N/A     -       -
0x382918        20      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   asc3350p        asc3350p        N/A     -       -
0x3829a8        21      N/A     SERVICE_DISABLED        SERVICE_STOPPED SERVICE_KERNEL_DRIVER   asc3550 asc3550 N/A     -       -
0x382a38        22      N/A     SERVICE_DEMAND_START    SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS       aspnet_state    ASP.NET State Service   N/A -
```

Listing All Loaded Drivers

```
sudo vol -f zeus2x4.vmem   windows.dricverscan.DriverScan
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$ sudo vol -f zeus2x4.vmem windows.driverscan.DriverScan
Volatility 3 Framework 2.8.0
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. These should be placed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
Offset  Start   Size    Service Key     Driver Name     Name

0x1f0b478       0xb1e59000      0x2a180 kmixer  kmixer  \Driver\kmixer
0x1ff32c0       0xf8790000      0x9e80  NDProxy NDProxy \Driver\NDProxy
0x1ff3f38       0xf87b0000      0xe880  usbhub  usbhub  \Driver\usbhub
0x1ff4730       0xf8a8a000      0x1100  swenum  swenum  \Driver\swenum
0x1ff51f0       0xf817d000      0x29000 iScsiPrt        iScsiPrt        \Driver\iScsiPrt
0x1ff7838       0xf8780000      0x9f00  TermDD  TermDD  \Driver\TermDD
0x1ff9030       0xf81ce000      0x2fe80 rdpdr   rdpdr   \Driver\rdpdr
0x1ff9180       0xf8108000      0x5df00 Update  Update  \Driver\Update
0x1ffa498       0xf88b0000      0x4080  Raspti  Raspti  \Driver\Raspti
0x2041b10       0xf88d0000      0x4a80  Msfs    Msfs    \FileSystem\Msfs
0x204cda0       0xf88d8000      0x7880  Npfs    Npfs    \FileSystem\Npfs
0x204dda0       0xf88c8000      0x5200  VgaSave VgaSave \Driver\VgaSave
0x2056f38       0xf8a92000      0x1080  mnmdd   mnmdd   \Driver\mnmdd
0x2057408       0xb2ef3000      0x58480 Tcpip   Tcpip   \Driver\Tcpip
0x2061ca8       0xb2f4c000      0x12600 IPSec   IPSec   \Driver\IPSec
0x2062340       0xf89e0000      0x2280  RasAcd  RasAcd  \Driver\RasAcd
0x2062be0       0xf8a90000      0x1080  Beep    Beep    \Driver\Beep
0x2063858       0xb2db1000      0x6f280 MRxSmb  MRxSmb  \FileSystem\MRxSmb
0x2065b30       0xf85e0000      0x8700  Wanarp  Wanarp  \Driver\Wanarp
0x206a250       0xf8620000      0xf900  Cdfs    Cdfs    \FileSystem\Cdfs
0x209f4b8       0xf8770000      0xed80  sysaudio        sysaudio        \Driver\sysaudio
0x20afa38       0xb2e86000      0x22580 prl_fs  prl_fs  \FileSystem\prl_fs
0x20c68b0       0xb2064000      0x40a80 HTTP    HTTP    \Driver\HTTP
0x20f4950       0xf8a48000      0x3c80  mssmbios        mssmbios        \Driver\mssmbios
0x210dbb8       0xb24df000      0x23180 Fastfat Fastfat \FileSystem\Fastfat
0x212d200       0x0     0x0     \Driver\Win32k  Win32k  \Driver\Win32k
0x212d790       0xb2503000      0xa7400 Hardlock        Hardlock        \Driver\Hardlock
0x2166f10       0xb2bbb000      0x3900  Ndisuio Ndisuio \Driver\Ndisuio
0x216e9f8       0xf88a8000      0x4580  Ptilink Ptilink \Driver\Ptilink
0x2172da0       0xb2ecb000      0x27c00 NetBT   NetBT   \Driver\NetBT
0x217a030       0xf826d000      0x17800 ac97intc        ac97intc        \Driver\ac97intc
0x217b030       0xf8760000      0x8900  Gpc     Gpc     \Driver\Gpc
0x217d030       0xf8750000      0xbd00  PptpMiniport    PptpMiniport    \Driver\PptpMiniport
0x2180da0       0xf88b8000      0x5000  Flpydisk        Flpydisk        \Driver\Flpydisk
0x2181268       0xf8710000      0xf600  Cdrom   Cdrom   \Driver\Cdrom
0x21814e8       0xf820f000      0x16580 NdisWan NdisWan \Driver\NdisWan
0x2181728       0xf8740000      0xa200  RasPppoe        RasPppoe        \Driver\RasPppoe
0x2182bf8       0xf8a28000      0x3d80  Serenum Serenum \Driver\Serenum
0x2186928       0xb277b000      0xf000  NPF     NPF     \Driver\NPF
0x218a5a0       0xb2d8b000      0x25500 IpNat   IpNat   \Driver\IpNat
0x218cbe0       0xb25d3000      0x2c180 MRxDAV  MRxDAV  \FileSystem\MRxDAV
0x218f698       0xf8ab0000      0x1a80  ParVdm  ParVdm  \Driver\ParVdm
```

Get All Executed Processes

```
sudo vol -f zeus2x4.vmem   windows.psscan.PsScan
```

```
┌──(kali㉿kali)-[~/Zeus/collectedInfo]
└─$ sudo vol -f ../zeus2x4.vmem   windows.psscan.PsScan
Volatility 3 Framework 2.8.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correc
ed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

