

Lab 3: Malware analysis

Name: Mohamad Nour Shahin

Group number: B22-CBS-01

Questions to Answer

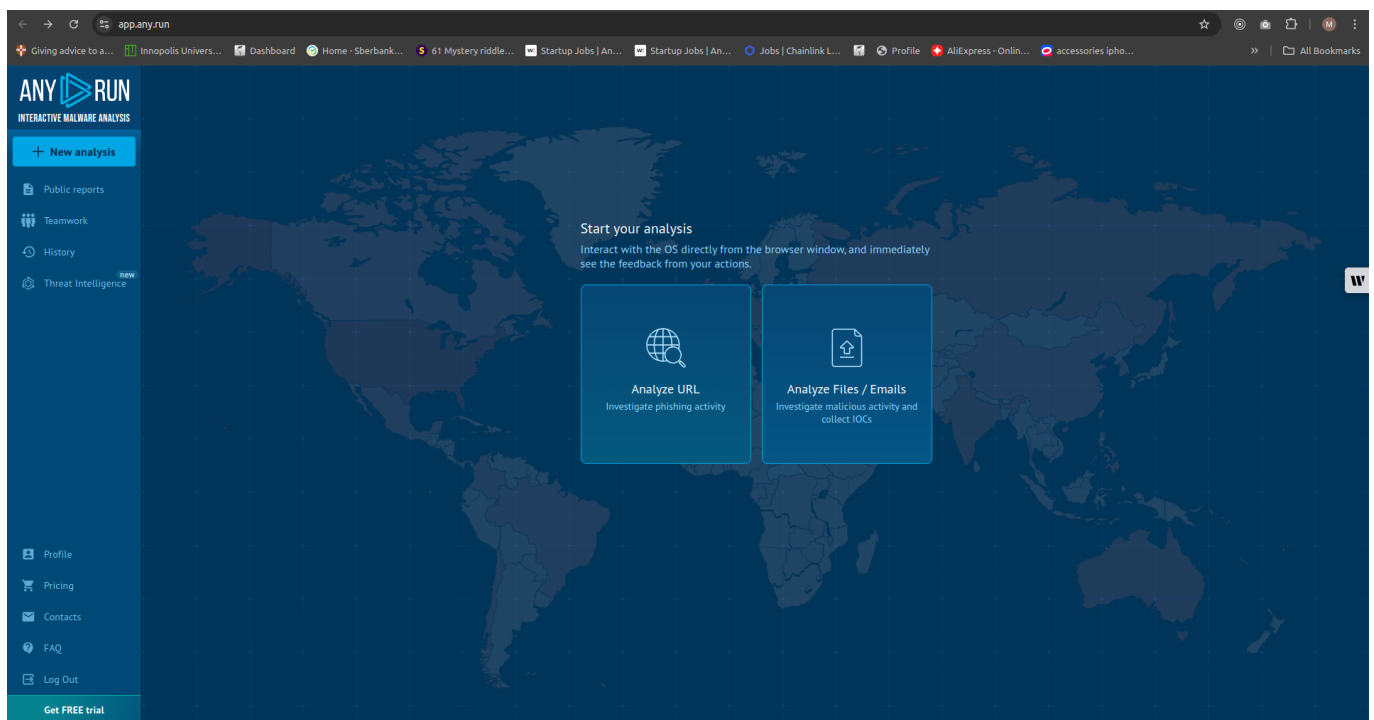
1. Preparation

Choose a sandboxing solution, some recommended ones includes the following.

- [Cuckoo \(Bonus point if you set up Cuckoo in an isolated VM\)](#)
- [Hybrid Analysis](#)
- [Any.run](#)
- [Intezer Analyze](#)
- [Joe Sandbox](#)

Solution:

I will choose third choice [Any.run](#) as we practice with it during lab. I created an account on it. here is the screenshot of it:



2. Let's get some malware

Select a malware that you want to analyse in the sandbox selected in step 1.

- You can download some malware/ransomware from the internet. For example [TheZoo](#), [MalwareBazaar Database](#). You can also check your email for any spam with malicious attachment.
- Don't select the same malware used in the classwork.
- Be careful when you run them, these are real malware.

Solution:

I searched in the [MalwareBazaar Database](#), and I will use this [Malware](#)

The screenshot shows the MalwareBazaar Database entry for a sample with SHA256 hash 01ec7b1066d7c55e262dc375bf5fd13a1fc9706c3db4b3522ac8b9d2453b52. The entry is categorized as TrickBot. The interface includes tabs for Intelligence, IOCs, YARA, File information, and Comments. The main content area displays various hashes (SHA256, SHA3-384, SHA1, MD5, humanhash), file name (GST INVOICE.exe), download link, signature (TrickBot), file size (689152 bytes), first/last seen dates, file type (exe), MIME type (application/x-dosexec), imphash, sdspep, TLSH, and TrID results. The reporter is listed as zocaman.

