Lab 3: Malware analysis

Name: Mohamad Nour Shahin

Group number: B22-CBS-01

Questions to Answer

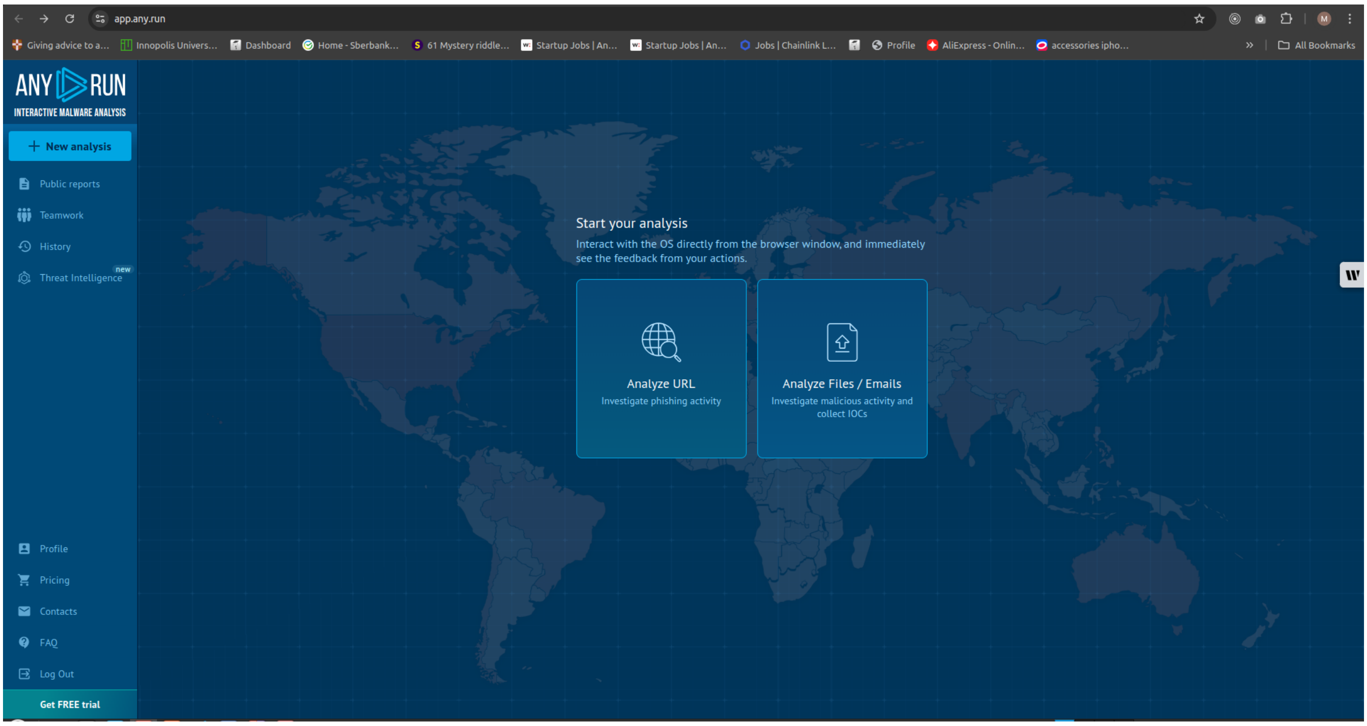
1. Preparation

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:



Start your analysis

Interact with the OS directly from the browser window, and immediately see the feedback from your actions.

2. Let's get some malware

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

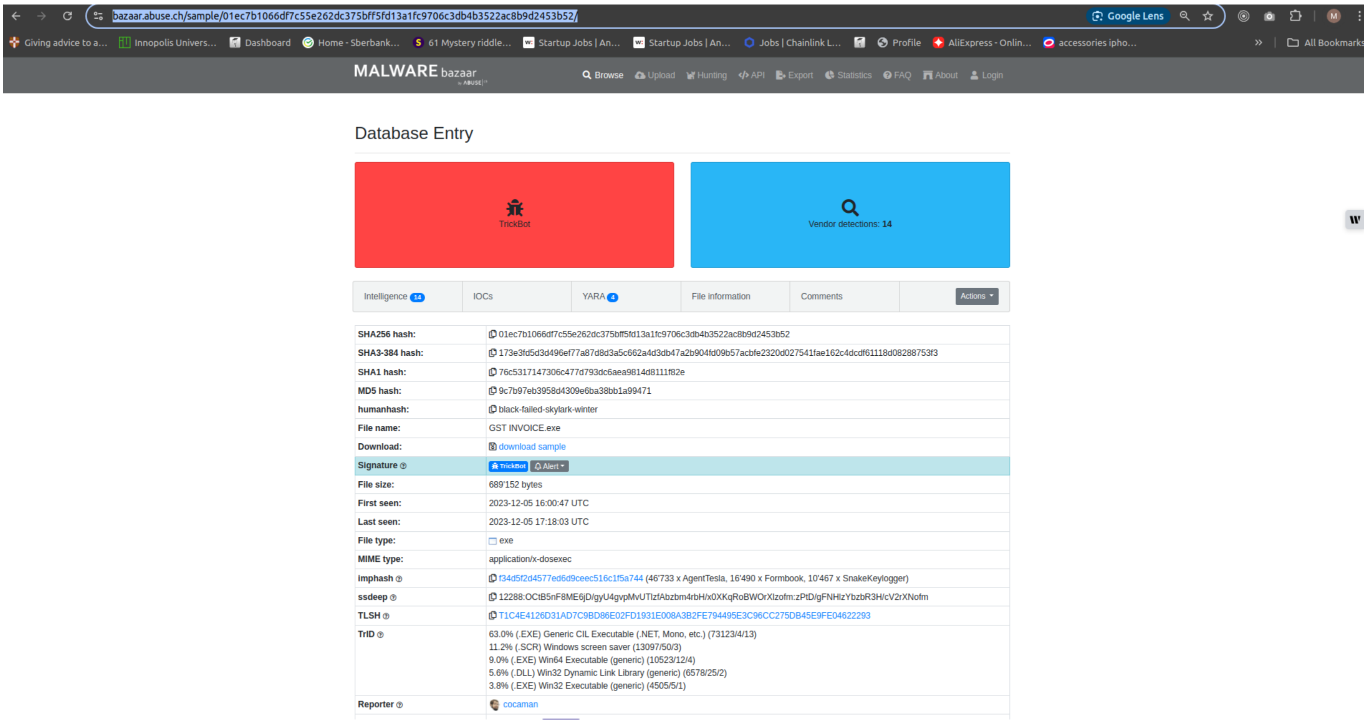
- You can download some malware/ransomware from the internet. For example TheZoo, MalwareBazaar Database. You can also check your email for any spam with malicious attachment.