3276    3772    ihah.exe        0x1e87da0       1       45      0       False   2010-09-09 19:56:32.000000 UTC  N/A     Disabled
2588    744     alg.exe 0x1e8a368       6       107     0       False   2010-09-02 12:25:44.000000 UTC  N/A     Disabled
3984    1084    wuauclt.exe     0x1eab2f8       8       325     0       False   2010-09-09 19:52:45.000000 UTC  N/A     Disabled
3772    2404    b98679df6defbb3 0x1f4bb28       1       46      0       False   2010-09-09 19:56:19.000000 UTC  N/A     Disabled
3788    1752    ImmunityDebugge 0x1ffb6d8       2       103     0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
2972    1752    ImmunityDebugge 0x2001ad0       2       87      0       False   2010-09-08 19:14:36.000000 UTC  N/A     Disabled
940     1084    wuauclt.exe     0x205dda0       4       126     0       False   2010-09-02 12:26:40.000000 UTC  N/A     Disabled
2404    1752    ImmunityDebugge 0x2066478       2       85      0       False   2010-09-09 19:56:19.000000 UTC  N/A     Disabled
572     744     coherence.exe   0x2077da0       4       51      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
2204    2972    nifek_locked.ex 0x207bda0       2       38      0       False   2010-09-08 19:14:36.000000 UTC  N/A     Disabled
632     436     prl_tools.exe   0x2086798       9       107     0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
472     744     jqs.exe 0x2089558       5       146     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
488     744     sqlservr.exe    0x208abf0       25      306     0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
1616    744     spoolsv.exe     0x2095500       13      140     0       False   2010-09-02 12:25:24.000000 UTC  N/A     Disabled
1908    1752    prl_cc.exe      0x20ee580       14      133     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
364     744     svchost.exe     0x2129370       4       88      0       False   2010-09-02 12:25:33.000000 UTC  N/A     Disabled
1936    1752    jusched.exe     0x212ada0       1       43      0       False   2010-09-02 12:25:26.000000 UTC  N/A     Disabled
2180    1084    wscntfy.exe     0x213dda0       3       48      0       False   2010-09-02 12:25:41.000000 UTC  N/A     Disabled
1192    744     svchost.exe     0x214f488       13      175     0       False   2010-09-02 12:25:23.000000 UTC  N/A     Disabled
912     744     svchost.exe     0x2150b90       20      202     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1084    744     svchost.exe     0x2151da0       58      1327    0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
1140    744     svchost.exe     0x21521b0       6       81      0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
436     744     prl_tools_servi 0x2189530       3       78      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
3508    3788    anaxu.exe       0x219e5c8       2       54      0       False   2010-09-08 22:39:40.000000 UTC  N/A     Disabled
744     692     services.exe    0x21a5da0       15      279     0       False   2010-09-02 12:25:22.000000 UTC  N/A     Disabled
660     744     sqlwriter.exe   0x21aa7e8       4       84      0       False   2010-09-02 12:25:36.000000 UTC  N/A     Disabled
1752    1720    explorer.exe    0x21b2020       22      520     0       False   2010-09-02 12:25:25.000000 UTC  N/A     Disabled
```

```
sudo vol -f zeus2x4.vmem   windows.cmdline.Cmdline
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$  sudo vol -f zeus2x4.vmem    windows.cmdline.CmdLine
Volatility 3 Framework 2.8.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to c
ed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x10 is not valid (process exited?)
596     smss.exe        \SystemRoot\System32\smss.exe
668     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemTyp
rServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
692     winlogon.exe    winlogon.exe
744     services.exe    C:\WINDOWS\system32\services.exe
756     lsass.exe       C:\WINDOWS\system32\lsass.exe
912     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
992     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
1084    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1140    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1192    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1436    iscsiexe.exe    C:\WINDOWS\System32\iscsiexe.exe
1616    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1752    explorer.exe    C:\WINDOWS\Explorer.EXE
1900    SharedIntApp.ex "C:\Program Files\Parallels\Parallels Tools\SIA\SharedIntApp.exe" /start
1908    prl_cc.exe      "C:\Program Files\Parallels\Parallels Tools\prl_cc.exe"
1936    jusched.exe     "C:\Program Files\Java\jre6\bin\jusched.exe"
364     svchost.exe     Required memory at 0x20044 is inaccessible (swapped)
472     jqs.exe "C:\Program Files\Java\jre6\bin\jqs.exe" -service -config "C:\Program Files\Java\jre6\lib\deploy\jqs\jqs.conf"
488     sqlservr.exe    "c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe" -sSQLEXPRESS
572     coherence.exe   Required memory at 0x20044 is inaccessible (swapped)
436     prl_tools_servi Required memory at 0x20044 is inaccessible (swapped)
632     prl_tools.exe   "C:\Program Files\Parallels\Parallels Tools\Services\prl_tools.exe"
660     sqlwriter.exe   "c:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe"
2180    wscntfy.exe     C:\WINDOWS\system32\wscntfy.exe
2588    alg.exe Required memory at 0x20044 is inaccessible (swapped)
```

Get Detailed Process Tree

```
sudo vol -f zeus2x4.vmem   windows.pstree.Pstree
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$ sudo vol -f zeus2x4.vmem   windows.pstree.PsTree
Volatility 3 Framework 2.8.0
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. These should be placed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

