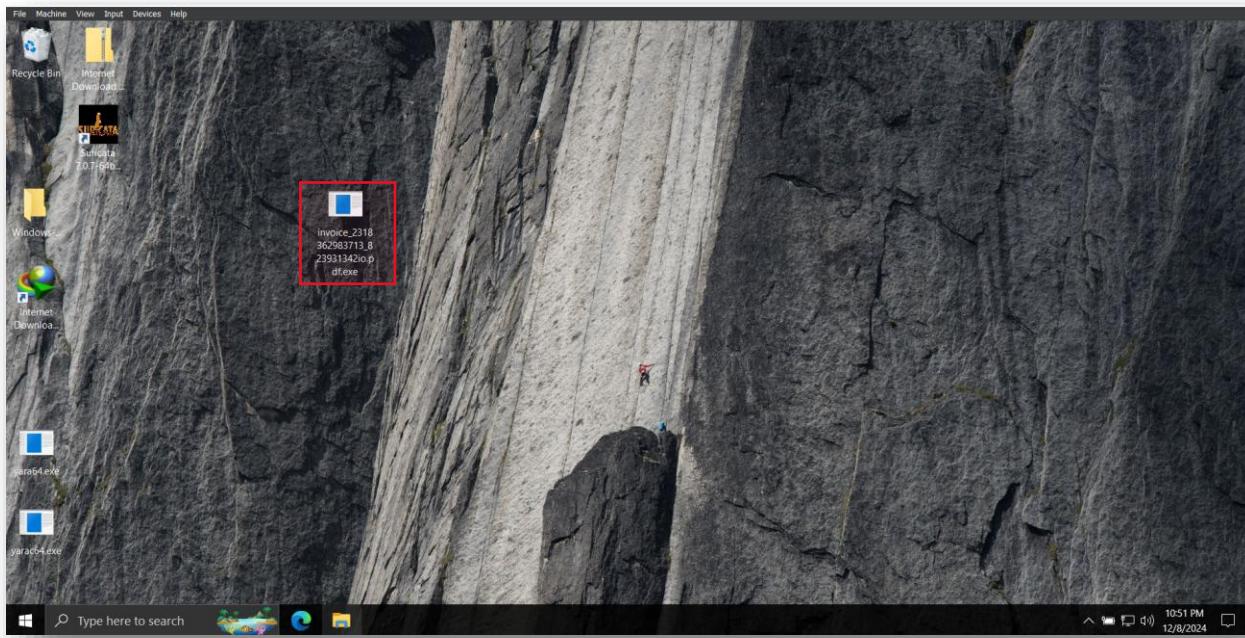


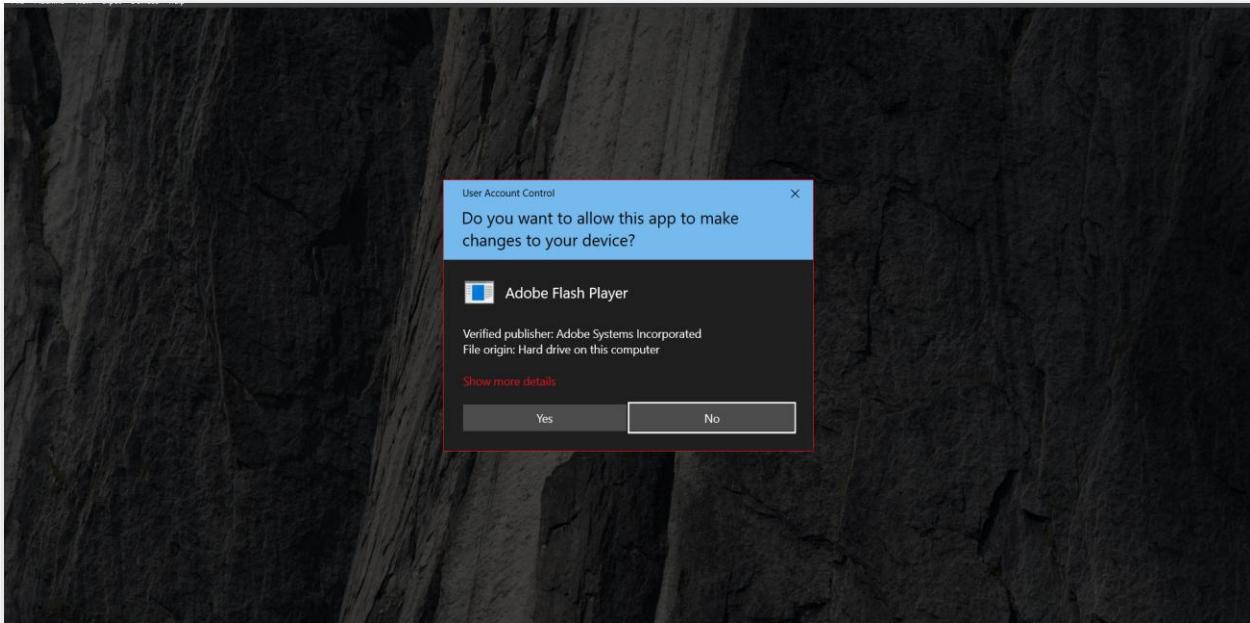
Proactive Project

Simulate Malware Execution:

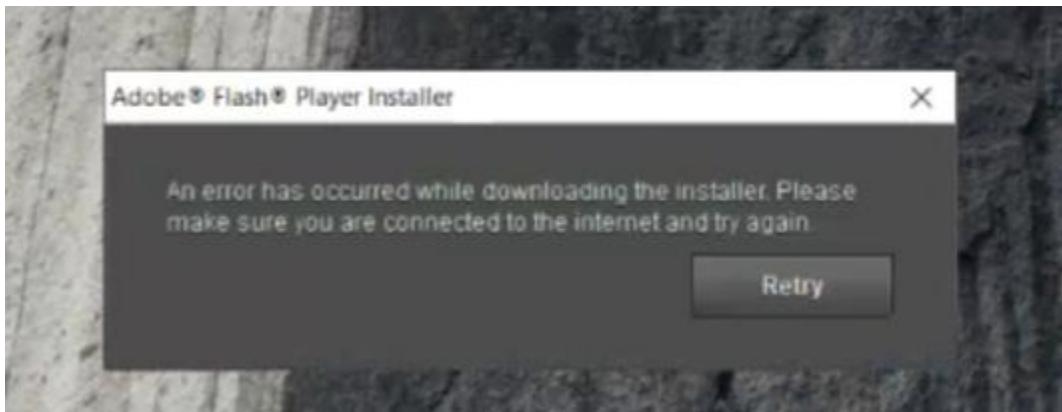
We are using a Windows 10 Enterprise Virtual Machine on Virtual Box



Here we have the **ZEUS malware** before we run the malware, we will open **Wireshark** and start capturing the packets to further analysis.



After Running it a UAC pops and requires changes approval from Adobe Flash Player. It doesn't matter if we click yes or no it will do the same because if we clicked no, the UAC window will reappear.



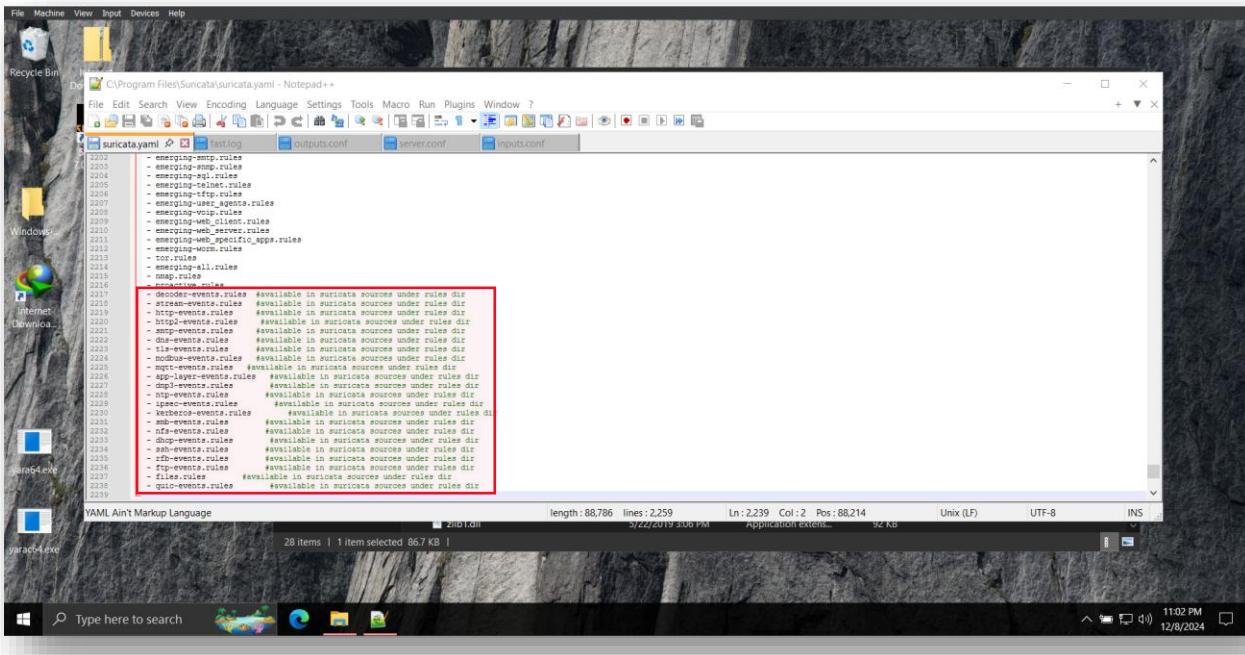
If we click on retry it will just reload and fail again.