- 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

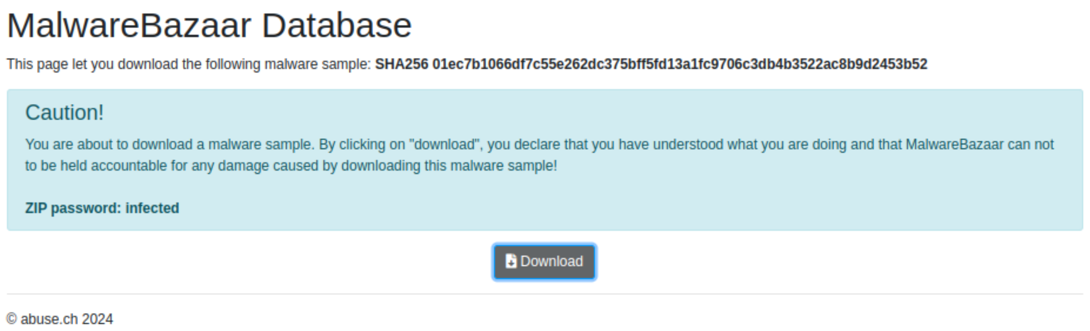


Database Entry

TrickBot

Vendor detections: **14**

SHA256 hash:	01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52
SHA3-384 hash:	173e3fd5d3d496ef77a87d8d3a5c662a4d3db47a2b904fd09b57acbfe2320d027541fae162c4dcdf61118d08288753f3
SHA1 hash:	76c5317147306c477d793dc6aea9814d8111f82e
MD5 hash:	9c7b97eb3958d4309e6ba38bb1a99471
humanhash:	black-failed-skylark-winter
File name:	GST INVOICE.exe
Download:	download sample
Signature	TrickBot Alert
File size:	689'152 bytes
First seen:	2023-12-05 16:00:47 UTC
Last seen:	2023-12-05 17:18:03 UTC
File type:	exe
MIME type:	application/x-dosexec
imphash	f34d5f2d4577ed6d9ceec516c1f5a744 (46'733 x AgentTesla, 16'490 x Formbook, 10'467 x SnakeKeylogger)
ssdeep	12288:OCtB5nF8ME6jD/gyU4gvpMvUTIzfAbzbm4rbH/x0XKqRoBWOrXIzofm:zPtD/gFNHlzYbzbR3H/cV2rXNofm
TLSH	T1C4E4126D31AD7C9BD86E02FD1931E008A3B2FE794495E3C96CC275DB45E9FE04622293
TrID	63.0% (.EXE) Generic CIL Executable (.NET, Mono, etc.) (73123/4/13) 11.2% (.SCR) Windows screen saver (13097/50/3) 9.0% (.EXE) Win64 Executable (generic) (10523/12/4) 5.6% (.DLL) Win32 Dynamic Link Library (generic) (6578/25/2) 3.8% (.EXE) Win32 Executable (generic) (4505/5/1)
Reporter	cocaman



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

© abuse.ch 2024

---

3. Sandbox analysis

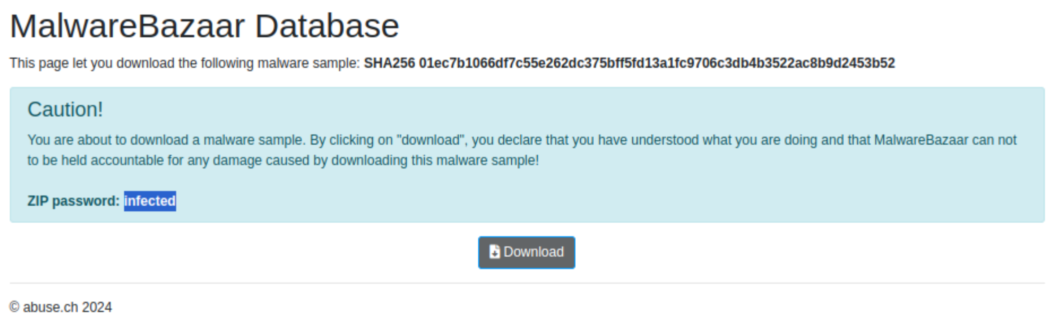
Run your malware in the sandbox.