4       0       System  0x823c8a00      57      671     N/A     False   N/A     N/A     -       -       -
* 596   4       smss.exe        0x82292da0      3       19      N/A     False   2010-09-02 12:25:18.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\smss.exe       \SystemRoot\System32\smss.exe       \SystemRoot\System32\smss.exe
** 692   596     winlogon.exe    0x822c09f8      21      588     0       False   2010-09-02 12:25:22.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\winlogon.exe   winlogon.exe        \??\C:\WINDOWS\system32\winlogon.exe
a** 744 692     services.exe    0x821a5da0      15      279     0       False   2010-09-02 12:25:22.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\services.exe   C:\WINDOWS\system32\services.exe     C:\WINDOWS\system32\services.exe
**** 992        744     svchost.exe     0x822c8bf8      10      277     0       False   2010-09-02 12:25:22.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\svchost.exeC:\WINDOWS\system32\svchost -k rpcss     C:\WINDOWS\system32\svchost.exe
**** 1192       744     svchost.exe     0x8214f488      13      175     0       False   2010-09-02 12:25:23.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\svchost.exeC:\WINDOWS\system32\svchost.exe -k LocalService C:\WINDOWS\system32\svchost.exe
**** 488        744     sqlservr.exe    0x8208abf0      25      306     0       False   2010-09-02 12:25:33.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe  "c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlserv
**** 364        744     svchost.exe     0x82129370      4       88      0       False   2010-09-02 12:25:33.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe-    -
**** 912        744     svchost.exe     0x82150b90      20      202     0       False   2010-09-02 12:25:22.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\svchost.exeC:\WINDOWS\system32\svchost -k DcomLaunch       C:\WINDOWS\system32\svchost.exe
**** 1616       744     spoolsv.exe     0x82095500      13      140     0       False   2010-09-02 12:25:24.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\spoolsv.exeC:\WINDOWS\system32\spoolsv.exe C:\WINDOWS\system32\spoolsv.exe
**** 1140       744     svchost.exe     0x821521b0      6       81      0       False   2010-09-02 12:25:22.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\svchost.exeC:\WINDOWS\system32\svchost.exe -k NetworkService       C:\WINDOWS\system32\svchost.exe
**** 436        744     prl_tools_servi 0x82189538      3       78      0       False   2010-09-02 12:25:36.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Parallels\Parallels Tools\Services\prl_tools_service.exe   -       -
***** 632       436     prl_tools.exe   0x82086798      9       107     0       False   2010-09-02 12:25:36.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Parallels\Parallels Tools\Services\prl_tools.exe     "C:\Program Files\Parallels\Parallels Tools\Services\prl_tools.ex
**** 660        744     sqlwriter.exe   0x821aa7e8      4       84      0       False   2010-09-02 12:25:36.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe  "c:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe" c:\Progra
**** 472        744     jqs.exe 0x82089558      5       146     0       False   2010-09-02 12:25:33.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Java\jre6\bin\jqs.exe"C:\Program Files\Java\jre6\bin\jqs.exe" -service -config "C:\Program Files\Java\jre6\lib\deploy\jqs\jqs.c
**** 1436       744     iscsiexe.exe    0x8221e278      6       78      0       False   2010-09-02 12:25:24.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\iscsiexe.exe       C:\WINDOWS\System32\iscsiexe.exe        C:\WINDOWS\System32\iscsiexe.exe
**** 1084       744     svchost.exe     0x82151da0      58      1327    0       False   2010-09-02 12:25:22.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\svchost.exeC:\WINDOWS\System32\svchost.exe -k netsvcs       C:\WINDOWS\System32\svchost.exe
***** 3984      1084    wuauclt.exe     0x81eab2f8      8       325     0       False   2010-09-09 19:52:45.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\wuauclt.exe"C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local[43c]$USDS82f0c54ad7b58b46a717b19ec999e73f C
***** 940       1084    wuauclt.exe     0x8205dda0      4       126     0       False   2010-09-02 12:26:40.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\wuauclt.exe"C:\WINDOWS\system32\wuauclt.exe"       C:\WINDOWS\system32\wuauclt.exe
***** 2180      1084    wscntfy.exe     0x8213dda0      3       48      0       False   2010-09-02 12:25:41.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\wscntfy.exeC:\WINDOWS\system32\wscntfy.exe C:\WINDOWS\system32\wscntfy.exe
***** 3768      1084    rundll32.exe    0x82311648      1       53      0       False   2010-09-09 19:56:33.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\rundll32.exe       C:\WINDOWS\System32\rundll32.exe C:\WINDOWS\System32\firewall.cpl,ShowNotificationDialog /configu
**** 2588       744     alg.exe 0x81e8a368      6       107     0       False   2010-09-02 12:25:44.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\alg.exe         -  -
**** 572        744     coherence.exe   0x82077da0      4       51      0       False   2010-09-02 12:25:36.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Parallels\Parallels Tools\Services\coherence.exe       -       -
a** 756 692     lsass.exe       0x822c8798      24      437     0       False   2010-09-02 12:25:22.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe      C:\WINDOWS\system32\lsass.exe       C:\WINDOWS\system32\lsass.exe
** 668   596     csrss.exe       0x821f2978      14      471     0       False   2010-09-02 12:25:21.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\system32\csrss.exe      C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=W
xRequestThreads=16      \??\C:\WINDOWS\system32\csrss.exe
1752    1720    explorer.exe    0x821b2020      22      520     0       False   2010-09-02 12:25:25.000000 UTC  N/A     \Device\HarddiskVolume1\WINDOWS\explorer.exe    C:\WINDOWS\Explorer.EXE     C:\WINDOWS\Explorer.EXE
* 2404  1752    ImmunityDebugge 0x82066478      2       85      0       False   2010-09-09 19:56:19.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe   "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C
munityDebugger.exe
** 3772 2404    b98679df6defbb3 0x81f4bb28      1       46      0       False   2010-09-09 19:56:19.000000 UTC  N/A     \Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\b98679df6defbb3dc0e12463880c9dd7.exe   "C:\Documents and Settings\Administrator\Desktop\b98679df
a** 3276        3772    ihah.exe        0x81e87da0      1       45      0       False   2010-09-09 19:56:32.000000 UTC  N/A     \Device\HarddiskVolume1\Documents and Settings\Administrator\Application Data\Obyt\ihah.exe "C:\Documents and Settings\Administrator\Application Data\Obyt\ih
* 1900  1752    SharedIntApp.ex 0x822b96c0      3       75      0       False   2010-09-02 12:25:25.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Parallels\Parallels Tools\SIA\SharedIntApp.exe       "C:\Program Files\Parallels\Parallels Tools\SIA\SharedIntApp.exe" /start
* 1932  1752    ImmunityDebugge 0x82282380      2       86      0       False   2010-09-08 19:23:02.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe   "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C
** 952   1932    vaelh.exe       0x8223c020      2       40      0       False   2010-09-08 19:23:02.000000 UTC  N/A     \Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\vaelh.exe      "C:\Documents and Settings\Administrator\Desktop\vaelh.exe"      C:\Documents and
* 3788  1752    ImmunityDebugge 0x81ff6d8       2       103     0       False   2010-09-08 22:39:40.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe   "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C
** 3508  3788    anaxu.exe       0x8219e5c8      2       54      0       False   2010-09-08 22:39:40.000000 UTC  N/A     \Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\anaxu.exe      "C:\Documents and Settings\Administrator\Desktop\anaxu.exe"      C:\Documents and
* 1936  1752    jusched.exe     0x8212ada0      1       43      0       False   2010-09-02 12:25:26.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Java\jre6\bin\jusched.exe     "C:\Program Files\Java\jre6\bin\jusched.exe"    C:\Program Files\Java\jre6\bin\jusched.exe
* 1908  1752    prl_cc.exe      0x820ee580      14      133     0       False   2010-09-02 12:25:25.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Parallels\Parallels Tools\prl_cc.exe  "C:\Program Files\Parallels\Parallels Tools\prl_cc.exe"      C:\Program Files\Parallel
* 2972  1752    ImmunityDebugge 0x82001ad0      2       87      0       False   2010-09-08 19:14:36.000000 UTC  N/A     \Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe   "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C
** 2204  2972    nifek_locked.ex 0x8207bda0      2       38      0       False   2010-09-08 19:14:36.000000 UTC  N/A     \Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\nifek_locked.exe      "C:\Documents and Settings\Administrator\Desktop\nifek_locked.exe"      C
```

Dumping Malicious process