Finally, the malware disappears from the desktop and the flash player tries to connect to something but fails.

Basic Conclusion:

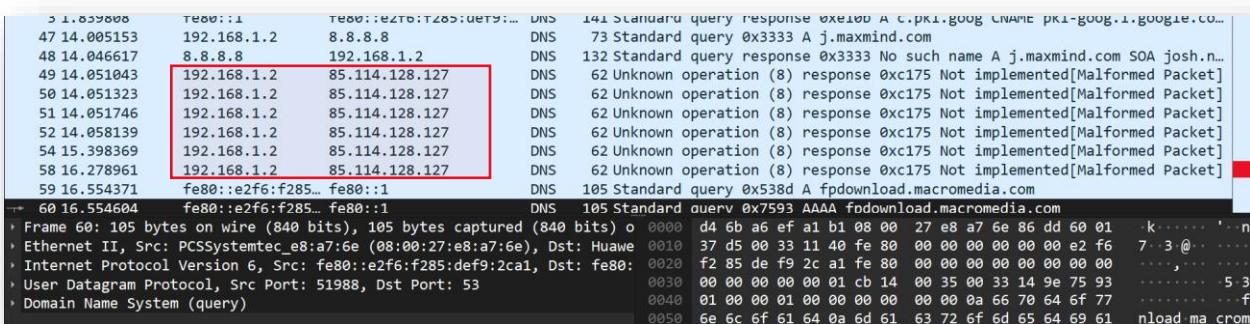
- Has Anti-VM capabilities
- Dropped an executable
- Deleted / Moved the main executable

Configure Suricata for Network Monitoring:



After Installing Suricata we went to its directory specifically `suricata.yaml` file to uncomment the default rules and we downloaded a collection of rules in one file called [emerging-all.rules](#) to work with in our project.

We opened the captured packets to check its behavior using **Wireshark**



When analyzing the packets using Wireshark, I noticed that the malware sends a malformed DNS request to **85.114.128.127**.

Communicating Files (30.1 K)			
Scanned	Detections	Type	Name
2022-08-11	54 / 70	Win32 EXE	isheriff_79afa840519f73e421b69fcbedd7b515.bin
2014-04-29	39 / 51	Win32 EXE	file1.exe
2013-10-30	37 / 47	Win32 EXE	Stub32.exe
2014-04-29	38 / 51	Win32 EXE	Branding.exe
2014-04-29	42 / 51	Win32 EXE	ildxyv
2016-06-05	43 / 57	Win32 EXE	isheriff_aef75438c59a650710f447ca2c7b58c.bin
2017-02-08	44 / 56	Win32 EXE	ab.exe
2013-08-15	3 / 45	Win32 EXE	5bf16fb4b9b58ba40170c942566e815b_kaf0x0
2017-02-08	45 / 57	Win32 EXE	ca659ad86df1714b46ed9b792e82b75f_kaf0x0
2013-09-20	6 / 48	Win32 EXE	9fbb1a87d67cb4c98b9fa88a440e45ce_kaf0x0
2014-04-29	37 / 51	Win32 EXE	vt-upload-9p2M1
2014-04-29	33 / 51	Win32 EXE	ab.exe
2014-04-29	38 / 51	Win32 EXE	ab.exe
2015-05-31	39 / 56	Win32 EXE	a29b3c67922b9fe5511e5792b73d8f2.virus
2024-10-30	57 / 72	Win32 EXE	ab.exe
2014-04-29	38 / 51	Win32 EXE	Registry Workshop
2014-06-07	35 / 51	Win32 EXE	vt-upload-tHxot
2019-02-13	50 / 70	Win32 EXE	GOOGLEUPDATE.EXE
2013-09-03	18 / 46	Win32 EXE	ZlhXdmzo
2014-04-29	42 / 50	Win32 EXE	Stub32.exe
2016-06-05	47 / 57	Win32 EXE	isheriff_33e40fdf31b4708a894a5ccbf7cf8b7.bin
2014-11-06	37 / 54	Win32 EXE	f15d24effec2261eadd10adf32f76c84
2013-11-18	32 / 46	Win32 EXE	Stub32.exe
2014-11-04	38 / 54	Win32 EXE	ab.exe

When searching for it on Virus Total It was flagged as safe, but by noticing the files that communicates with this Ip I knew It was malicious.

```
1 |alert ip any any -> 85.114.128.127 any (msg:"ZEUS Trojan C2 Connect: 85.114.128.127"; sid:1000123; rev:1;)
```

By knowing this I made a Suricata rule to alert when connecting to that IP and adding it to the suricata.yaml file.

```
.\suricata.exe -c suricata.yaml -i 192.168.1.2 -l log --service-install
```

So, by using these commands I used the suricata.yaml file as the config file and I listened on my ip address and made the logs dumps into the log folder and finally

--service-install: to add it as a service to run on startup.

Integrate with Splunk:

```
1 [tcpout]
2   defaultGroup = default-autolb-group
3
4 [tcpout:default-autolb-group]
5   server = 192.168.1.9:9997
6
7 [tcpout-server://192.168.1.9:9997]
```

Now we need to forward these alerts to Splunk for centralized analysis.

We started by configuring the main server to send the alerts on using this path:

```
C:\Program Files\SplunkUniversalForwarder\etc\system\local\outputs.conf
```

```
[monitor://C:\Program Files\Suricata\log\fast.log]
disabled = false
index = suricata
```

Suricata appends detailed event logs to fast.log in real-time, enabling Splunk to ingest and analyze security events promptly.

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

We go to settings then forwarding and receiving

Add new

Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

9997

For example, 9997 will receive data on TCP port 9997.

Cancel

Save

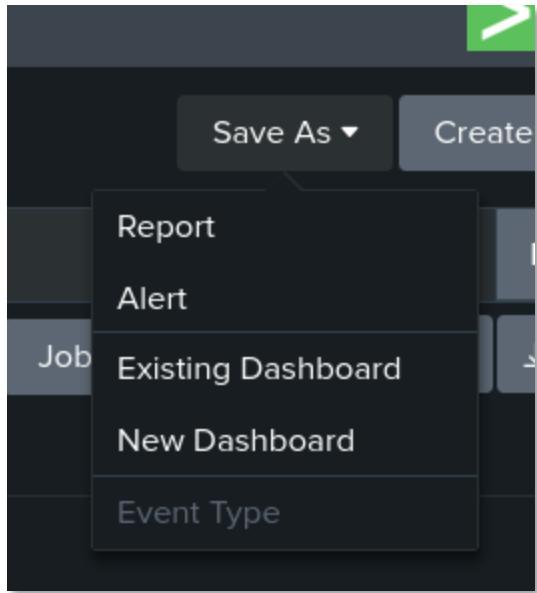
Then we add a new receiving to listen on port 9997

The screenshot shows the Splunk Enterprise interface. On the left, the 'Indexes' page lists 16 indexes, including '_audit', '_configtrack', '_dsappear', '_dsclient', and '_suricata'. A modal window titled 'New Index' is open, showing 'General Settings' for a new index named 'suricata'. The 'Index Data Type' is set to 'Events'. The 'Home Path' and 'Cold Path' fields are both set to 'optional'. At the bottom of the modal are 'Save' and 'Cancel' buttons. The main dashboard area shows a summary of storage usage: 1 MB free, 458.28 GB used, and 0 GB available.

Then we go to settings/index and create a new index to isolate Suricata events.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query 'index=suricata | search "ZEUS"'. Below the search bar, it says '9 events (12/15/24 10:00:00.000 PM to 12/16/24 10:39:13.000 PM)'. The search results are displayed under the 'Events (9)' tab. The interface includes various controls like 'Timeline format', 'Zoom Out', 'Format', 'Show: 20 Per Page', and 'View: List'.

Then we go to search for ZEUS from Suricata index



Then we will save it as an alert.