MalwareBazaar Database

This page let you download the following malware sample: **SHA256 01ec7b1066d7c55e262dc375bf5fd13a1fc9706c3db4b3522ac8b9d2453b52**

Caution!

You are about to download a malware sample. By clicking on "download", you declare that you have understood what you are doing and that MalwareBazaar can not be held accountable for any damage caused by downloading this malware sample!

ZIP password: infected

Download

© abuse.ch 2024

3. Sandbox analysis

Run your malware in the sandbox.

- See what kind of traces, artifacts, connections your sandbox detects.
- Analyze the behavior of the malware, and write about what the malware does and the goals of the malware.

- Does the malware have some sandbox detection? If yes, try to detect and defeat the techniques used for that.

Solution:

1. Firstly I downloaded the malware as zip, unzip, upload the file to the [Any.run](#) , and I will set the configuration:

MalwareBazaar Database

This page let you download the following malware sample: **SHA256 01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52**

Caution!

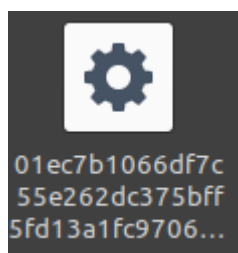
You are about to download a malware sample. By clicking on "download", you declare that you have understood what you are doing and that MalwareBazaar can not to be held accountable for any damage caused by downloading this malware sample!

ZIP password: **infected**

Download

© abuse.ch 2024

- after unzip it:



New analysis

Simple modePro mode

New VM video streaming beta

URL or file upload

01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe

Start object from

Open in browser

Temp directory

Microsoft Edge

Change extension to valid

On

Hide source

Command line

Type or choose a preset

Duration, sec

1015304560

Network

Connected

HTTPS MITM PROXY

Fake net

Route internet traffic through (optional):

Route via TOR

Residential proxy

User VPN (0/100)

Fastest geo

Choose

Add a confi

Privacy

Only me

Team

Who has a link

Public

The report will be deleted in

2 weeks

Preset configuration (1/100)

Default

Autosave changes

Operating system

Windows 10 (64 bit)

Auto confirm UAC

On

Pre-installed soft set

Complete

Locale (OS Language)

United States (en-US)

Applications

Hot fixes

Tools collection

CCleaner	6.20
Mozilla Firefox (x64 en-US)	123.0
Mozilla Maintenance Service	123.0
Notepad++ (64-bit x64)	7.9.1
Microsoft OneNote - en-us	16.0.16026.20146
Microsoft Office Professional 2019 - de-de	16.0.16026.20146
Microsoft Office Professional 2019 - en-us	16.0.16026.20146
Microsoft Office Professional 2019 - es-es	16.0.16026.20146
Microsoft Office Professionnel 2019 - fr-fr	16.0.16026.20146
Microsoft Office Professional 2019 - it-it	16.0.16026.20146
Microsoft Office Professional 2019 - ja-jp	16.0.16026.20146

Additional settings

Automated Interactivity (ML)

new

ChatGPT Access

Run a public analysis

- we add more time for analyzing.