```
sudo vol -f zeus2x4.vmem  -o ./procdump windows.memmap.Memmap --pid 3276 --dump
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$  vol -f zeus2x4.vmem -o /home/kali/Zeus/collectedInfo/pdump windows.memmap.Memmap --pid 3276 --dump
Volatility 3 Framework 2.8.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to c
ed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
Virtual Physical        Size    Offset in File  File output

0x10000 0x1d6b9000      0x1000  0x0     pid.3276.dmp
0x20000 0x1017a000      0x1000  0x1000  pid.3276.dmp
0x12d000        0xa38000        0x1000  0x2000  pid.3276.dmp
0x12e000        0x1c50b000      0x1000  0x3000  pid.3276.dmp
0x12f000        0xe2bc000       0x1000  0x4000  pid.3276.dmp
0x130000        0x10b95000      0x1000  0x5000  pid.3276.dmp
0x131000        0x10b16000      0x1000  0x6000  pid.3276.dmp
0x140000        0x19c0b000      0x1000  0x7000  pid.3276.dmp
0x150000        0x9e01000       0x1000  0x8000  pid.3276.dmp
0x151000        0x19782000      0x1000  0x9000  pid.3276.dmp
0x152000        0x6bc5000       0x1000  0xa000  pid.3276.dmp
0x153000        0x19dea000      0x1000  0xb000  pid.3276.dmp
0x154000        0x6a72000       0x1000  0xc000  pid.3276.dmp
0x155000        0x1396d000      0x1000  0xd000  pid.3276.dmp
0x156000        0x1c1fd000      0x1000  0xe000  pid.3276.dmp
0x157000        0x15048000      0x1000  0xf000  pid.3276.dmp
0x158000        0xad89000       0x1000  0x10000 pid.3276.dmp
0x159000        0x7e0a000       0x1000  0x11000 pid.3276.dmp
0x15a000        0x1bc4b000      0x1000  0x12000 pid.3276.dmp
0x15b000        0x54d0000       0x1000  0x13000 pid.3276.dmp
0x15c000        0x13352000      0x1000  0x14000 pid.3276.dmp
0x15d000        0x5f9b000       0x1000  0x15000 pid.3276.dmp
0x15e000        0x1151c000      0x1000  0x16000 pid.3276.dmp
0x15f000        0x12d9d000      0x1000  0x17000 pid.3276.dmp
0x160000        0x371f000       0x1000  0x18000 pid.3276.dmp
0x161000        0x1b7e0000      0x1000  0x19000 pid.3276.dmp
0x162000        0x19961000      0x1000  0x1a000 pid.3276.dmp
0x163000        0x14263000      0x1000  0x1b000 pid.3276.dmp
0x164000        0xeb64000       0x1000  0x1c000 pid.3276.dmp
```

Dump Files of Malicious Process