Save As Alert

Title: Zeus Trojan Connection

Description: Optional

Permissions: Private

Alert type: Scheduled

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results ▾
is greater than ▾ 0
in 1 minute(s) ▾

Trigger: Once For each result

Throttle ?

Trigger Actions

+ Add Actions ▾

When triggered: Add to Triggered Alerts Remove

Severity: High

Cancel Save

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

1 Alerts

All Yours This App's filter Q

i Title ▾	Actions	Owner ▾	App ▾	Sharing ▾	Status ▾
> Zeus Trojan Connection	Open in Search Edit ▾	m4l4vi	search	Private	Enabled

Here we can show the alerts we wrote for now.

Triggered Alerts

Filter						Showing 1 - 2 of 2 results	20 per ...	1 of 1 pages	<
App	Search & Report... ▾	Owner	All owners ▾	Severity	All severity ▾	Alert name	All alerts ▾		
<input type="checkbox"/>	Time ▾		Alert name ▾	App ▾	Type ▾	Severity ▾	Mode ▾	Actions	
<input type="checkbox"/>	2024-12-16 22:44:29 EET	Zeus Trojan Connection		search	Real-time	● High	Digest	View Results Edit Search Delete	
<input type="checkbox"/>	2024-12-16 22:44:28 EET	Zeus Trojan Connection		search	Real-time	● High	Digest	View Results Edit Search Delete	

Next, we executed the malware again to identify any triggered alerts.

Advanced Security Settings for An0n

Name: C:\Users\An0n
Owner: SYSTEM [Change](#)

Permissions Auditing Effective Access

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click [Edit](#) (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
All	Everyone	Full control	C:\Users\	This folder, subfolders and files

[Add](#) [Remove](#) [View](#)

[Disable inheritance](#)

Replace all child object auditing entries with inheritable auditing entries from this object

[OK](#) [Cancel](#) [Apply](#)

We audit the **Users** folder to the windows event logs of any file creations or deletions

```
host="DESKTOP-R74UPAT" EventCode=4663
```

Event ID 4663: Indicates an attempt to access an object, such as file creation, modification, or deletion.

After some investigation we found that the malware adding files in temp we can confirm it using the event code above.

```
12/16/24      12/16/2024 09:32:36 PM
9:32:36.000 PM LogName=Security
                  EventCode=4663
                  EventType=0
                  ComputerName=DESKTOP-R74UPAT
                  SourceName=Microsoft Windows security auditing.
                  Type=Information
                  RecordNumber=466651
                  Keywords=Audit Success
                  TaskCategory=File System
                  OpCode=Info
                  Message=An attempt was made to access an object.

                  Subject:
                      Security ID:          S-1-5-21-2826541408-2641107319-1920346365-1001
                      Account Name:         An0n
                      Account Domain:       DESKTOP-R74UPAT
                      Logon ID:             0x13F6B

                  Object:
                      Object Server:        Security
                      Object Type:          File
                      Object Name:          C:\Users\An0n\AppData\Local\Temp\InstallFlashPlayer.exe
                      Handle ID:            0x5cc
                      Resource Attributes:   S:AI

                  Process Information:
                      Process ID:           0x2944
                      Process Name:          C:\Users\An0n\Desktop\invoice_2318362983713_823931342io.exe
```

A thorough examination of the temporary directory revealed that the malicious invoice.exe executable had dropped falshplayer.exe, with the intent of launching it.

Malicious Activity ZEUS Trojan

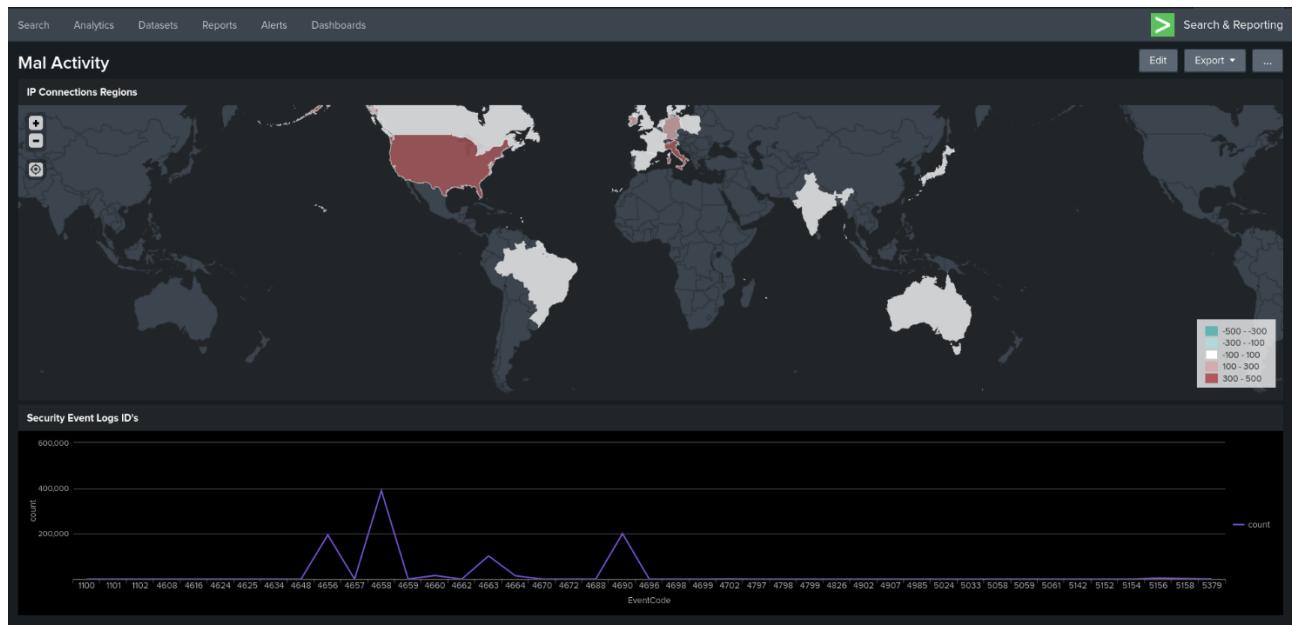
Process_Name="*\invoice_2318362983713_823931342io.pdf.exe"

Now we searched for this file in any path to find out if this file manipulates any process

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

Actions	Owner	App	Sharing	Status
Open in Search Edit	m4l4vi	search	Private	Enabled
Open in Search Edit	m4l4vi	search	Private	Enabled



Finally, we make this query to create a dashboard

Title IP Connections Regions

Search String

```
index=main | table Destination_Address | iplocation Destination_Address | stats count by Country | geom geo_countries featureIdField="Country"
```

Run Search ↗

Title Security Event Logs ID's

Search String

```
index=main source="WinEventLog:Security" | stats count by EventCode
```

Run Search ↗

Queries to create this dashboard.

Volatility & Yara Rules

Working on the memory dump that you provided to us on classroom [🔗](#)

I'll be working on Volatility Workbench (GUI Volatility) and Volatility 2

First, we need to list all processes we've got using (pslist and pstree) volatility plugins