- 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!

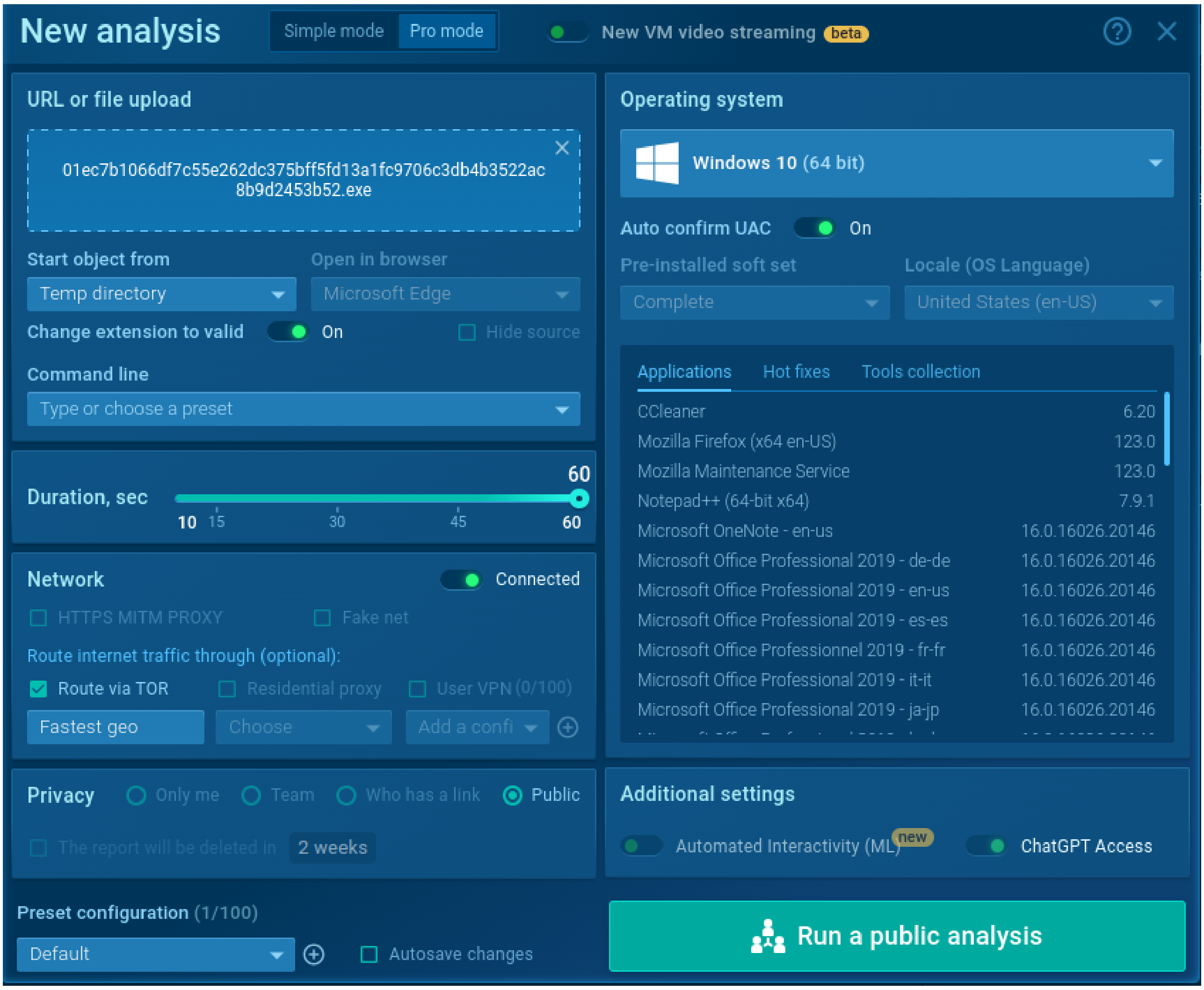
You are about to download a malware sample. By clicking on "download", you declare that you have understood what you are doing and that MalwareBazaar can not to be held accountable for any damage caused by downloading this malware sample!

ZIP password: infected

© abuse.ch 2024

- after unzip it:

01ec7b1066df7c
55e262dc375bff
5fd13a1fc9706...



New analysis

URL or file upload

01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe

Start object from: Temp directory

Open in browser: Microsoft Edge

Change extension to valid: On

□ Hide source

Command line: Type or choose a preset

Duration, sec: 60

Network: Connected

□ HTTPS MITM PROXY □ Fake net

Route internet traffic through (optional):

☑ Route via TOR □ Residential proxy □ User VPN (0/100)

Fastest geo

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)

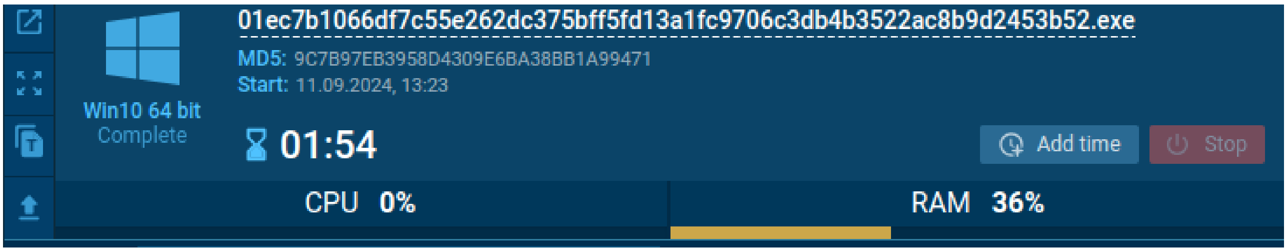
CCleaner	6.20
Mozilla Firefox (x64 en-US)	123.0
Mozilla Maintenance Service	123.0
Notepad++ (64-bit x64)	7.9.1
Microsoft OneNote - en-us	16.0.16026.20146
Microsoft Office Professional 2019 - de-de	16.0.16026.20146
Microsoft Office Professional 2019 - en-us	16.0.16026.20146
Microsoft Office Professional 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: Off

ChatGPT Access: On

- we add more time for analyzing.