```
 sudo vol -f .. /zeus2x4.vmem -o /home/kali/Zeus/collectedInfo/procdump/ windows.dumpfiles --pid
3772
```

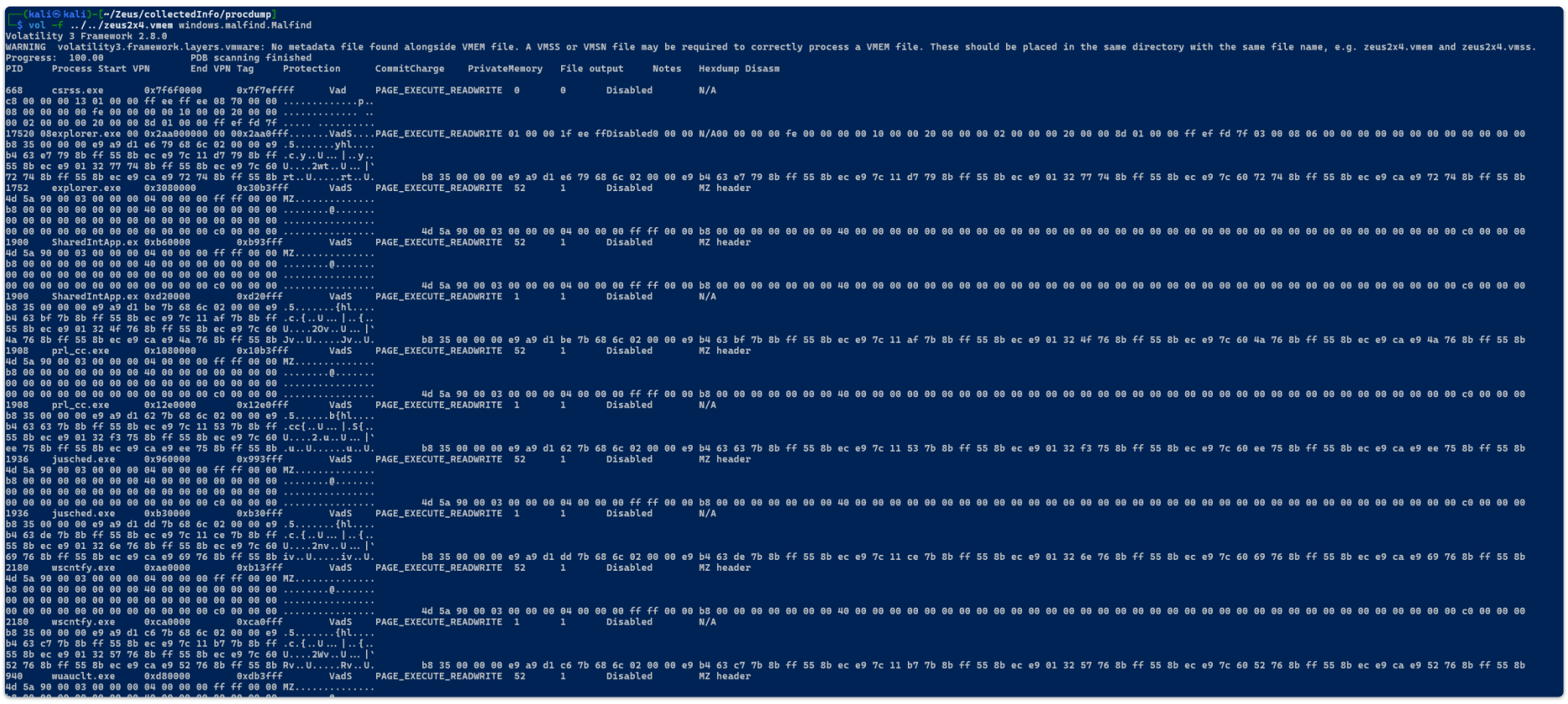
```
─$ vol -f ../zeus2x4.vmem -o /home/kali/Zeus/pdump  windows.dumpfiles --pid 3772
Volatility 3 Framework 2.8.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file.
These should be placed in the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0x82069028      b98679df6defbb3dc0e12463880c9dd7.exe    file.0x82069028.0x822e08c0.DataSectionObject.b98679df6defbb3dc0e12463880c9dd7.ex
e-3.dat
ImageSectionObject      0x82069028      b98679df6defbb3dc0e12463880c9dd7.exe    file.0x82069028.0x82005ca0.ImageSectionObject.b98679df6defbb3dc0e12463880c9dd7.e
xe-3.img
DataSectionObject       0x822277f8      kernel32.dll    file.0x822277f8.0x8237cb78.DataSectionObject.kernel32.dll-6.dat
ImageSectionObject      0x822277f8      kernel32.dll    file.0x822277f8.0x821c2008.ImageSectionObject.kernel32.dll-6.img
DataSectionObject       0x8233db78      msvcrt.dll      file.0x8233db78.0x8237d860.DataSectionObject.msvcrt.dll-6.dat
ImageSectionObject      0x8233db78      msvcrt.dll      file.0x8233db78.0x822a7330.ImageSectionObject.msvcrt.dll-6.img
DataSectionObject       0x82251980      ole32.dll       file.0x82251980.0x822d66b8.DataSectionObject.ole32.dll-6.dat
ImageSectionObject      0x82251980      ole32.dll       file.0x82251980.0x82092528.ImageSectionObject.ole32.dll-6.img
DataSectionObject       0x821c9420      ws2_32.dll      file.0x821c9420.0x822d8930.DataSectionObject.ws2_32.dll-6.dat
ImageSectionObject      0x821c9420      ws2_32.dll      file.0x821c9420.0x822b3ef0.ImageSectionObject.ws2_32.dll-6.img
DataSectionObject       0x821997c0      netapi32.dll    file.0x821997c0.0x82348930.DataSectionObject.netapi32.dll-6.dat
ImageSectionObject      0x821997c0      netapi32.dll    file.0x821997c0.0x821dd008.ImageSectionObject.netapi32.dll-6.img
```

Malicious Memory Activity Checking

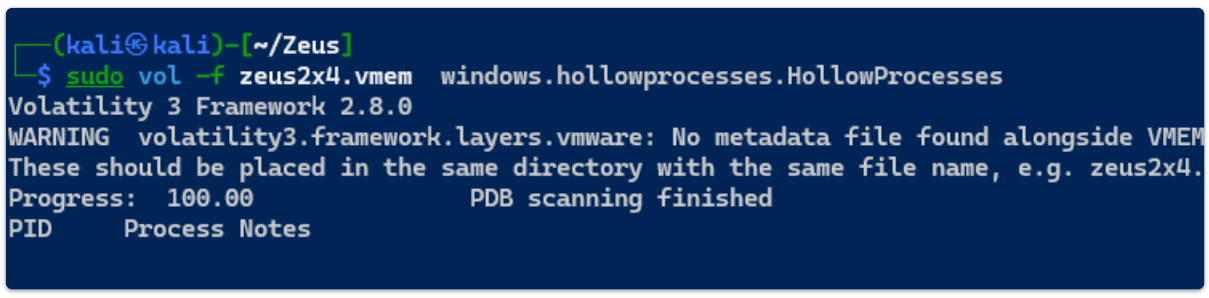
MalFind

```
sudo vol -f .. / .. /zeus2x4.vmem windows.malfind. Malfind
```



Process Hollow

```
sudo vol -f zeus.vmem windows.hollowprocess.HollowProcess
```



SupsiciousThreads

```
sudo vol -f zeus2x4.vmem   windows.suspicious_threads.SupsiciousThreads
```

```
┌──(kali㉿kali)-[~/Zeus]
└─$ sudo vol -f zeus2x4.vmem   windows.suspicious_threads.SupsiciousThreads
Volatility 3 Framework 2.8.0
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. These should be placed in the same directory with the
Progress:  100.00               PDB scanning finished
Process PID     TID     Context Address VAD Path        Note