pslist

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0x823c8a00	57	671	N/A	False	N/A	N/A	Disabled
596	4	smss.exe	0x82292da0	3	19	N/A	False	2010-09-02 12:25:18.000000 UTC	N/A	Disabled
668	596	csrss.exe	0x821f2978	14	471	0	False	2010-09-02 12:25:21.000000 UTC	N/A	Disabled
692	596	winlogon.exe	0x822c09f8	21	588	0	False	2010-09-02 12:25:22.000000 UTC	N/A	Disabled
744	692	services.exe	0x821a5da0	15	279	0	False	2010-09-02 12:25:22.000000 UTC	N/A	Disabled
756	692	lsass.exe	0x822c8798	24	437	0	False	2010-09-02 12:25:22.000000 UTC	N/A	Disabled
912	744	svchost.exe	0x82150b90	20	202	0	False	2010-09-02 12:25:22.000000 UTC	N/A	Disabled
992	744	svchost.exe	0x822c8bf8	10	277	0	False	2010-09-02 12:25:22.000000 UTC	N/A	Disabled
1084	744	svchost.exe	0x82151da0	58	1327	0	False	2010-09-02 12:25:22.000000 UTC	N/A	Disabled
1140	744	svchost.exe	0x821521b0	6	81	0	False	2010-09-02 12:25:22.000000 UTC	N/A	Disabled
1192	744	svchost.exe	0x8214f488	13	175	0	False	2010-09-02 12:25:23.000000 UTC	N/A	Disabled
1436	744	iscsие.exe	0x8221e278	6	78	0	False	2010-09-02 12:25:24.000000 UTC	N/A	Disabled
1616	744	spoolsv.exe	0x82095500	13	140	0	False	2010-09-02 12:25:24.000000 UTC	N/A	Disabled
1752	1720	explorer.exe	0x821b2020	22	520	0	False	2010-09-02 12:25:25.000000 UTC	N/A	Disabled
1900	1752	SharedIntApp.ex	0x822b96c0	3	75	0	False	2010-09-02 12:25:25.000000 UTC	N/A	Disabled
1908	1752	prl_cc.exe	0x820ee580	14	133	0	False	2010-09-02 12:25:25.000000 UTC	N/A	Disabled
1936	1752	jusched.exe	0x8212ada0	1	43	0	False	2010-09-02 12:25:26.000000 UTC	N/A	Disabled
364	744	svchost.exe	0x82129370	4	88	0	False	2010-09-02 12:25:33.000000 UTC	N/A	Disabled
472	744	jqs.exe	0x82089558	5	146	0	False	2010-09-02 12:25:33.000000 UTC	N/A	Disabled
488	744	sqlservr.exe	0x8208abf0	25	306	0	False	2010-09-02 12:25:33.000000 UTC	N/A	Disabled
572	744	coherence.exe	0x82077da0	4	51	0	False	2010-09-02 12:25:36.000000 UTC	N/A	Disabled
436	744	prl_tools_servi	0x82189530	3	78	0	False	2010-09-02 12:25:36.000000 UTC	N/A	Disabled
632	436	prl_tools.exe	0x82086798	9	107	0	False	2010-09-02 12:25:36.000000 UTC	N/A	Disabled
660	744	sqlwriter.exe	0x821aa7e8	4	84	0	False	2010-09-02 12:25:36.000000 UTC	N/A	Disabled
2180	1084	wscntfy.exe	0x8213dd00	3	48	0	False	2010-09-02 12:25:41.000000 UTC	N/A	Disabled
2588	744	alg.exe	0x81e8a368	6	107	0	False	2010-09-02 12:25:44.000000 UTC	N/A	Disabled
940	1084	wuauctl.exe	0x8205dda0	4	126	0	False	2010-09-02 12:26:40.000000 UTC	N/A	Disabled
2972	1752	ImmunityDebugge	0x82001ad0	2	87	0	False	2010-09-08 19:14:36.000000 UTC	N/A	Disabled
2204	2972	nifek_locked.ex	0x8207bda0	2	38	0	False	2010-09-08 19:14:36.000000 UTC	N/A	Disabled
1932	1752	ImmunityDebugge	0x82282380	2	86	0	False	2010-09-08 19:23:02.000000 UTC	N/A	Disabled
952	1932	vaelh.exe	0x8223c020	2	40	0	False	2010-09-08 19:23:02.000000 UTC	N/A	Disabled
3788	1752	ImmunityDebugge	0x81ffbd6d8	2	103	0	False	2010-09-08 22:39:40.000000 UTC	N/A	Disabled
3508	3788	anaxu.exe	0x8219e5c8	2	54	0	False	2010-09-08 22:39:40.000000 UTC	N/A	Disabled
3984	1084	wuauctl.exe	0x81eab2f8	8	325	0	False	2010-09-09 19:52:45.000000 UTC	N/A	Disabled
2404	1752	ImmunityDebugge	0x82066478	2	85	0	False	2010-09-09 19:56:19.000000 UTC	N/A	Disabled
3772	2404	b98679df6defbb3	0x81f4bb28	1	46	0	False	2010-09-09 19:56:19.000000 UTC	N/A	Disabled
3276	3772	ihah.exe	0x81e87da0	1	45	0	False	2010-09-09 19:56:32.000000 UTC	N/A	Disabled
3768	1084	rundll32.exe	0x82311648	1	53	0	False	2010-09-09 19:56:33.000000 UTC	N/A	Disabled

Time Stamp: Mon Dec 16 18:12:00 2024

pstree

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0x823c8a00	57	671	N/A	False	N/A	-
* 596	4	smss.exe	0x82292da0	3	19	N/A	False	2010-09-02 12:25:18.000000 UTC	N/A
** 692	596	winlogon.exe	0x822c09f8	21	588	0	False	2010-09-02 12:25:22.000000 UTC	N/A
*** 744	692	services.exe	0x821a5da0	15	279	0	False	2010-09-02 12:25:22.000000 UTC	N/A
**** 992	744	svchost.exe	0x822c8bf8	10	277	0	False	2010-09-02 12:25:22.000000 UTC	
**** 1192	744	svchost.exe	0x8214f488	13	175	0	False	2010-09-02 12:25:23.000000 UTC	
**** 488	744	sqlservr.exe	0x8208abf0	25	306	0	False	2010-09-02 12:25:33.000000 UTC	
**** 364	744	svchost.exe	0x82129370	4	88	0	False	2010-09-02 12:25:33.000000 UTC	
**** 912	744	svchost.exe	0x82150b90	20	202	0	False	2010-09-02 12:25:22.000000 UTC	
**** 1616	744	spoolsv.exe	0x82095500	13	140	0	False	2010-09-02 12:25:24.000000 UTC	
**** 1140	744	svchost.exe	0x821521b0	6	81	0	False	2010-09-02 12:25:22.000000 UTC	
**** 436	744	prl_tools_servi	0x82189530	3	78	0	False	2010-09-02 12:25:36.000000 UTC	
**** 632	436	prl_tools.exe	0x82086798	9	107	0	False	2010-09-02 12:25:36.000000 UTC	
**** 660	744	sqlwriter.exe	0x821aa7e8	4	84	0	False	2010-09-02 12:25:36.000000 UTC	
**** 472	744	jqs.exe	0x82089558	5	146	0	False	2010-09-02 12:25:33.000000 UTC	N/A
**** 1436	744	iscsие.exe	0x8221e278	6	78	0	False	2010-09-02 12:25:24.000000 UTC	
**** 1084	744	svchost.exe	0x82151da0	58	1327	0	False	2010-09-02 12:25:22.000000 UTC	
**** 3984	1084	wuauctl.exe	0x81eab2f8	8	325	0	False	2010-09-09 19:52:45.000000 UTC	
**** 940	1084	wuauctl.exe	0x8205dda0	4	126	0	False	2010-09-02 12:26:40.000000 UTC	
**** 2180	1084	wscntfy.exe	0x8213dd00	3	48	0	False	2010-09-02 12:25:41.000000 UTC	
**** 3768	1084	rundll32.exe	0x82311648	1	53	0	False	2010-09-09 19:56:33.000000 UTC	
**** 2588	744	alg.exe	0x81e8a368	6	107	0	False	2010-09-02 12:25:44.000000 UTC	N/A
**** 572	744	coherence.exe	0x82077da0	4	51	0	False	2010-09-02 12:25:36.000000 UTC	
**** 756	692	lsass.exe	0x822c8798	24	437	0	False	2010-09-02 12:25:22.000000 UTC	N/A
** 668	596	csrss.exe	0x821f2978	14	471	0	False	2010-09-02 12:25:21.000000 UTC	N/A
1752	1720	explorer.exe	0x821b2020	22	520	0	False	2010-09-02 12:25:25.000000 UTC	N/A
* 2404	1752	ImmunityDebugge	0x82066478	2	85	0	False	2010-09-09 19:56:19.000000 UTC	N/A
** 3772	2404	b98679df6defbb3	0x81f4bb28	1	46	0	False	2010-09-09 19:56:19.000000 UTC	N/A
*** 3276	3772	ihah.exe	0x81e87da0	1	45	0	False	2010-09-09 19:56:32.000000 UTC	
* 1900	1752	SharedIntApp.ex	0x822b96c0	3	75	0	False	2010-09-02 12:25:25.000000 UTC	N/A
* 1932	1752	ImmunityDebugge	0x82282380	2	86	0	False	2010-09-08 19:23:02.000000 UTC	N/A
* 952	1932	vaelh.exe	0x8223c020	2	40	0	False	2010-09-08 19:23:02.000000 UTC	N/A
* 3788	1752	ImmunityDebugge	0x81ffb6d8	2	103	0	False	2010-09-08 22:39:40.000000 UTC	N/A
* 3508	3788	anaxu.exe	0x8219e5c8	2	54	0	False	2010-09-08 22:39:40.000000 UTC	N/A
* 1938	1752	jusched.exe	0x8212ada0	1	43	0	False	2010-09-02 12:25:26.000000 UTC	N/A
* 1908	1752	prl_cc.exe	0x820ee580	14	133	0	False	2010-09-02 12:25:25.000000 UTC	N/A
* 2972	1752	ImmunityDebugge	0x82001ad0	2	87	0	False	2010-09-08 19:14:36.000000 UTC	N/A
** 2204	2972	nifek_locked.ex	0x8207bda0	2	38	0	False	2010-09-08 19:14:36.000000 UTC	N/A

Time Stamp: Mon Dec 16 18:14:12 2024

We can see from the process tree there's a sql server and there's a VM running on the system on startup (sqlserver.exe),(prl_tools.exe) which Parallels Tools for the running VM.