Win10 64 bit

Complete

01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe

MD5: 9C7B97EB3958D4309E6BA38BB1A99471

Start: 11.09.2024, 13:23

01:54

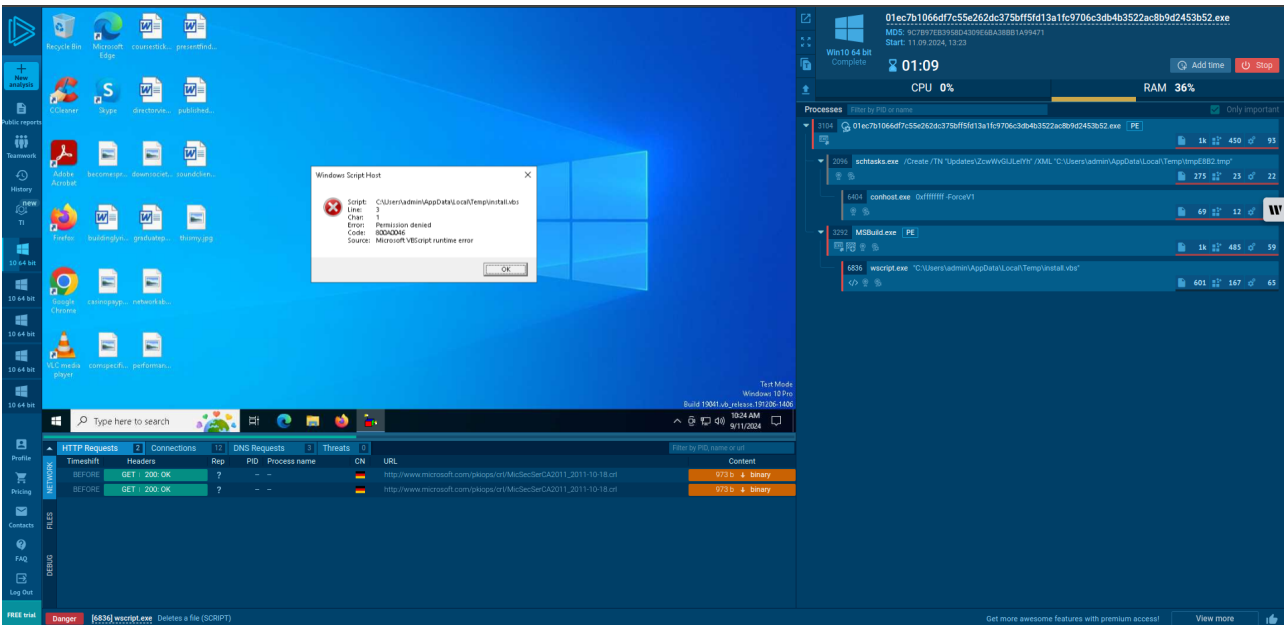
Add time

Stop

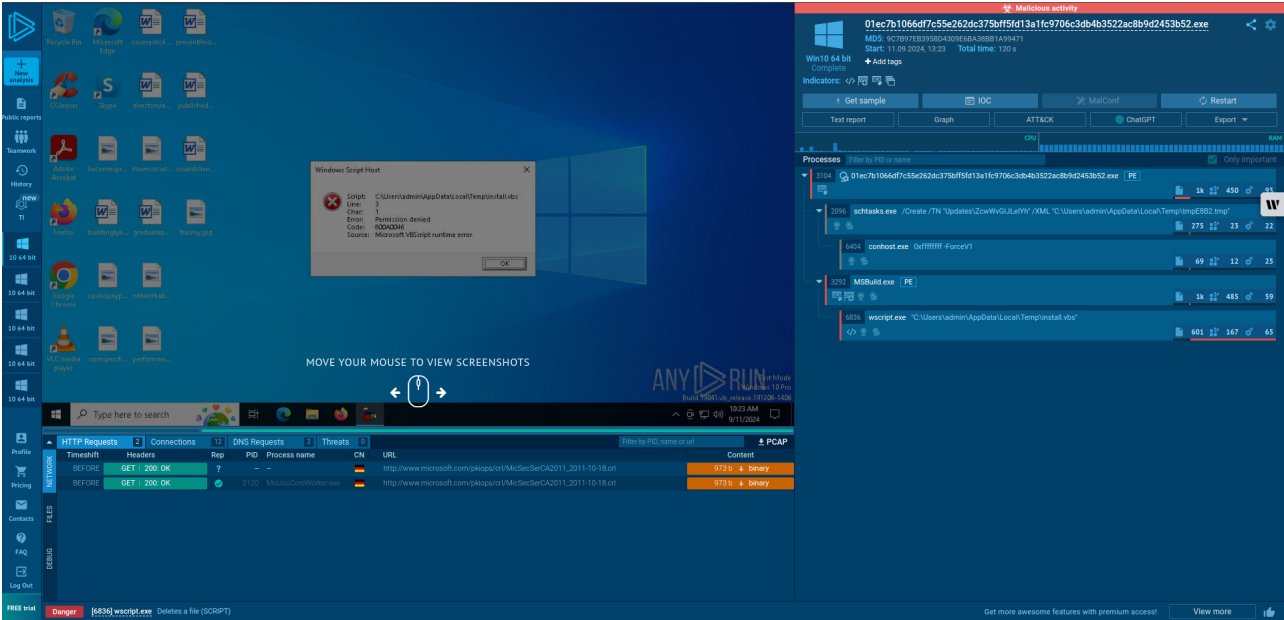
CPU 0%

RAM 36%

- processing:

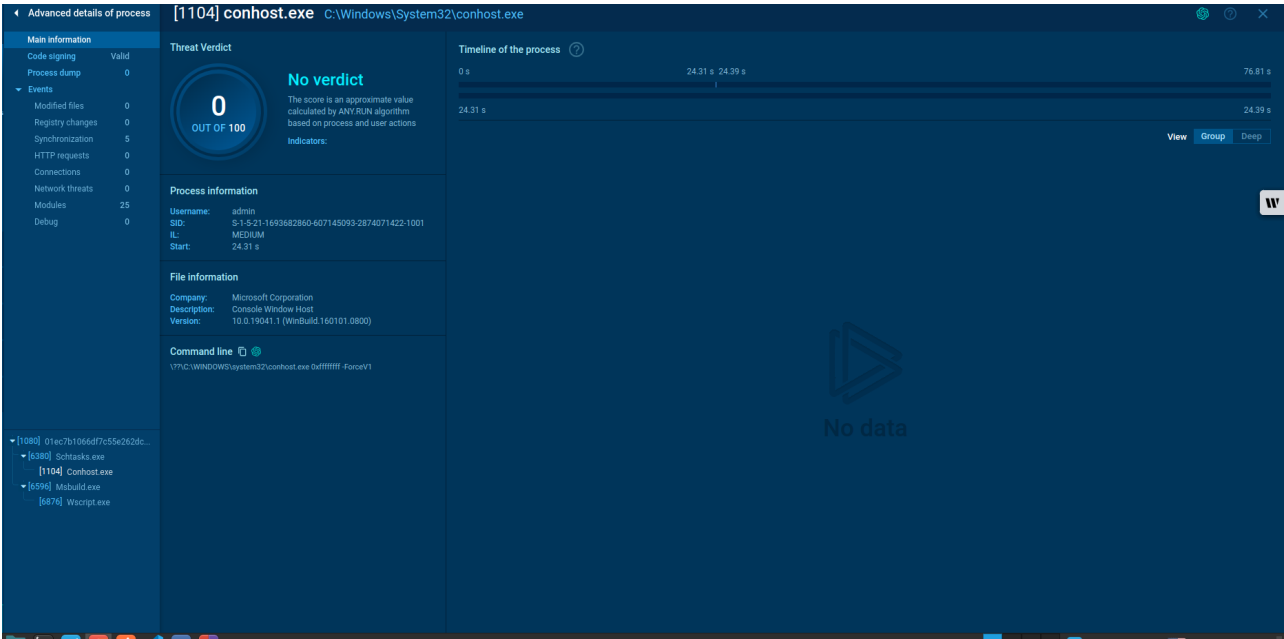
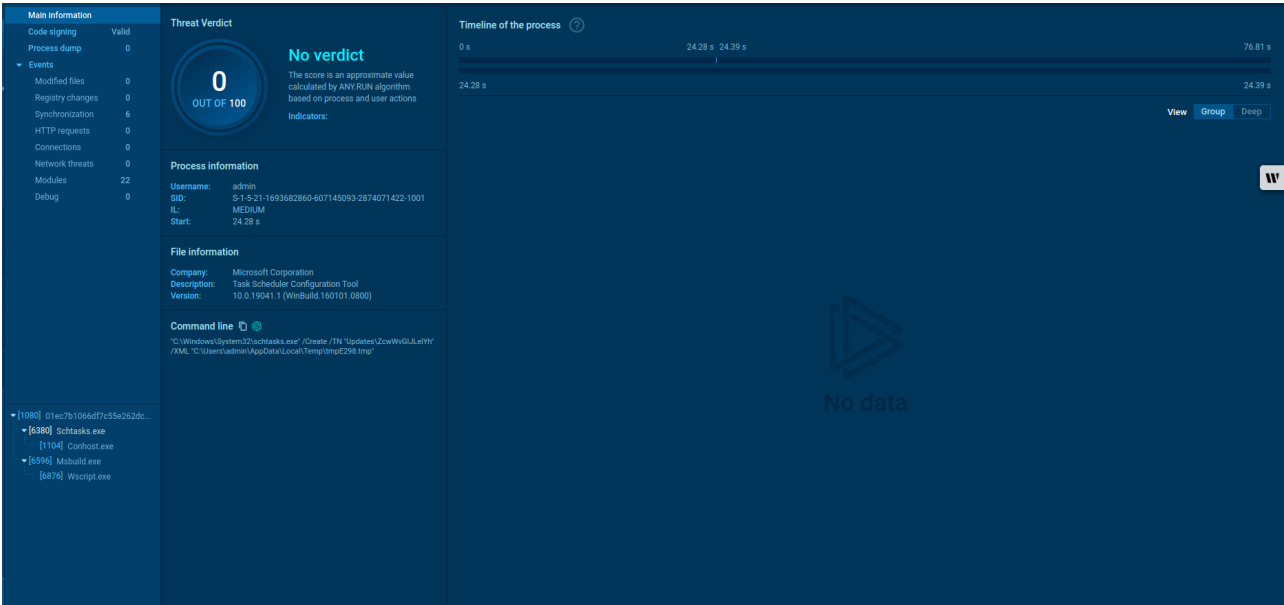