smss.exe        596     600     Win32Start      0x0     <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x0), which is not backed by a file
smss.exe        596     600     Win32Start      0x0     <Non-File Backed Region>        VAD at base address (0x0) hosting this thread has an unexpected starting protection PAGE_READWRITE
smss.exe        596     608     Win32Start      0x1282  <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x0), which is not backed by a file
smss.exe        596     608     Win32Start      0x1282  <Non-File Backed Region>        VAD at base address (0x0) hosting this thread has an unexpected starting protection PAGE_READWRITE
csrss.exe       668     676     Win32Start      0x0     <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x0), which is not backed by a file
csrss.exe       668     676     Win32Start      0x0     <Non-File Backed Region>        VAD at base address (0x0) hosting this thread has an unexpected starting protection PAGE_READWRITE
csrss.exe       668     684     Win32Start      0xf56e4 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xe0000), which is not backed by a file
csrss.exe       668     684     Win32Start      0xf56e4 <Non-File Backed Region>        VAD at base address (0xe0000) hosting this thread has an unexpected starting protection PAGE_READWRITE
csrss.exe       668     704     Win32Start      0xf56e0 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xe0000), which is not backed by a file
csrss.exe       668     704     Win32Start      0xf56e0 <Non-File Backed Region>        VAD at base address (0xe0000) hosting this thread has an unexpected starting protection PAGE_READWRITE
csrss.exe       668     1916    Win32Start      0xf56e1 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xe0000), which is not backed by a file
csrss.exe       668     1916    Win32Start      0xf56e1 <Non-File Backed Region>        VAD at base address (0xe0000) hosting this thread has an unexpected starting protection PAGE_READWRITE
csrss.exe       668     1944    Win32Start      0xf56df <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xe0000), which is not backed by a file
csrss.exe       668     1944    Win32Start      0xf56df <Non-File Backed Region>        VAD at base address (0xe0000) hosting this thread has an unexpected starting protection PAGE_READWRITE
winlogon.exe    692     740     Win32Start      0xf258d <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x70000), which is not backed by a file
winlogon.exe    692     740     Win32Start      0xf258d <Non-File Backed Region>        VAD at base address (0x70000) hosting this thread has an unexpected starting protection PAGE_READWRITE
services.exe    744     3020    Win32Start      0xf56e2 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
services.exe    744     3020    Win32Start      0xf56e2 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
lsass.exe       756     784     Win32Start      0xf53ae <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
lsass.exe       756     784     Win32Start      0xf53ae <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
lsass.exe       756     828     Win32Start      0xf5688 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
lsass.exe       756     828     Win32Start      0xf5688 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
lsass.exe       756     1452    Win32Start      0xf56e3 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
lsass.exe       756     1452    Win32Start      0xf56e3 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
lsass.exe       756     3268    Win32Start      0xf53b9 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
lsass.exe       756     3268    Win32Start      0xf53b9 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     912     1860    Win32Start      0xf53ce <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     912     1860    Win32Start      0xf53ce <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     992     1024    Win32Start      0xf5684 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     992     1024    Win32Start      0xf5684 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     1084    1096    Win32Start      0xf566b <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     1084    1096    Win32Start      0xf566b <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     1084    1172    Win32Start      0xf260c <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     1084    1172    Win32Start      0xf260c <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     1084    1596    Win32Start      0xf504b <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     1084    1596    Win32Start      0xf504b <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     1084    1828    Win32Start      0xf2407 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     1084    1828    Win32Start      0xf2407 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     1084    3532    Win32Start      0xf568e <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     1084    3532    Win32Start      0xf568e <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     1084    3948    Win32Start      0xf5021 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     1084    3948    Win32Start      0xf5021 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
svchost.exe     1140    3176    Win32Start      0xf5459 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
svchost.exe     1140    3176    Win32Start      0xf5459 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
spoolsv.exe     1616    1864    Win32Start      0xf504a <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
spoolsv.exe     1616    1864    Win32Start      0xf504a <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
explorer.exe    1752    2948    Win32Start      0xf2629 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
explorer.exe    1752    2948    Win32Start      0xf2629 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
explorer.exe    1752    3832    Win32Start      0xf560a <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
explorer.exe    1752    3832    Win32Start      0xf560a <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
explorer.exe    1752    3188    Win32Start      0x309d35b       <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x3080000), which is not backed by a file
explorer.exe    1752    3188    Win32Start      0x309d35b       <Non-File Backed Region>        VAD at base address (0x3080000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
explorer.exe    1752    1948    Win32Start      0x309c626       <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x3080000), which is not backed by a file
explorer.exe    1752    1948    Win32Start      0x309c626       <Non-File Backed Region>        VAD at base address (0x3080000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
explorer.exe    1752    3232    Win32Start      0x309c2cd       <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x3080000), which is not backed by a file
explorer.exe    1752    3232    Win32Start      0x309c2cd       <Non-File Backed Region>        VAD at base address (0x3080000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
explorer.exe    1752    3028    Win32Start      0x3095734       <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x3080000), which is not backed by a file
explorer.exe    1752    3028    Win32Start      0x3095734       <Non-File Backed Region>        VAD at base address (0x3080000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
explorer.exe    1752    3284    Win32Start      0x30aa086       <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x3080000), which is not backed by a file
explorer.exe    1752    3284    Win32Start      0x30aa086       <Non-File Backed Region>        VAD at base address (0x3080000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
explorer.exe    1752    3604    Win32Start      0x30aa0fc       <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x3080000), which is not backed by a file
explorer.exe    1752    3604    Win32Start      0x30aa0fc       <Non-File Backed Region>        VAD at base address (0x3080000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
prl_cc.exe      1908    3784    Win32Start      0xf5693 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
prl_cc.exe      1908    3784    Win32Start      0xf5693 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
prl_cc.exe      1908    448     Win32Start      0xf2591 <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x90000), which is not backed by a file
prl_cc.exe      1908    448     Win32Start      0xf2591 <Non-File Backed Region>        VAD at base address (0x90000) hosting this thread has an unexpected starting protection PAGE_READWRITE
sqlwriter.exe   660     1884    Win32Start      0xf258f <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xd0000), which is not backed by a file
sqlwriter.exe   660     1884    Win32Start      0xf258f <Non-File Backed Region>        VAD at base address (0xd0000) hosting this thread has an unexpected starting protection PAGE_READWRITE
wscntfy.exe     2180    3056    Win32Start      0xb0a086        <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xae0000), which is not backed by a file
wscntfy.exe     2180    3056    Win32Start      0xb0a086        <Non-File Backed Region>        VAD at base address (0xae0000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
wscntfy.exe     2180    3136    Win32Start      0xb0a0fc        <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xae0000), which is not backed by a file
wscntfy.exe     2180    3136    Win32Start      0xb0a0fc        <Non-File Backed Region>        VAD at base address (0xae0000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
wuauclt.exe     940     1480    Win32Start      0xf569e <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xa0000), which is not backed by a file
wuauclt.exe     940     1480    Win32Start      0xf569e <Non-File Backed Region>        VAD at base address (0xa0000) hosting this thread has an unexpected starting protection PAGE_READWRITE
wuauclt.exe     940     2268    Win32Start      0xf258b <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xa0000), which is not backed by a file
wuauclt.exe     940     2268    Win32Start      0xf258b <Non-File Backed Region>        VAD at base address (0xa0000) hosting this thread has an unexpected starting protection PAGE_READWRITE
nifek_locked.ex 2204    2480    Win32Start      0x92ab55        <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0x910000), which is not backed by a file
nifek_locked.ex 2204    2480    Win32Start      0x92ab55        <Non-File Backed Region>        VAD at base address (0x910000) hosting this thread has an unexpected starting protection PAGE_EXECUTE_READWRITE
vaelh.exe       952     3588    Win32Start      0xa5ab55        <Non-File Backed Region>        This thread started execution in the VAD starting at base address (0xa40000), which is not backed by a file
```

Threat Intelligence

Adding IOCs to your SOC DB

Generating New Rules

Using `YarGen` for Generating Rules and IOCs Based on Collected Evidences from Digital Forensics Process