And some services for running it, in addition to some dll's

These are the cmd command and the full path for all these processes that we talked about

```
\System32\smss.exe    \SystemRoot\System32\smss.exe  \SystemRoot\System32\smss.exe
\System32\winlogon.exe winlogon.exe   (?)C:\WINDOWS\system32\winlogon.exe
\System32\services.exe C:\WINDOWS\system32\services.exe   C:\WINDOWS\system32\services.exe
\Windows\system32\svchost.exe C:\WINDOWS\system32\svchost -k rpcss   C:\WINDOWS\system32\svchost.exe
\Windows\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService C:\WINDOWS\system32\svchost.exe
\Program Files\Microsoft SQL Server\MSQL.1\MSSQL\Binn\sqlservr.exe "c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe" -sSQLEXPRESS c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe
\Windows\system32\svchost.exe -
\Windows\system32\svchost.exe C:\WINDOWS\system32\svchost -k DcomLaunch C:\WINDOWS\system32\svchost.exe
\Windows\system32\spoolsv.exe C:\WINDOWS\system32\spoolsv.exe C:\WINDOWS\system32\spoolsv.exe
\Windows\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkService C:\WINDOWS\system32\svchost.exe
\Program Files\Parallels\Parallels Tools\Services\prl_tools_service.exe -
\Program Files\Parallels\Parallels Tools\Services\prl_tools.exe "C:\Program Files\Parallels\Parallels Tools\Services\prl_tools.exe" C:\Program Files\Parallels\Parallels Tools\Services\prl_tools.exe
\Program Files\Microsoft SQL Server\90\Shared\sqwriter.exe "C:\Program Files\Microsoft SQL Server\90\Shared\sqwriter.exe" c:\Program Files\Microsoft SQL Server\90\Shared\sqwriter.exe
\Java\jre6\bin\jqs.exe "C:\Program Files\Java\jre6\bin\jqs.exe" -service -config "C:\Program Files\Java\jre6\lib\deploy\jqa\jqs.conf" C:\Program Files\Java\jre6\bin\jqs.exe
\Windows\system32\icscie.exe C:\WINDOWS\System32\icscie.exe C:\WINDOWS\System32\icscie.exe
\Windows\system32\svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvc C:\WINDOWS\System32\svchost.exe
\Windows\system32\wuauclt.exe "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\{43c1SUDS82f0c54ad7b58b46a717b19ec999e73f C:\WINDOWS\system32\wuauclt.exe
\Windows\system32\wuauclt.exe "C:\WINDOWS\system32\wuauclt.exe" C:\WINDOWS\system32\wuauclt.exe
\Windows\system32\wscnfy.exe C:\WINDOWS\System32\wscnfy.exe C:\WINDOWS\System32\wscnfy.exe
\Windows\System32\rundll32.exe C:\WINDOWS\System32\rundll32.exe C:\WINDOWS\System32\firewall.cpl>ShowNotificationDialog /configure "C:\WINDOWS\explorer.exe" C:\WINDOWS\System32\rundll32.exe
\sys32\alg.exe -
\Program Files\Parallels\Parallels Tools\Services\coherence.exe -
\sys32\lsass.exe C:\WINDOWS\system32\lsass.exe C:\WINDOWS\system32\lsass.exe
```

Nothing really seems suspicious to me till now

So, let's see and investigate the next processes block (that have a fresh start process tree)

1752	1720	explorer.exe	0x821b2020	22	520	0
* 2404	1752	ImmunityDebugge	0x82066478	2	85	0
** 3772	2404	b98679df6defbb3	0x81f4bb28	1	46	0
*** 3276	3772	ihah.exe	0x81e87da0	1	45	
* 1900	1752	SharedIntApp.ex	0x822b96c0	3	75	0
* 1932	1752	ImmunityDebugge	0x82282380	2	86	0
** 952	1932	vaelh.exe	0x8223c020	2	40	0
* 3788	1752	ImmunityDebugge	0x81ffb6d8	2	103	0
** 3508	3788	anaxu.exe	0x8219e5c8	2	54	0
* 1936	1752	jusched.exe	0x8212ada0	1	43	0
* 1908	1752	prl_cc.exe	0x820ee580	14	133	0
* 2972	1752	ImmunityDebugge	0x82001ad0	2	87	0
** 2204	2972	nifek locked.ex	0x8207bda0	2	38	0

We can see there's a process for Immunity Debugger that has been executed from the explorer, and then it opened another application that has a very suspicious name (b98679df6defbb3), and this suspicious process executed another process (vaelh.exe).

Each time Immunity Debugger executes, it executes another suspicious process.

We need to see the full name and the full path of these processes

```
\Device\HarddiskVolume1\WINDOWS\explorer.exe      C:\WINDOWS\Explorer.EXE C:\WINDOWS\Explorer.EXE
\Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe      "C:\Program
\Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\b98679df6defbb3dc0e12463880c9dd7.exe
N/A      \Device\HarddiskVolume1\Documents and Settings\Administrator\Application Data\Obyt\ihah.exe      "C:
\Device\HarddiskVolume1\Program Files\Parallels\Parallels Tools\ SIA\SharedIntApp.exe      "C:\Program Files\P
\Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe      "C:\Program
\Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\vaelh.exe      "C:\Documents and Settings\
\Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe      "C:\Program
\Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\anaxu.exe      "C:\Documents and Settings\
\Device\HarddiskVolume1\Program Files\Java\jre6\bin\jusched.exe "C:\Program Files\Java\jre6\bin\jusched.exe
\Device\HarddiskVolume1\Program Files\Parallels\Parallels Tools\prl_cc.exe      "C:\Program Files\Parallels
\Device\HarddiskVolume1\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe      "C:\Program
\Device\HarddiskVolume1\Documents and Settings\Administrator\Desktop\nifek locked.exe      "C:\Documents and S
```

We can see the full name and path for the executed programs, there's one of them that has a long alphanumeric name that seems like a hash
(b98679df6defbb3dc0e12463880c9dd7.exe) Let's check if it's a valid hash or not using hash analyzer online tool [🔗](#):

Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

Analyze

Hash:	b98679df6defbb3dc0e12463880c9dd7
Salt:	Not Found
Hash type:	MD5 or MD4
Bit length:	128
Character length:	32
Character type:	hexidecimal

Now we are sure that the process name is a valid MD5 hash, Let's check [Virustotal](#)

46/54 security vendors flagged this file as malicious

Community Score: 46 / 54

Ydeku

peexe

Size: 165.50 KB | Last Analysis Date: 9 years ago | EXE

DETECTION **DETAILS** **COMMUNITY** 4

Basic properties

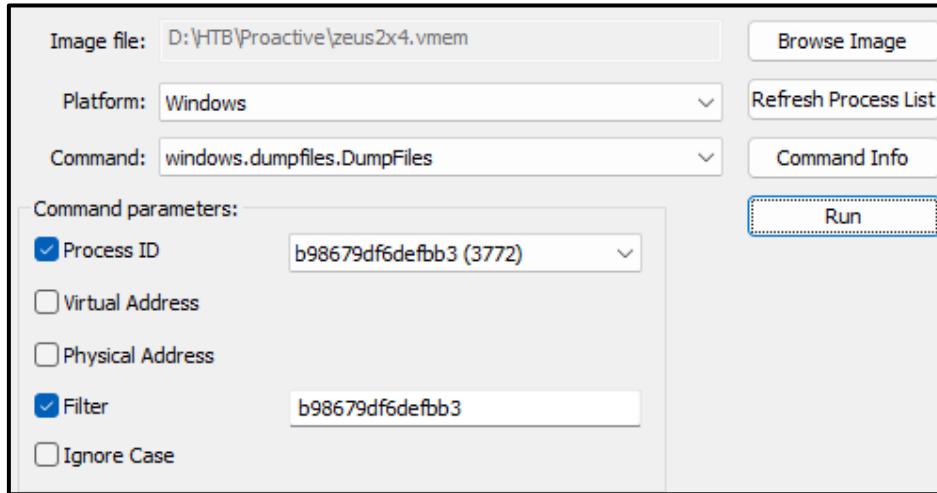
MD5	b98679df6defbb3dc0e12463880c9dd7
SHA-1	126326ba5a74ac903a7655d04403f88ea75f9a542
Vhash	659e4e7d8e33a9945b228c60d31f3924212126ecd2a2604baf28c7539a4d4230
Authentihash	015046655d15506424100ff7z48z150029zf
Impishash	4736a55e9d9995acc45eb62f3995cf83b079b46ecb3f99bb20afb317a37486e8
SSDeep	e3558ed4938f8c18e5cf2f201d32245c
File type	3072:NDTTPBmEJxvqOIEExymdqejT2lenes8bWWQDjJGXNYyR32d02dMdhECfp:NDTTPVnynulbVWcdgayZ262uTf
Magic	Win32 EXE executable windows win32 pe peexe
TrID	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	Win32 Executable MS Visual C++ (generic) (67.3%) Win32 Dynamic Link Library (generic) (14.2%) Win32 Executable (generic) (9.7%) Generic Win/DOS Executable (4....
	165.50 KB (169472 bytes)

History

Creation Time	2008-07-12 15:50:54 UTC
First Seen In The Wild	2017-11-07 23:42:59 UTC
First Submission	2010-04-16 22:40:03 UTC
Last Submission	2015-11-15 07:03:25 UTC
Last Analysis	2015-11-15 07:03:25 UTC

There won't be a clear way to confirm if it's harmful or not such as Virustotal score.