- after processing:



1. connections:

NETWORK	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
	BEFORE	GET 200: OK	✓	-	-	🇮🇹	http://www.microsoft.com/pkiops/cr/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary
	BEFORE	GET 200: OK	✓	-	-	🇮🇹	http://www.microsoft.com/pkiops/cr/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary
	BEFORE	GET 200: OK	✓	-	-	🇮🇹	http://www.microsoft.com/pkiops/cr/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary
FILES	BEFORE	TCP	✓	-	-	🇮🇹	40.127.240.158 443 settings-win.data.microsoft.com MICROSOFT-CORP-MSN-AS-BLOCK	↑ 731 B ↓ 7.64 Kb
	BEFORE	UDP	✓	4	System	🇮🇹	192.168.100.255 138 -	↑ 2.47 Kb ↓ -
	BEFORE	TCP	✓	-	-	🇮🇹	40.127.240.158 443 settings-win.data.microsoft.com MICROSOFT-CORP-MSN-AS-BLOCK	↑ 888 B ↓ 4.18 Kb
	BEFORE	TCP	✓	-	-	🇮🇹	40.127.240.158 443 settings-win.data.microsoft.com MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1.31 Kb ↓ 4.22 Kb
DEBUG	BEFORE	TCP	✓	-	-	🇮🇹	23.33.233.193 80 www.microsoft.com AKAMAI-AS	↑ 209 B ↓ 1.43 Kb
	BEFORE	TCP	✓	2120	MoUsCoreWorker.exe	🇮🇹	23.33.233.193 80 www.microsoft.com AKAMAI-AS	↑ 209 B ↓ 1.43 Kb
	BEFORE	TCP	✓	-	-	🇮🇹	23.33.233.193 80 www.microsoft.com AKAMAI-AS	↑ 209 B ↓ 1.43 Kb
	BEFORE	TCP	✓	2120	MoUsCoreWorker.exe	🇮🇹	23.33.233.193 80 www.microsoft.com AKAMAI-AS	↑ 209 B ↓ 1.43 Kb
DEBUG	BEFORE	TCP	✓	2120	svchost.exe	🇮🇹	40.127.240.158 443 settings-win.data.microsoft.com MICROSOFT-CORP-MSN-AS-BLOCK	↑ 860 B ↓ 4.22 Kb
	BEFORE	TCP	✓	2400	svchost.exe	🇮🇹	40.127.240.158 443 settings-win.data.microsoft.com MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1.66 Kb ↓ 7.80 Kb
	BEFORE	TCP	✓	2120	MoUsCoreWorker.exe	🇮🇹	40.127.240.158 443 settings-win.data.microsoft.com MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1.09 Kb ↓ 17.8 Kb
	BEFORE	TCP	✓	2120	MoUsCoreWorker.exe	🇮🇹	40.127.240.158 443 settings-win.data.microsoft.com MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1.09 Kb ↓ 17.8 Kb



- fourth process:



- fifth process it's trying to sleep to evasion detection, but we got it with increasing the time and without it:

Advanced details of process [6876] wscript.exe C:\Windows\SysWOW64\wscript.exe

Main information

- Code signing: Valid
- Process dump: 0
- Script tracer: 0
- YScript: 4
- Events: 0
- Modified files: 0
- Registry changes: 0
- Synchronization: 19
- HTTP requests: 0
- Connections: 0
- Network threats: 0
- Modules: 64
- Debug: 0

Threat Verdict

100 OUT OF 100 **Malicious**

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators: <>

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-28740371422-1001
RL: MEDIUM
Start: 24.64 s

File information

Company: Microsoft Corporation
Description: Microsoft ® Windows Based Script Host
Version: 5.812.10240.16384

Command line

"C:\WINDOWS\system32\WScript.exe" "C:\Users\admin\AppData\Local\Temp\Uninstall.vbs"

Timeline of the process

0 s 24.64 s 76.81 s

Danger 2

- T1070.004 File Deletion (1)
 - Deletes a file (SCRIPT)
- T1497.003 Time Based Evasion (1)
 - Uses sleep, probably for evasion detection (SCRIPT)

Warning 2

- Deletes system .NET executable
- Creates FileSystem object to access computer's file system (SCRIPT)

Processes

- [6876] wscript.exe
- [6380] Schtasks.exe
- [1104] Conhost.exe
- [6596] Msbuild.exe