```
python yargen.py -m /home/CollectedInfo/Zeus -o ../Zeus/Updated-IOC.rules
```

```
┌──(kali㉿kali)-[~/yarGen]
└─$ python yarGen.py -m /home/kali/Zeus -o ../Zeus/YarGen.rules
/home/kali/yarGen/yarGen.py:1152: SyntaxWarning: invalid escape sequence '\w'
  cleanedName = re.sub('[^\w]', r'_', cleanedName)
/home/kali/yarGen/yarGen.py:1354: SyntaxWarning: invalid escape sequence '\w'
  rule_name = re.sub('[^\w]', r'_', rule_name)
/home/kali/yarGen/yarGen.py:1494: SyntaxWarning: invalid escape sequence '\w'
  cleanedName = re.sub('[^\w]', r'_', cleanedName)
------------------------------------------------------------------------

                    _____
  __ _____ _____/ ___/__ ___
 / // / _ `/ __/ (_ / -_) _ \
 \_, /\_,_/_/  \___/\__/_//_/
/___/  Yara Rule Generator
       Florian Roth, August 2023, Version 0.24.0

  Note: Rules have to be post-processed
  See this post for details: https://medium.com/@cyb3rops/121d29322282
------------------------------------------------------------------------
[+] Using identifier 'Zeus'
[+] Using reference 'https://github.com/Neo23x0/yarGen'
[+] Using prefix 'Zeus'
[+] Processing PEStudio strings ...
[+] Reading goodware strings from database 'good-strings.db' ...
    (This could take some time and uses several Gigabytes of RAM depending on your db size)
[+] Loading ./dbs/good-imphashes-part2.db ...
[+] Total: 1056 / Added 1056 entries
[+] Loading ./dbs/good-exports-part5.db ...
[+] Total: 167302 / Added 167302 entries
[+] Loading ./dbs/good-imphashes-part6.db ...
[+] Total: 1087 / Added 31 entries
[+] Loading ./dbs/good-imphashes-part3.db ...
[+] Total: 4908 / Added 3821 entries
[+] Loading ./dbs/good-imphashes-part5.db ...
[+] Total: 12242 / Added 7334 entries
[+] Loading ./dbs/good-imphashes-part8.db ...
[+] Total: 12425 / Added 183 entries
[+] Loading ./dbs/good-exports-part3.db ...
[+] Total: 240254 / Added 72952 entries
[+] Loading ./dbs/good-strings-part4.db ...
[+] Total: 2292468 / Added 2292468 entries
[+] Loading ./dbs/good-exports-part4.db ...
[+] Total: 266964 / Added 26710 entries
```

YARA Rules Testing

Testing IOC Detection Result on Malicious File

```
┌──(kali㉿kali)-[~/Zeus]
└─$ yara -s YarGen.rules invoice_2318362983713_823931342io.pdf.exe
invoice_2318362983713_823931342io_pdf invoice_2318362983713_823931342io.pdf.exe
0x15f36:$s1: ejDmZKid5htD0UB[gZTHJVrLlTaTBBsBS18pEuDJBuMks{0H0zRNleRt2kh8S:QPqP/2v2JFYWjpubc,vQKhJvYCDZsyJKTWY,B6xyzRzzHY6Ezu44u6U6LOL[dhqVMn
0x311f6:$s2: corect.com
0x31a49:$s3: USER32.GetShellWindow
0x31d13:$s4: KERNEL32.GetThreadPriority
0x319e2:$s5: KERNEL32.SystemTimeToFileTime
0x31ada:$s6: KERNEL32.CreateIoCompletionPort
0x319a7:$s7: USER32.GetKeyNameTextA
0x31b13:$s8: KERNEL32.GetShortPathNameA
0x271a8:$s9: kqKDSPX2HCYOP/CYRnffTI[QZT{BN8Tafn,Jg2Ko[0X+i1oOknPp4ubEZniy2Q:OfQpxex4frsHQLes46ehHemEMxU9LPw{6VUKMC06pOw6cLW395ZdQdqxqDI6UQu7W
0x31939:$s10: KERNEL32.GetWindowsDirectoryA
0x31be1:$s11: KERNEL32.GetStartupInfoW
0x3180c:$s12: Dumpcotsavo
0x1ae26:$s13: 9tc34LSgjT7ksJmvD1NxsNewhlynXj97U7O2OIsjnaNv0Vglp5FzexmnW7uVORnovysoxu0sKAIn0NYuxRcwu81fYFOEugVLBVJ+3jUAl/w2{hHZhK9leprOkc:ehsEO
0x2dae8:$s14: IKe397ub8CXtoFKc4rpl7t{DViecb2T7YM1yKaiMRmyCfs8Q:m[+PtURL3Myem6ZTR6kTSYjeph4xg1wlgrno+H0p81Wmn78yBOY76uEWgJRfJUWBsYj9UhYSyka,41W
0x309b7:$s15: gi4HzEwf0b9TQHjtEoOXk3TgcahTZe3sCGwEOg5iVBZz3WW7wkiNIMrnH0ZuSagxOTBaU93fuzD4BD7yiAU9MT6yUdT+fdoMjVpOOlOGZZVdXPV7cfpzMrUnxewB5eYr
0x3c461:$s16:         <requestedExecutionLevel level='asInvoker' uiAccess="false"/>
0x31fa1:$s17: USER32.GetUpdateRgn
0x31dbb:$s18: USER32.GetMonitorInfoW
0x23d08:$s19: fvifsB4KEyDcEPd9ma,mZmhSNAXYsZEbZZclOdUQCS6p8uEip/hwoawNRzsRy6G5JFIyRhp/pLoGOKTt68dv6HMz:ofAI7VI7o8lZxQpqKq51M3U,Nsk0Fy1rZVIdPKI
0x222bc:$s20: jqiXzmPzIU8V590Xs8,5xbUM7YgXcpsjiizfRlhaQhH/pYXxG8LJqjhVskFt34KOlaJG9KCGjT,brQrWn/xuwTW3xm,CyP60F936QWqfEhEgN1gM830gOtrTb6hbP7ir
```

Testing IOC Detection Result on Memory Dump