01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe

MD5: 9C7B97EB3958D4309E6BA38BB1A99471

Start: 11.09.2024, 13:23

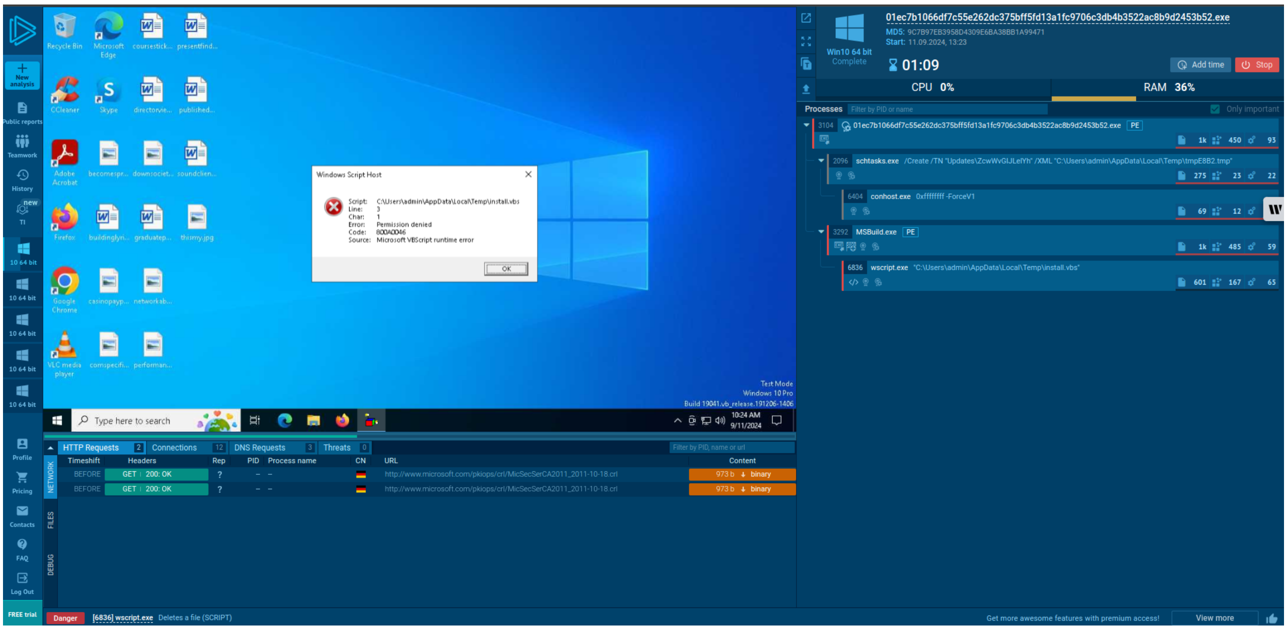
Win10 64 bit
Complete

01:54

CPU 0%

RAM 36%

- proccessing:



01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe
MD5: 9C7B97EB3958D4309E6BA38BB1A99471
Start: 11.09.2024, 13:23
Win10 64 bit Complete
01:09
CPU 0% RAM 36%

Windows Script Host

```
Script:   C:\Users\admin\AppData\Local\Temp\install.vbs
Line:     3
Char:     1
Error:    Permission denied
Code:     800A0046
Source:   Microsoft VBScript runtime error
```