Now let's dump the process and make a quick investigation into it



Using Exiftool on it to see the metadata of the file

```
(kali㉿kali)-[~/media/sf_HTB/Proactive]
$ exiftool file.0x82069028.0x82005ca0.ImageSectionObject.b98679df6defbb3dc0e12463880c9dd7.exe.img
ExifTool Version Number          : 13.00
File Name                      : file.0x82069028.0x82005ca0.ImageSectionObject.b98679df6defbb3dc0e12463880c9dd7.exe.img
Directory                       :
File Size                       : .
File Modification Date/Time    : 2024:12:16 12:34:01-05:00
File Access Date/Time          : 2024:12:16 12:54:28-05:00
File Inode Change Date/Time   : 2024:12:16 12:34:20-05:00
File Permissions                : -rwxrwx—
File Type                       : Win32 EXE
File Type Extension            : exe
MIME Type                       : application/octet-stream
Machine Type                   : Intel 386 or later, and compatibles
Time Stamp                      : 2008:07:12 11:50:54-04:00
Image File Characteristics     : No relocs, Executable, 32-bit
PE Type                         : PE32
Linker Version                 : 9.0
Code Size                       : 141824
Initialized Data Size          : 59392
Uninitialized Data Size        : 0
Entry Point                     : 0x1880b
OS Version                      : 5.0
Image Version                  : 0.0
Subsystem Version               : 5.0
Subsystem                        : Windows GUI
File Version Number             : 10.6.1094.74
Product Version Number          : 10.6.1094.74
File Flags Mask                 : 0x003f
File Flags                       : (none)
File OS                          : Windows NT 32-bit
Object File Type                : Executable application
File Subtype                    : 0
Language Code                  : English (U.S.)
Character Set                  : Unicode
Company Name                    : Yldaepupreapagytek
File Description                : Igkyliybotetafwa
Original File Name              : Ydeku
Internal Name                   : Wefietrenuyz
Legal Copyright                 : Egewylvekeez
Legal Trademarks                : Ufhokibiedqereo
Product Name                     : Iwhahu
```

We can see these attributes are not specific or even written using an appropriate English language so it's more suspicious to be malicious, we can see the original file name is the same file name we see on [virustotal \(Ydeku\)](#).

Now let's return to this image and analyze the rest suspicious files that are child processes for this malicious file:

1752	1720	explorer.exe	0x821b2020	22	520	0	
*	2404	1752	ImmunityDebugge	0x82066478	2	85	0
**	3772	2404	b98679df6defbb3	0x81f4bb28	1	46	0
***	3276		3772 ihah.exe	0x81e87da0	1	45	
*	1900	1752	SharedIntApp.ex	0x822b96c0	3	75	0
*	1932	1752	ImmunityDebugge	0x82282380	2	86	0
**	952	1932	vaelh.exe	0x8223c020	2	40	0
*	3788	1752	ImmunityDebugge	0x81ffb6d8	2	103	0
**	3508	3788	anaxu.exe	0x8219e5c8	2	54	0
*	1936	1752	jusched.exe	0x8212ada0	1	43	0
*	1908	1752	prl_cc.exe	0x820ee580	14	133	0
*	2972	1752	ImmunityDebugge	0x82001ad0	2	87	0
**	2204	2972	nifek locked.ex	0x8207bda0	2	38	0

Now Let's Dump (**ihah.exe**) and investigate it:

```
(kali㉿kali)-[~/media/sf_HTB/Proactive]
└─$ exiftool file.0x81e815c8.0x82247520.ImageSectionObject.ihah.exe.img
ExifTool Version Number          : 13.00
File Name                        : file.0x81e815c8.0x82247520.ImageSectionObject.ihah.exe.img
Directory                         :
File Size                         : 172 kB
File Modification Date/Time     : 2024:12:16 13:27:21-05:00
File Access Date/Time           : 2024:12:16 13:27:46-05:00
File Inode Change Date/Time    : 2024:12:16 13:27:37-05:00
File Permissions                 : -rwxrwx—
File Type                         : Win32 EXE
File Type Extension              : exe
MIME Type                         : application/octet-stream
Machine Type                     : Intel 386 or later, and compatibles
Time Stamp                        : 2008:01:25 09:18:42-05:00
Image File Characteristics      : No relocs, Executable, 32-bit
PE Type                           : PE32
Linker Version                   : 9.0
Code Size                         : 142336
Initialized Data Size            : 59392
Uninitialized Data Size          : 0
Entry Point                      : 0xc294
OS Version                        : 5.0
Image Version                    : 0.0
Subsystem Version                 : 5.0
Subsystem                          : Windows GUI
File Version Number               : 7.3.2484.1905
Product Version Number            : 7.3.2484.1905
File Flags Mask                  : 0x003f
File Flags                         : (none)
File OS                            : Windows NT 32-bit
Object File Type                 : Executable application
File Subtype                      : 0
Language Code                     : English (U.S.)
Character Set                     : Unicode
Company Name                      : Ynagzakoykfeziucbye
File Description                  : Vuupfaopescoydba
Original File Name                : Axumexupleopikoft
Internal Name                     : Wyzesofooqbukyabykb
Legal Copyright                   : Haezmoxacamedua
Legal Trademarks                  : Ziypewurkaucitamifg
Product Name                      : Bydoycgui
```

Also, another random characters that doesn't represent a name at all.

The original name of the file (**Axumexupleopikoft**) that we got from Exiftool, is the same as shown in [virustotal](#).

Security vendors' analysis				Do you want to automate checks?		
Ad-Aware	Gen:Trojan.Heur.Zbot.4	AegisLab	Troj.Crypt.XPACK.Gen.IBT4			
AhnLab-V3	Trojan/Win32.Zbot	Arcabit	Trojan.Heur.Zbot.4			
Avast	Win32.Zbot-MSU [Trj]	AVG	Cryptic.ERX			
Avira (no cloud)	TR/ATRAPS.Gen2	AVware	Trojan-PWS.Win32.Zbot.gen.y (v)			
Baidu	Win32.Trojan.WisdomEyes.151026.9950....	BitDefender	Gen:Trojan.Heur.Zbot.4			
Bkav Pro	HW32.Packed.F6B2	CMC	Trojan-Spy.Win32.Zbot.110			

And so on for all other files, all of them has a High Community Score and seems to be malicious

1752	1720	explorer.exe	0x821b2020	22	520	0
* 2404	1752	ImmunityDebugge	0x82066478	2	85	0
** 3772	2404	b98679df6defbb3	0x81f4bb28	1	46	0
*** 3276		ihah.exe	0x81e87da0	1	45	
* 1900	1752	SharedIntApp.ex	0x822b96c0	3	75	0
* 1932	1752	ImmunityDebugge	0x82282380	2	86	0
** 952	1932	vaelh.exe	0x8223c020	2	40	0
* 3788	1752	ImmunityDebugge	0x81ffb6d8	2	103	0
** 3508	3788	anaxu.exe	0x8219e5c8	2	54	0
* 1936	1752	jusched.exe	0x8212ada0	1	43	0
* 1908	1752	prl_cc.exe	0x820ee580	14	133	0
* 2972	1752	ImmunityDebugge	0x82001ad0	2	87	0
** 2204	2972	nifek_locked.ex	0x8207bda0	2	38	0

vaelh.exe

Analysis :

```
(kali㉿kali)-[~/media/sf_HTB/Proactive]
$ exiftool file.0x82263470.0x820f3eb8.ImageSectionObject.vaelh.exe.img
ExifTool Version Number : 13.00
File Name : file.0x82263470.0x820f3eb8.ImageSectionObject.vaelh.exe.img
Directory : .
File Size : 107 kB
File Modification Date/Time : 2024:12:16 13:36:50-05:00
File Access Date/Time : 2024:12:16 13:39:38-05:00
File Inode Change Date/Time : 2024:12:16 13:37:02-05:00
File Permissions : -rwxrwx—
File Type : Win32 EXE
File Type Extension : exe
MIME Type : application/octet-stream
Machine Type : Intel 386 or later, and compatibles
Time Stamp : 1998:06:28 02:34:08-04:00
Image File Characteristics : No relocs, Executable, 32-bit
PE Type : PE32
Linker Version : 8.8
Code Size : 98304
Initialized Data Size : 8192
Uninitialized Data Size : 36864
Entry Point : 0x21c90
OS Version : 4.0
Image Version : 0.0
Subsystem Version : 4.0
Subsystem : Windows GUI
File Version Number : 8.5.0.3
Product Version Number : 8.5.0.3
File Flags Mask : 0x003f
File Flags : (none)
File OS : Windows NT 32-bit
Object File Type : Dynamic link library
File Subtype : 0
Language Code : Neutral
Character Set : Unicode
File Version : 8.5.0.3
Product Version : 8.5.0.3
File Description : Kaspersky Anti-Virus
Company Name : Kaspersky Lab
Legal Copyright : Copyright © Kaspersky Lab 1997-2009.
Product Name : Kaspersky Anti-Virus
Legal Trademarks : Kaspersky™ Anti-Virus ® is registered trademark of Kaspersky Lab.
Internal Name : AVP
```