```
┌──(kali㉿kali)-[~/Zeus]
└─$  sudo vol -f zeus2x4.vmem    yarascan.YaraScan --yara-file Updated-IOCs.rules
Volatility 3 Framework 2.8.0
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
the same directory with the same file name, e.g. zeus2x4.vmem and zeus2x4.vmss.
Progress:  100.00               PDB scanning finished
Offset  Rule    Component       Value

0x8213df14      _dlls_process_main_malware_threads_process_privs_handels_Process_Tree_23        $s1     77 73 63 6e 74 66 79 2e 65 78 65
0x8223c194      _dlls_process_main_malware_threads_process_privs_handels_Process_Tree_23        $s2     76 61 65 6c 68 2e 65 78 65
0x8219e73c      _dlls_process_main_malware_threads_process_privs_handels_Process_Tree_23        $s3     61 6e 61 78 75 2e 65 78 65
0x8205df14      _dlls_process_main_malware_threads_process_privs_handels_Process_Tree_23        $s4     77 75 61 75 63 6c 74 2e 65 78 65
0x820ee6f4      _dlls_process_main_malware_threads_process_privs_handels_Process_Tree_23        $s5     70 72 6c 5f 63 63 2e 65 78 65
0x8207bf14      _dlls_process_main_malware_threads_process_privs_handels_Process_Tree_23        $s6     6e 69 66 65 6b 5f 6c 6f 63 6b 65 64 2e 65 78
0x821aa95c      _dlls_process_main_malware_threads_process_privs_handels_Process_Tree_23        $s7     73 71 6c 77 72 69 74 65 72 2e 65 78 65
```

Documenting Tested IOCs

	A	B	C
1	**File**	**Offset**	**String ID**
2	invoice_2318362983713_823931342io.pdf.exe	0x15f36:$s1:	ejDmZKid5htD0UB[gZTHJVrLlTaTBBsBS18pEuDJBuMks{0H0zRNleRt2kh8S:QPqP/2v2JFYWjpubc,vQKhJvYCDZsvJKTWY,B6xyzRzzHY6Ezu44u6U6LOL[dhqVMn
3	invoice_2318362983713_823931342io.pdf.exe	0x311f6:$s2:	corect.com
4	invoice_2318362983713_823931342io.pdf.exe	0x31a49:$s3:	USER32.GetShellWindow
5	invoice_2318362983713_823931342io.pdf.exe	0x31d13:$s4:	KERNEL32.GetThreadPriority
6	invoice_2318362983713_823931342io.pdf.exe	0x319e2:$s5:	KERNEL32.SystemTimeToFileTime
7	invoice_2318362983713_823931342io.pdf.exe	0x31ada:$s6:	KERNEL32.CreateIoCompletionPort
8	invoice_2318362983713_823931342io.pdf.exe	0x319a7:$s7:	USER32.GetKeyNameTextA
9	invoice_2318362983713_823931342io.pdf.exe	0x31b13:$s8:	KERNEL32.GetShortPathNameA
10	invoice_2318362983713_823931342io.pdf.exe	0x271a8:$s9:	kqKDSPX2HCYOP/CYRnffTI[QZT{BN8Tafn,Jg2Ko[0X+i1oOknPp4ubEZniy2Q:OfQpxex4frsHQLes46ehHemEMxU9LPw{6VUKMC06pOw6cLW395ZdQdqxqDI6UQu7W
11	invoice_2318362983713_823931342io.pdf.exe	0x31939:$s10:	KERNEL32.GetWindowsDirectoryA
12	invoice_2318362983713_823931342io.pdf.exe	0x31be1:$s11:	KERNEL32.GetStartupInfoW
13	invoice_2318362983713_823931342io.pdf.exe	0x3180c:$s12:	Dumpcotsavo
14	invoice_2318362983713_823931342io.pdf.exe	0x1ae26:$s13:	9tc34LSgjT7ksJmvD1NxsNewhlynXj97U7O2OIsjnaNv0Vglp5FzexmnW7uVORnovysoxu0sKAIn0NYuxRcwu81fYFOEugVLBVJ+3jUAl/w2{hHZhK9leprOkc:ehsEQ
15	invoice_2318362983713_823931342io.pdf.exe	0x2dae8:$s14:	IKe397ub8CXtoFKc4rpl7t{DViecb2T7YM1yKaiMRmyCfs8Q:m[+PtURL3Myem6ZTR6kTSYjeph4xg1wlgrno+H0p81Wmn78yBOY76uEWgJRfJUWBsYj9UhYSyka,41W
16	invoice_2318362983713_823931342io.pdf.exe	0x309b7:$s15:	gi4HzEwf0b9TQHjtEoOXk3TgcahTZe3sCGwEOg5iVBZz3WW7wkiNIMrnH0ZuSagxOTBaU93fuzD4BD7yiAU9MT6yUdT+fdoMjVpOOlOGZZVdXPV7cfpzMrUnxewB5eYr
17	invoice_2318362983713_823931342io.pdf.exe	0x3c461:$s16:	
18	invoice_2318362983713_823931342io.pdf.exe	0x31fa1:$s17:	USER32.GetUpdateRgn
19	invoice_2318362983713_823931342io.pdf.exe	0x31dbb:$s18:	USER32.GetMonitorInfoW
20	invoice_2318362983713_823931342io.pdf.exe	0x23d08:$s19:	fvifsB4KEyDcEPd9ma,mZmhSNAXYsZEbZZclOdUQCS6p8uEip/hwoawNRzsRy6G5JFIyRhp/pLoGOKTt68dv6HMz:ofAI7VI7o8lZxQpqKq51M3U,Nsk0Fy1rZVIdPKI
21	invoice_2318362983713_823931342io.pdf.exe	0x222bc:$s20:	jqiXzmPzIU8V590Xs8,5xbUM7YgXcpsjiizfRlhaQhH/pYXxG8LJqjhVskFt34KOlaJG9KCGjT,brQrWn/xuwTW3xm,CyP60F936QWqfEhEgN1gM830gOtrTb6hbP7ir
22			
23			