Processes

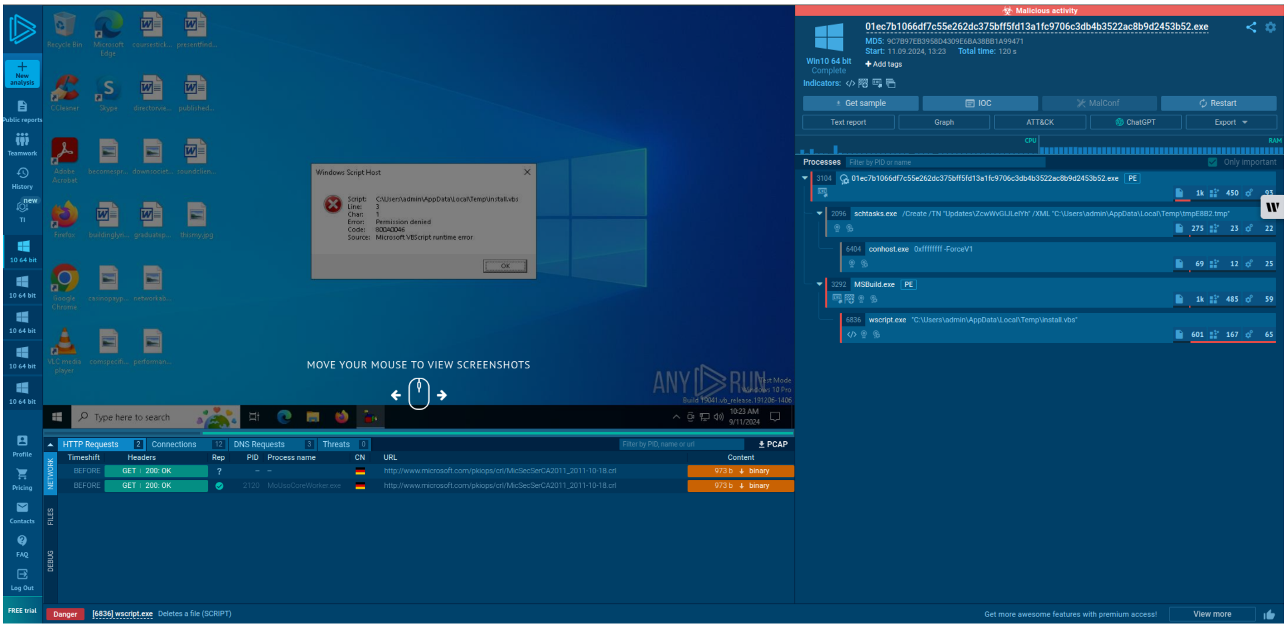
```
3104 01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe PE       1k  450  93
  2096 schtasks.exe /Create /TN "Updates\ZcwWvGIJLeIYh" /XML "C:\Users\admin\AppData\Local\Temp\tmpE8B2.tmp"   275  23  22
    6404 conhost.exe 0xffffffff -ForceV1                                         69  12
  3292 MSBuild.exe PE                                                            1k  485  59
    6836 wscript.exe "C:\Users\admin\AppData\Local\Temp\install.vbs"             601  167  65
```

HTTP Requests 2 | Connections 12 | DNS Requests 3 | Threats 0

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	?	–	–	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
BEFORE	GET 200: OK	?	–	–	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary

Danger [6836] wscript.exe Deletes a file (SCRIPT)

- after processing:



Malicious activity

01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe
MD5: 9C7B97EB3958D4309E6BA38BB1A99471
Start: 11.09.2024, 13:23 Total time: 120 s
Win10 64 bit Complete

Processes

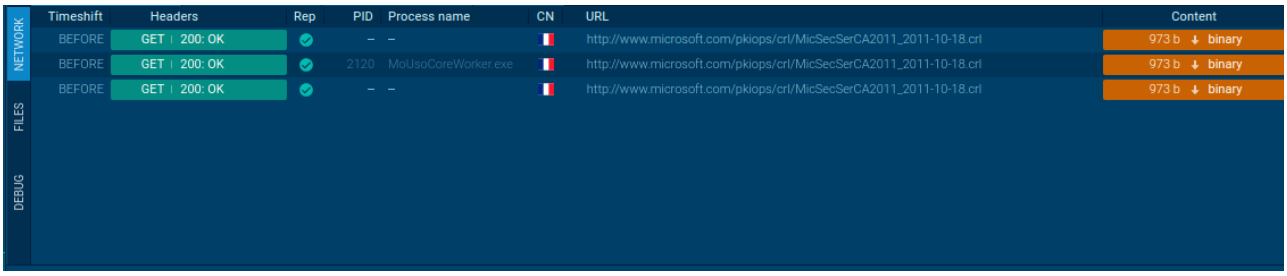
```
3104 01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe PE       1k  450  93
  2096 schtasks.exe /Create /TN "Updates\ZcwWvGIJLeIYh" /XML "C:\Users\admin\AppData\Local\Temp\tmpE8B2.tmp"   275  23  22
    6404 conhost.exe 0xffffffff -ForceV1                                         69  12  25
  3292 MSBuild.exe PE                                                            1k  485  59
    6836 wscript.exe "C:\Users\admin\AppData\Local\Temp\install.vbs"             601  167  65
```

HTTP Requests 2 | Connections 12 | DNS Requests 3 | Threats 0

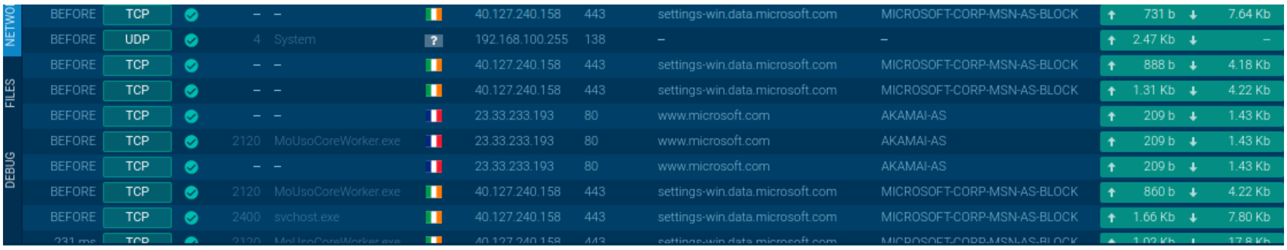
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	?	–	–	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
BEFORE	GET 200: OK	✓	2120	MoUsoCoreWorker.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary

Danger [6836] wscript.exe Deletes a file (SCRIPT)