Based on the information from the metadata of the (**vaelh.exe**) file we can see that it doesn't seem suspicious , whether virustotal has a high score to me malicious,

But virustotal has a high score based on 57 security vendors that flagged this as a malicious file, whether it seems that it has a valid File Description, Company name, legal copyright, product name. As shown in the following image it seems that it's packed with UPX

Community Score: 57 / 74

57/74 security vendors flagged this file as malicious

a70aa9b1b476e59d41646a43ef553f671566a195ff04b5d2243fa363c562f6e0
vaelh.img

peexe upx overlay

Size: 104.50 KB | Last Analysis Date: 5 years ago | EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Security vendors' analysis: 57/74

Do you want to automate checks?

Acronis (Static ML): Suspicious

Ad-Aware: Ad-Aware

Trojan.Generic.6031795

We can see it also from Detect it easy that it's packed with UPX and has a high entropy in the code which means that the file contains data that appears highly random or lacks recognizable patterns. (Entropy is a measure of uncertainty or randomness in data)

Type: PE32 | Sections: 00000000 | Size: 0001a200

Total: 7.64377 | Status: packed(95%)

PE32

Operation system: Windows(95)[I386, 32-bit, GUI]

Packer: UPX(3.03)[NRV,brute]

Overlay: Binary

(kali㉿kali)-[~/media/sf_HTB/Proactive]\$ exiftool file.0x82386bb0.0x8204f288.ImageSectionObject.anaxu.exe.img

File Name : file.0x82386bb0.0x8204f288.ImageSectionObject.anaxu.exe

File Size : 219 kB

File Modification Date/Time : 2024:12:16 13:51:46-05:00

File Access Date/Time : 2024:12:16 13:52:14-05:00

File Inode Change Date/Time : 2024:12:16 13:51:58-05:00

File Permissions : -rwxrwx—

File Type : Win32 EXE

File Type Extension : exe

MIME Type : application/octet-stream

Machine Type : Intel 386 or later, and compatibles

Time Stamp : 2005:07:23 17:40:54-04:00

Image File Characteristics : Executable, No line numbers, No symbols, 32-bit

PE Type : PE32

Linker Version : 7.0

Code Size : 53248

Initialized Data Size : 185344

Uninitialized Data Size : 0

Entry Point : 0xda30

OS Version : 8.4

Image Version : 6.0

Subsystem Version : 4.0

Subsystem : Windows GUI

File Version Number : 60.40.109.60

Product Version Number : 60.40.109.60

File Flags Mask : 0x003f

File Flags : (none)

File OS : Windows NT 32-bit

Object File Type : Executable application

File Subtype : 0

Language Code : Unknown (0681)

Character Set : Unknown (7EA3)

Company Name : ЛюбопытныйИзХобЧСШЖИ

File Description : школьГрбхбрЩзлнИИдщдл

File Version : 60.40.109.60

Internal Name : ИмпереоВКУлКцФобКилншэШФ

Legal Copyright : 7119-6856

Original File Name : 6sNkp.exe

Product Name : стГЦктиШЬХЖУдгюГтвРраЖЖ

Product Version : 60.40.109.60

Seems so suspicious to me, let's check virustotal also:

54 / 73

Community Score

54/73 security vendors flagged this file as malicious

216a3cb0d30054825e1b5decb141001c7ff20962f88e79e69c5cc7bd8324496f
anaxu.img

peexe overlay

Size 213.50 KB | Last Analysis Date 5 years ago | EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security vendors' analysis Do you want to automate checks?

Vendor	Result	Malware Type
Acronis (Static ML)	Suspicious	Ad-Aware
AegisLab	Trojan.Win32.Generic.4ic	Alibaba
		(?) PWSteal:Win32/Obfuscator.5fa7a396

NOTE: I didn't use (**windows.malfind**) plugin as it's not precise also, all files that I scanned above **malfind** found in addition to a lot of other false positive files, so I don't recommend using it.

All these files that we scanned were malicious, so let's see the network stats

We have two plugins in **volatility 2 (connscan)** which makes pool scanner for tcp connections, and (**connections**) which Prints list of open connections

connscan plugin

Offset(P)	Local Address	Remote Address	Pid
0x020f5410	10.211.55.5:1427	65.54.81.89:80	1084
0x02125008	10.211.55.5:1423	207.46.21.123:80	1084
0x022ace08	10.211.55.5:1432	193.43.134.14:80	1752

pid 1084 → svchost.exe

pid 1752 → explorer.exe

connection plugin

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

Explanation:

Since the malicious file has been executed from the explorer, (**ppid of his ppid is explorer.exe**), so we will focus on the explorer.exe connection, also because the other connections in connscan had belonged to svchost.exe, which is the main process of any running windows machine. Let's also check what I've said using virustotal

Scanning the ip address (**65.54.81.89**) which belongs to (**svchost.exe**) process

No security vendor flagged this IP address as malicious

65.54.81.89 (65.54.0.0/15)
AS 8075 (MICROSOFT-CORP-MSN-AS-BLOCK)

Community Score 0 / 94

US

Scanning the ip address (**207.46.21.123**) which belongs to (**svchost.exe**) process

10+ detected files communicating with this IP address

207.46.21.123 (207.46.0.0/19)
AS 8075 (MICROSOFT-CORP-MSN-AS-BLOCK)

Community Score 0 / 94

US

Now, Scanning the ip address (**193.43.134.14**) which belongs to (**explorer.exe**) process

4/94 security vendors flagged this IP address as malicious

193.43.134.14 (193.43.134.0/24)
AS 47583 (Hostinger International Limited)

Community Score 4 / 94

Last Analysis Date 14 days ago

US

So, I'm right, the malicious ip address must be related to (**explorer.exe**) process

Also, it has suspicious files dropped related to that ip address (**193.43.134.14**)

Communicating Files (2) ⓘ

Scanned	Detections	Type	Name
2020-05-02	56 / 72	Win32 EXE	b11502636f33742794df31e2e8290151.virus
2020-10-21	53 / 62	Win32 EXE	Wefietrenuyz

Let's check the second one :

53 / 62 security vendors flagged this file as malicious

8b65b15cd919828c01fe0ef859775d9cdea11973db568da80d601b04c546ae7b
Ydeku
peexe overlay

Size 168.00 KB | Last Analysis Date 4 years ago | EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Dynamic Analysis Sandbox Detections ⓘ

The sandbox Tencent HABO flags this file as: MALWARE

Security vendors' analysis ⓘ

			Do you want to automate checks?
Acronis (Static ML)	! Suspicious	Ad-Aware	! Gen:Trojan.Heur.Zbot.4
AhnLab-V3	ⓘ Trojan/Win32.Zbot.R1982	Arcabit	! Trojan.Heur.Zbot.4

(Ydeku), I think we've seen this before. Let's go to Details section and get the names and Signature info :

Names

Wefietrenuyz
Ydeku

file.None.0x822e08c0.dat

Signature info

Signature Verification

△ File is not signed

File Version Information

Copyright	Egewylvekeez
Product	lwhahu
Description	lqkyliybotetafwa
Original Name	Ydeku
Internal Name	Wefietrenuyz

From the first malicious process which its name was a valid MD5 hash (**b98679df6defbb3dc0e12463880c9dd7.exe**) has this scan :

Community Score 46 / 54

46/54 security vendors flagged this file as malicious

659e4e7d8e33a9945b228c60d31f3924212126ecd2a2604ba28c7539a4d4230

Ydeku

peexe

Size 165.50 KB

Last Analysis Date 9 years ago

EXE

REANALYZE SIMILAR MORE

DETECTION DETAILS COMMUNITY 4

Security vendors' analysis

AhnLab-V3	Trojan/Win32.Zbot	Antiy-AVL	Trojan[Packed]/Win32.Krap
Arcabit	Trojan.Heur.Zbot.4	Avast	Win32.Zbot-MSU [Trj]

And has these details:

Names

f26326f5a74ac903a7655d44037f88ea75f9a542_eu2.ex

Wefietrenuyz
Ydeku

l.php-m9dzF5
aa
EXCV.cpl

Signature info

Signature Verification

△ File is not signed

File Version Information

Copyright	Egewylvekeez
Product	lwhahu
Description	lqkyliybotetafwa
Original Name	Ydeku
Internal Name	Wefietrenuyz

YARA Rules

Create rules based on all malicious files that we've got from the memory dump and from Zeus Banking Malware.