3. I run it without more time, and I got same results. So the malware didn't have sandbox detection.

Windows Defender Security Center

01ec7b1066df7c5e262dc375bfff5d13a1fc9706c3db4b3522ac8b9d2453b52.exe

MD5: 5C7B07E2B99580A209E6A38801A99471
Start: 11/09/2024, 13:44

Win10 64 bit Complete

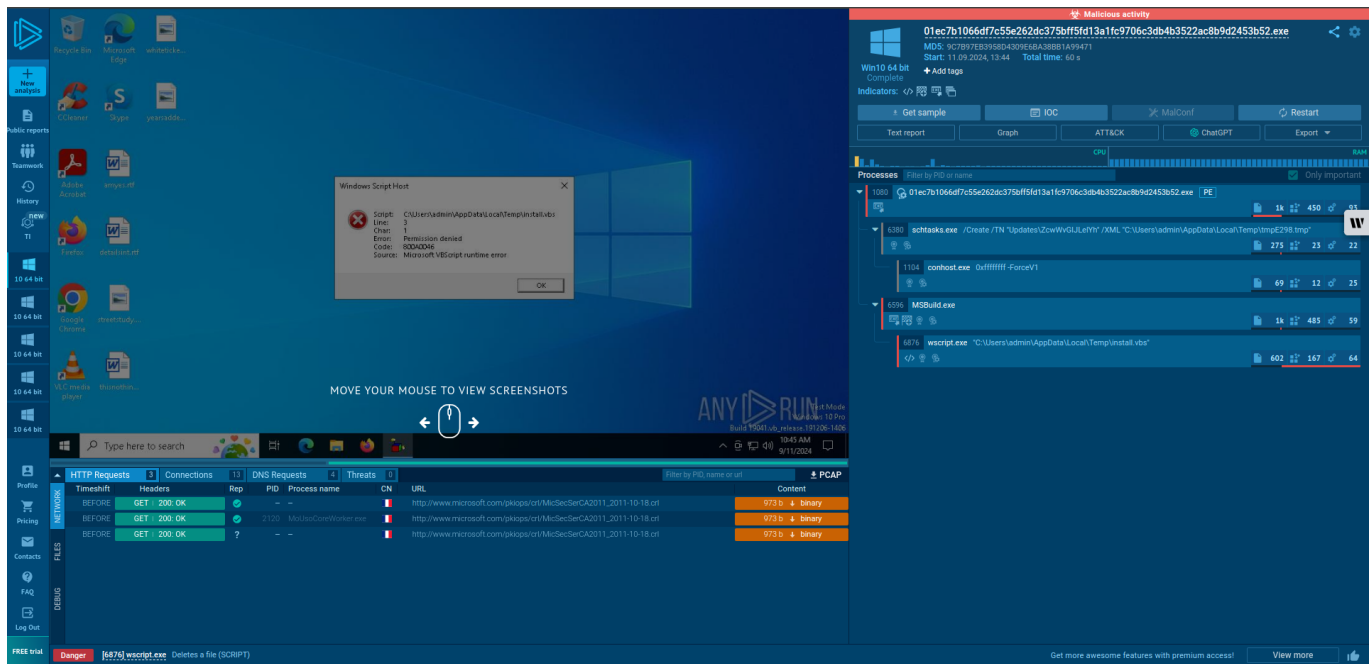
CPU 36% **RAM 38%**

Processes (Sorted by PID)

PID	Process name	Content
1080	01ec7b1066df7c5e262dc375bfff5d13a1fc9706c3db4b3522ac8b9d2453b52.exe	773 B Binary

HTTP Requests

TimeShift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET / 200 OK	✓	-	-	-	http://www.microsoft.com/pkcspec/McSecSecCA2011_10-18.txt	773 B Binary
BEFORE	GET / 200 OK	✓	-	-	-	http://www.microsoft.com/pkcspec/McSecSecCA2011_10-18.txt	773 B Binary
BEFORE	GET / 200 OK	?	-	-	-	http://www.microsoft.com/pkcspec/McSecSecCA2011_10-18.txt	773 B Binary



4. Links to reports generated by the tool:

[Any.run](#)

Without increasing the time With increasing the time

4. Remediation

- Suggest remediation actions for eradicating the malware from compromised endpoints. Include this in your malware analysis report.

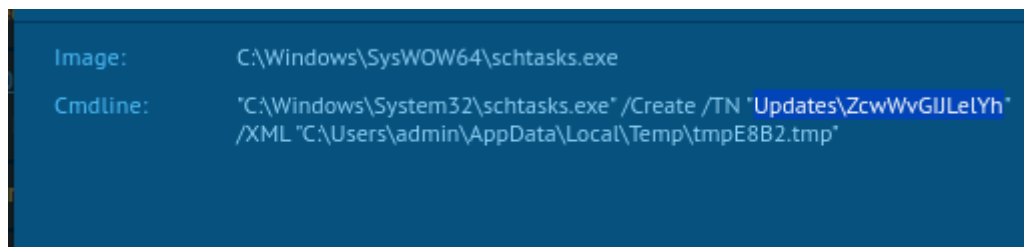
Note that generic recommendations will not be accepted. You need to suggest very specific steps that align with the results from your analysis.