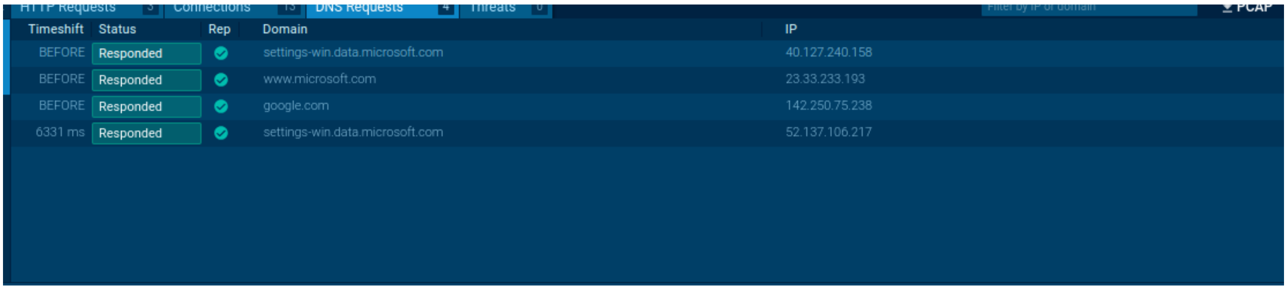
1. connections:



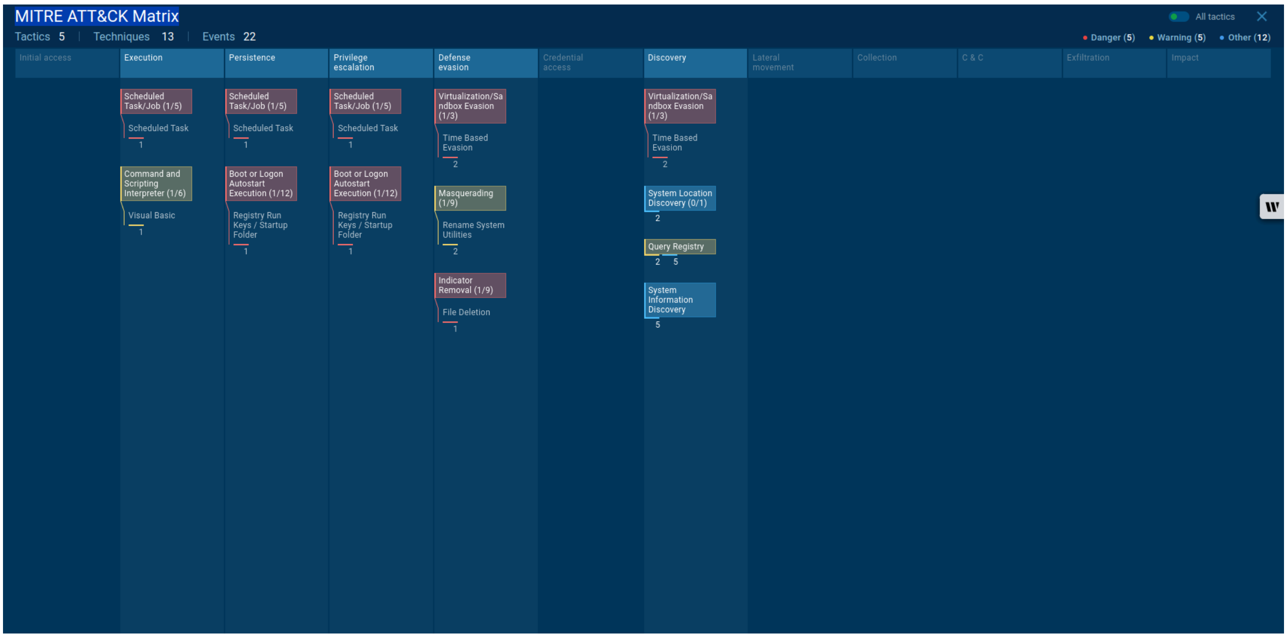
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	–	–	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
BEFORE	GET 200: OK	✓	2120	MoUsoCoreWorker.exe	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
BEFORE	GET 200: OK	✓	–	–	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary



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
BEFORE	TCP	✓	–	–	🇫🇷	23.33.233.193	80	www.microsoft.com	AKAMAI-AS	↑ 209 b	↓ 1.43 Kb
BEFORE	TCP	✓	2120	MoUsoCoreWorker.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	MoUsoCoreWorker.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
231 ms	TCP	✓	2120	MoUsoCoreWorker.exe	🇮🇪	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1.02 Kb	↓ 17.8 Kb



Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	40.127.240.158
BEFORE	Responded	✓	www.microsoft.com	23.33.233.193
BEFORE	Responded	✓	google.com	142.250.75.238
6331 ms	Responded	✓	settings-win.data.microsoft.com	52.137.106.217