First, Creating a custom rule based on all malicious files, all malicious file we need :

- invoice_2318362983713_823931342io.pdf.exe
- b98679df6defbb3dc0e12463880c9dd7.exe
- ihah.exe
- vaelh.exe
- anaxu.exe

```
└─(kali㉿kali)-[~/Desktop/Proactive]
$ ls
file.0x81e815c8.0x82247520.ImageSectionObject.ihah.exe.img
file.0x82069028.0x82005ca0.ImageSectionObject.b98679df6defbb3dc0e12463880c9dd7.exe.img
file.0x82263470.0x820f3eb8.ImageSectionObject.vaelh.exe.img
file.0x82386bb0.0x8204f288.ImageSectionObject.anaxu.exe.img
invoice_2318362983713_823931342io.pdf.exe
```

Generating the YARA rules using this command:

```
└─$ sudo python3 yarGen.py -m /home/kali/Desktop/Proactive/ -o /home/kali/Desktop/YaraGen.yar
```

```
└─(kali㉿kali)-[~/yarGen]
$ sudo python3 yarGen.py -m /home/kali/Desktop/Proactive/ -o /home/kali/Desktop/YaraGen.yar
/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 'Proactive'
[+] Using reference 'https://github.com/Neo23x0/yarGen'
[+] Using prefix 'Proactive'
[+] 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)
```

Let's read a sample of the YARA Rule that we generated:

```
1 /*
2  * YARA Rule Set
3  * Author: yarGen Rule Generator
4  * Date: 2024-12-16
5  * Identifier: Malicious_Findings
6  * Reference: https://github.com/Neo23x0/yarGen
7 */
8
9 /* Rule Set _____ */
10
11 rule _home_kali/Desktop_Malicious_Findings_ihah {
12     meta:
13         description = "Malicious_Findings - file ihah.exe"
14         author = "yarGen Rule Generator"
15         reference = "https://github.com/Neo23x0/yarGen"
16         date = "2024-12-16"
17         hash1 = "3b39bfc8c57c36b359d48506f6fada498407af5fb8cc9775e9aa4bd35c064470"
18     strings:
19         $s1 = "      <requestedExecutionLevel level=\"asInvoker\" uiAccess=\"false\"></requestedExecutionLevel>" fullword ascii
20         $s2 = "AAA8AAAAAAA" ascii /* base64 encoded string '==<+++++' */
21         $s3 = "      <description>Kee i l hiywildy ow</description>" fullword ascii
22         $s4 = "      processorArchitecture=\"*\" fullword ascii
23         $s5 = "      processorArchitecture=\"X86\" fullword ascii
24         $s6 = "      publicKeyTokens=\"6595b64144ccf1df\" fullword ascii
25         $s7 = "      version=\"6.0.0.0\" fullword ascii
26         $s8 = "      <trustInfo xmlns=\"urn:schemas-microsoft-com:asm.v3\">" fullword ascii
27         $s9 = "IIIIIIIVII" fullword ascii
28         $s10 = "BBBBBBBBBBBBBBBB" fullword ascii
29         $s11 = "JJJJJJJJJJHJJJJJJ" fullword ascii
30         $s12 = "IIIVIIBI" fullword ascii
31         $s13 = "JJFJJJJJ" fullword ascii
32         $s14 = "DINGXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGXXPADDING" fullword ascii
33         $s15 = "      name=\"Microsoft.Windows.Common-Controls\" fullword ascii
34         $s16 = "Ynagzakoykfzeiucbye" fullword wide
35         $s17 = "Vuupfaopescydba" fullword wide
36         $s18 = "Axumexupleopikoft" fullword wide
37         $s19 = "Wyzesofooqbukyabykb" fullword wide
38         $s20 = "Ziypewurkaucitamifg" fullword wide
39     condition:file_0x82069028_0x82005ca0_ImageSectionObject_b98679df6defbb3dc0e12463880c9dd7_exe
40     uint16(0) = 0x5a4d and filesize < 500KB and
41     8 of them
42 }
```

Now let's run the YARA rule on all malicious files inside (Malicious_Findings) Directory using this command:

```
1. ↴ $ yara YaraGen.yar Malicious_Findings
```

```
[kali㉿kali)-[~/Desktop]
$ yara YaraGen.yar Malicious_Findings
/home_kali/Desktop_Malicious_Findings_ihah Malicious_Findings/ihah.exe
b98679df6defbb3dc0e12463880c9dd7 Malicious_Findings/ihah.exe
/home_kali/Desktop_Malicious_Findings_vaelh Malicious_Findings/vaelh.exe
/home_kali/Desktop_Malicious_Findings_anaxu Malicious_Findings/anaxu.exe
invoice_2318362983713_823931342io_pdf Malicious_Findings/invoice_2318362983713_823931342io.pdf.exe
b98679df6defbb3dc0e12463880c9dd7 Malicious_Findings/b98679df6defbb3dc0e12463880c9dd7.exe
```

Run YARA command to print matching strings (Here's a sample of the whole output):

```
1. └$ yara -s YaraGen.yar Malicious_Findings
```

```
└──(kali㉿kali)-[~/Desktop]
$ yara -s YaraGen.yar Malicious_Findings
/home_kali/Desktop_Malicious_Findings_ihah Malicious_Findings/ihah.exe
0x29664:$s1: <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
0x7e68:$s2: AAA8AAAAAAA
0x83ba:$s2: AAA8AAAAAAA
0x29481:$s3: <description>Kea i l hiywldy ow</description>
0x29424:$s4: processorArchitecture="*"
0x2955e:$s5: processorArchitecture="X86"
0x29585:$s6: publicKeyToken="6595b64144ccf1df"
0x29541:$s7: version="6.0.0.0"
0x295ff:$s8: <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
0x84e1:$s9: IIIJIIVIII
0x8373:$s10: BBBB BBBB BBBB BBBB
0x7f67:$s11: JJJJJJJJJHJJJJJ
0x8220:$s12: IIIVIIBI
0x81c1:$s13: JJFJJJJJ
0x2950d:$s15: name="Microsoft.Windows.Common-Controls"
0x29158:$s16: Y\x00n\x00a\x00g\x00z\x00a\x00k\x00o\x00y\x00k\x00f\x00e\x00z\x00i\x00u\x00c\x00b\x00y\x00e\x00
0x291a8:$s17: V\x00u\x00o\x00p\x00f\x00a\x00o\x00p\x00e\x00s\x00c\x00o\x00y\x00d\x00b\x00a\x00
0x291f4:$s18: A\x00x\x00u\x00m\x00e\x00x\x00x\x00u\x00p\x00l\x00e\x00o\x00p\x00i\x00k\x00o\x00\x00f\x00t\x00
0x29238:$s19: W\x00y\x00z\x00e\x00s\x00o\x00f\x00o\x00o\x00q\x00b\x00u\x00k\x00y\x00a\x00b\x00y\x00k\x00b\x00
0x292cc:$s20: Z\x00i\x00y\x00p\x00e\x00w\x00u\x00r\x00k\x00a\x00u\x00c\x00i\x00t\x00a\x00m\x00i\x00f\x00g\x00
b98679df6defbb3dc0e12463880c9dd7 Malicious_Findings/ihah.exe
0x29664:$s1: <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
0x29562:$s3: processorArchitecture="X86"
0x29585:$s5: publicKeyToken="6595b64144ccf1df"
0x29541:$s7: version="6.0.0.0"
0x295ff:$s8: <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
0x29712:$s9: DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADINGPA
0x29722:$s9: DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
0x29732:$s9: DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
0x29742:$s9: DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
0x29752:$s9: DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
0x29762:$s9: DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
0x29772:$s9: DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
0x2950d:$s11: name="Microsoft.Windows.Common-Controls"
0x294b3:$s17: <dependency>
0x296f3:$s18: </trustInfo>
0x295ee:$s19: </dependency>
/home_kali/Desktop_Malicious_Findings_vaelh Malicious_Findings/vaelh.exe
0x19891:$s1: <requestedExecutionLevel level="asInvoker" uiAccess="false" />
0x17b25:$s2: GetCompu
```