For example:

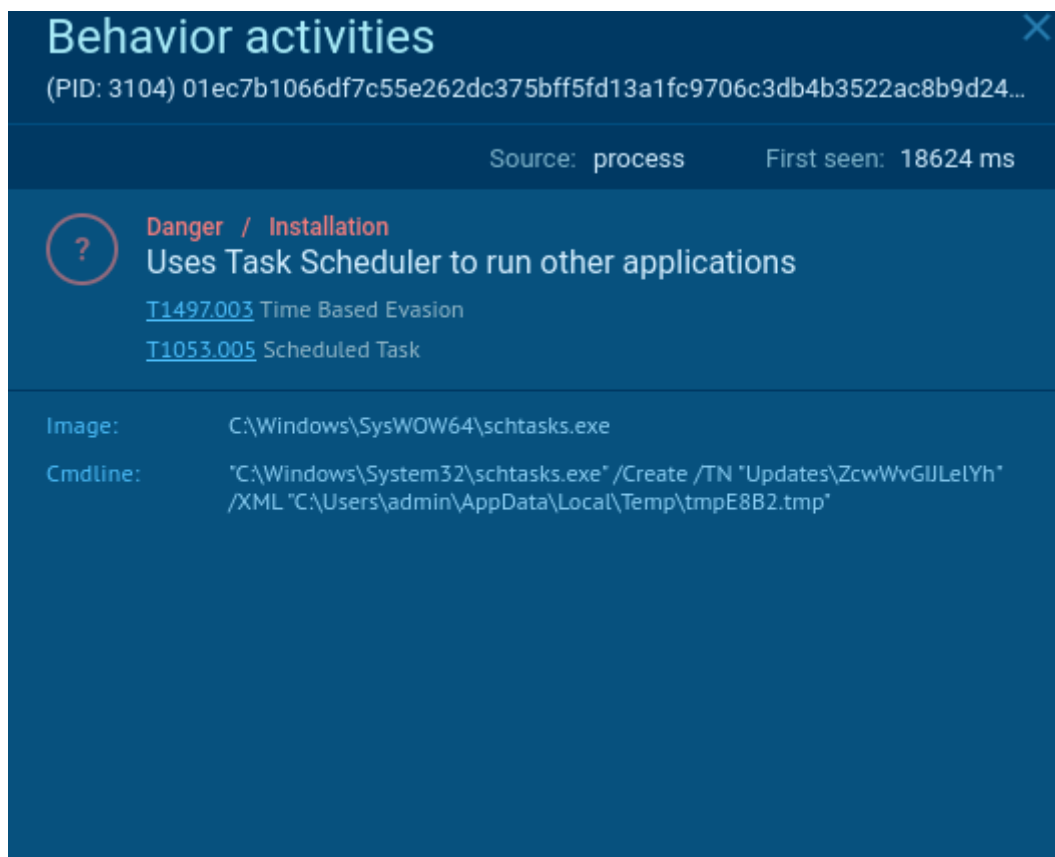
- Remove the executable dropped at C:\Program Files\dotnet\malware.exe ✓
- Remove the dropped executable ✗ Another example:
- Create a rule on the network firewall to block IP address xx.xx.xx.xx ✓
- Create a firewall rule ✗

Solution:

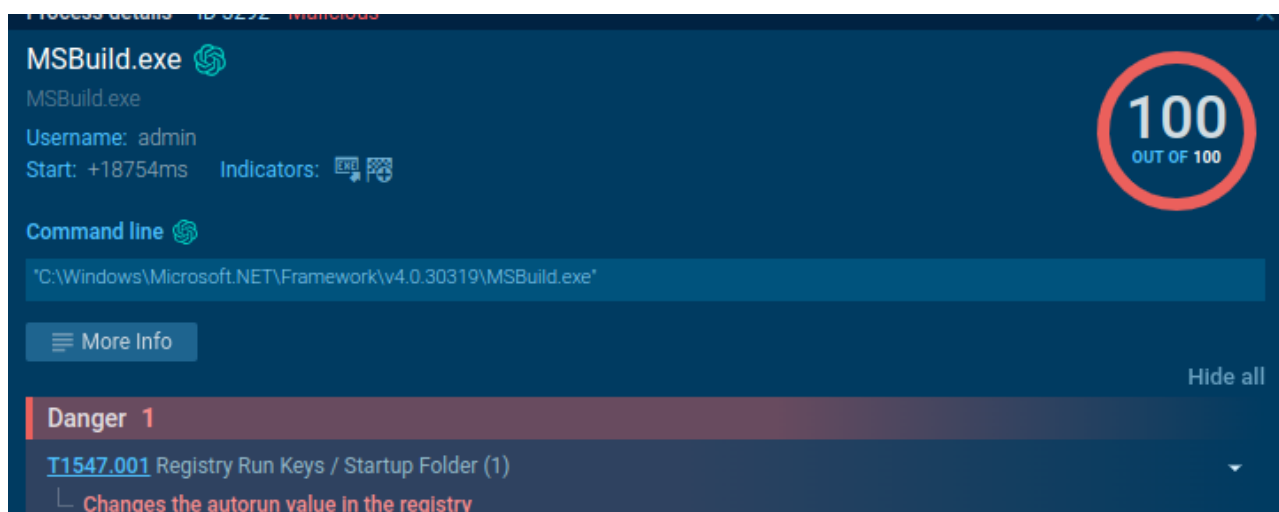
- Remove the executable dropped at
C:\Users\admin\AppData\Local\Temp\01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe
- kill this secduled task Updates\ZcwWvGIJLeYh



3. Remove the executable scheduled task C:\Windows\SysWOW64\schtasks.exe



4. Remove the executable C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe




5. restart the configuration C:\Users\admin\AppData\Roaming\vk1.exe" to its previous value or default one.

Behavior activities ✕

(PID: 3292) MSBuild.exe


Source: registry First seen: 18785 ms


Danger / Installation
Changes the autorun value in the registry
[T1547.001](#) Registry Run Keys / Startup Folder

Operation:	WRITE
Name:	VKL-X2HJ19
Value:	"C:\Users\admin\AppData\Roaming\vkLexe"
Key:	HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
TypeValue:	REG_NONE


6. Remove the script files C:\Windows\SysWOW64\wscript.exe, "C:\WINDOWS\System32\WScript.exe", "C:\Users\admin\AppData\Local\Temp\install.vbs"

Process details ID 6836 Malicious ✕

wscript.exe 

Microsoft® Windows Based Script Host

Username: admin
Start: +18960ms Indicators: </>

Command line 

































"C:\WINDOWS\System32\WScript.exe" "C:\Users\admin\AppData\Local\Temp\install.vbs"

[More Info](#)












100
OUT OF 100

[Hide all](#)

7. Create a rule on the network firewall to block IP address 40.127.240.158 which has unknwn Rep with process name: svchost.exe or null

NETWORK	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	
	BEFORE	UDP		4	System		192.168.100.255	138	-	-	
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	
FILES	BEFORE	TCP		-	-		104.107.161.181	80	www.microsoft.com	AKAMAI-AS	
	BEFORE	TCP		2120	MoUsocoreWorker.exe		104.107.161.181	80	www.microsoft.com	AKAMAI-AS	
DEBUG	BEFORE	TCP	?	6880	svchost.exe		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	
	BEFORE	UDP		3888	svchost.exe		239.255.255.250	1900	-	-	
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	
	BEFORE	UDP		3888	svchost.exe		239.255.255.250	1900	-	-	
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	
	9411 ms	TCP		6880	svchost.exe		4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	
	21722 ms	UDP		4	System		192.168.100.255	137	-	-	

8. Create a rule on the network firewall to block IP address 239.255.255.250 which has unkown CN with process name: svchost.exe or null

NETWORK	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	↑
	BEFORE	UDP	✓	4	System		192.168.100.255	138	-	-	↑
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	↑
	BEFORE	TCP	✓	-	-		104.107.161.181	80	www.microsoft.com	AKAMAI-AS	↑
	BEFORE	TCP	✓	2120	MoUsocoreWorker.exe		104.107.161.181	80	www.microsoft.com	AKAMAI-AS	↑
	BEFORE	TCP	?	6880	svchost.exe		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	↑
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	↑
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	↑
	BEFORE	UDP	✓	3888	svchost.exe		239.255.255.250	1900	-	-	↑
	BEFORE	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	↑
FILES	BEFORE	UDP	✓	4	System		192.168.100.255	137	-	-	↑ 544 b ↓ -
	9411 ms	TCP	?	-	-		40.127.240.158	443	-	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1.66 Kb ↓ 7.80 Kb
	21722 ms	TCP	✓	6880	svchost.exe		4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1.64 Kb ↓ 4.18 Kb
	21722 ms	UDP	✓	4	System		192.168.100.255	137	-	-	↑ 544 b ↓ -