MITRE ATT&CK Matrix

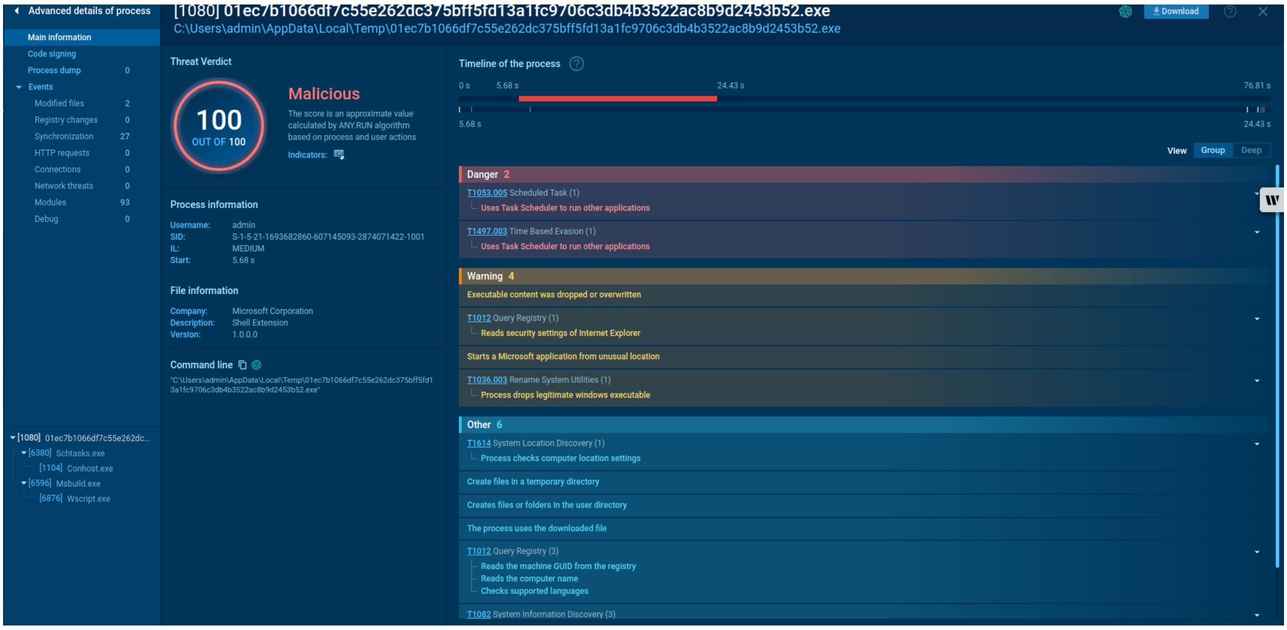
Tactics 5 | Techniques 13 | Events 22

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
	Scheduled Task/Job (1/5) Scheduled Task 1	Scheduled Task/Job (1/5) Scheduled Task 1	Scheduled Task/Job (1/5) Scheduled Task 1	Virtualization/Sandbox Evasion (1/3) Time Based Evasion 2		Virtualization/Sandbox Evasion (1/3) Time Based Evasion 2					
	Command and Scripting Interpreter (1/6) Visual Basic 1	Boot or Logon Autostart Execution (1/12) Registry Run Keys / Startup Folder 1	Boot or Logon Autostart Execution (1/12) Registry Run Keys / Startup Folder 1	Masquerading (1/9) Rename System Utilities 2		System Location Discovery (0/1) 2					
				Indicator Removal (1/9) File Deletion 1		Query Registry 2 5					
						System Information Discovery 5					

---

2. while monitoring the process:

- first process:



[1080] 01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe
C:\Users\admin\AppData\Local\Temp\01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe

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-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 5.68 s

File information

Company: Microsoft Corporation
Description: Shell Extension
Version: 1.0.0.0

Command line

"C:\Users\admin\AppData\Local\Temp\01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe"

```
[1080] 01ec7b1066df7c55e262dc...
  [6380] Schtasks.exe
    [1104] Conhost.exe
  [6596] Msbuild.exe
    [6876] Wscript.exe
```

Timeline of the process

0 s 5.68 s 24.43 s 76.81 s
5.68 s 24.43 s

Danger 2

T1053.005 Scheduled Task (1)
└ Uses Task Scheduler to run other applications

T1497.003 Time Based Evasion (1)
└ Uses Task Scheduler to run other applications

Warning 4

Executable content was dropped or overwritten

T1012 Query Registry (1)
└ Reads security settings of Internet Explorer

Starts a Microsoft application from unusual location

T1036.003 Rename System Utilities (1)
└ Process drops legitimate windows executable

Other 6

T1614 System Location Discovery (1)
└ Process checks computer location settings

Create files in a temporary directory

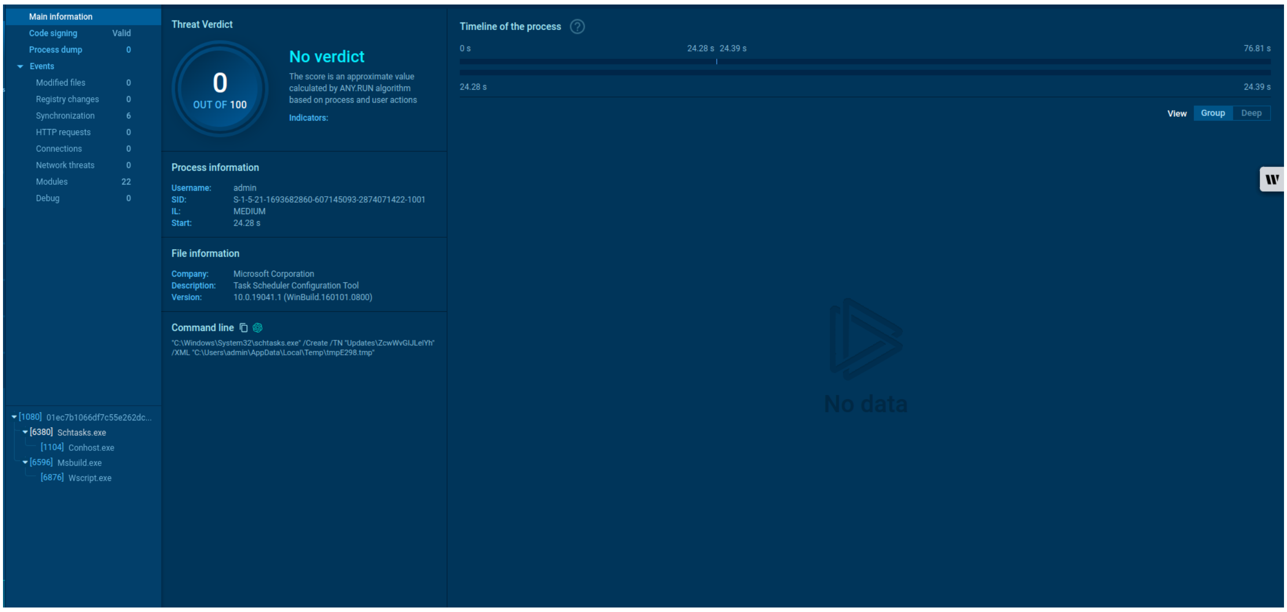
Creates files or folders in the user directory

The process uses the downloaded file

T1012 Query Registry (3)
├ Reads the machine GUID from the registry
├ Reads the computer name
└ Checks supported languages

T1082 System Information Discovery (3)

- second and third process:



Main information

Code signing Valid

Process dump 0

Events

Modified files 0

Registry changes 0

Synchronization 6

HTTP requests 0

Connections 0

Network threats 0

Modules 22

Debug 0

Threat Verdict

0 OUT OF 100

No verdict

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

Indicators:

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 24.28 s

File information

Company: Microsoft Corporation
Description: Task Scheduler Configuration Tool
Version: 10.0.19041.1 (WinBuild.160101.0800)

Command line

```
"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZcwWvGIJLeIYh"
/XML "C:\Users\admin\AppData\Local\Temp\tmpE298.tmp"
```

Timeline of the process

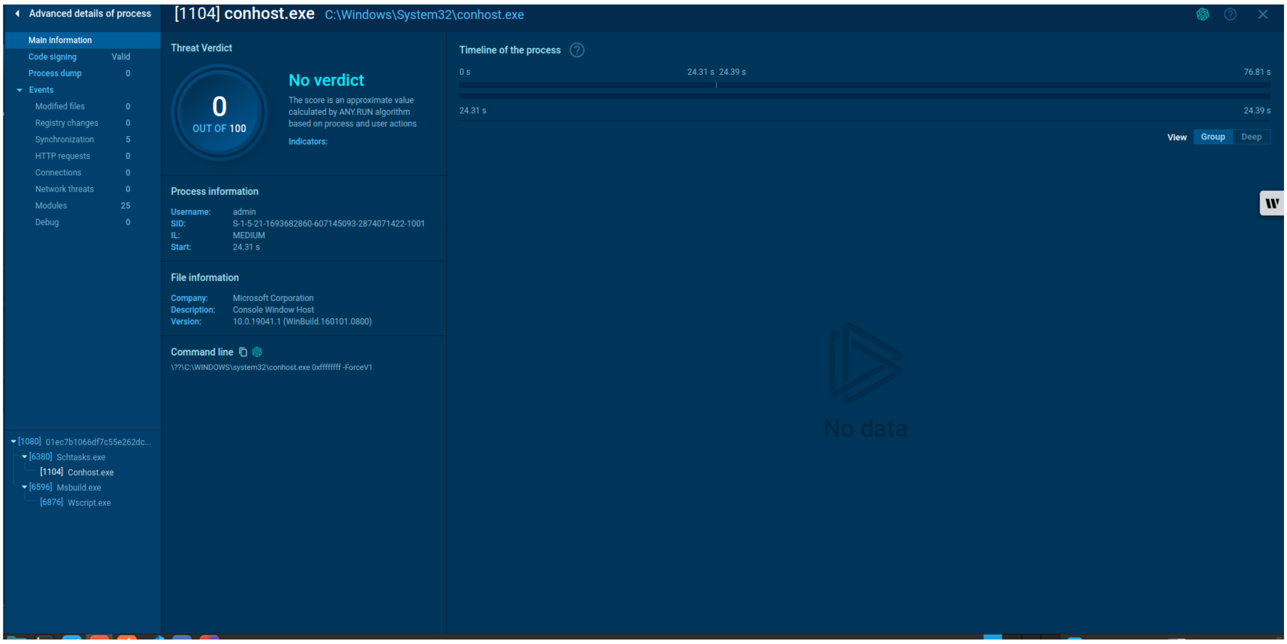
0 s 24.28 s 24.39 s 76.81 s

24.28 s 24.39 s

View Group Deep

No data

```
[1080] 01ec7b1066df7c55e262dc...
  [6380] Schtasks.exe
    [1104] Conhost.exe
  [6596] Msbuild.exe
    [6876] Wscript.exe
```



Advanced details of process

[1104] conhost.exe C:\Windows\System32\conhost.exe

Main information

Code signing Valid

Process dump 0

Events

Modified files 0

Registry changes 0

Synchronization 5

HTTP requests 0

Connections 0

Network threats 0

Modules 25

Debug 0

Threat Verdict

0 OUT OF 100

No verdict

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

Indicators:

Process information

Username: admin
SID: S-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 24.31 s

File information

Company: Microsoft Corporation
Description: Console Window Host
Version: 10.0.19041.1 (WinBuild.160101.0800)

Command line

```
\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
```

Timeline of the process

0 s 24.31 s 24.39 s 76.81 s

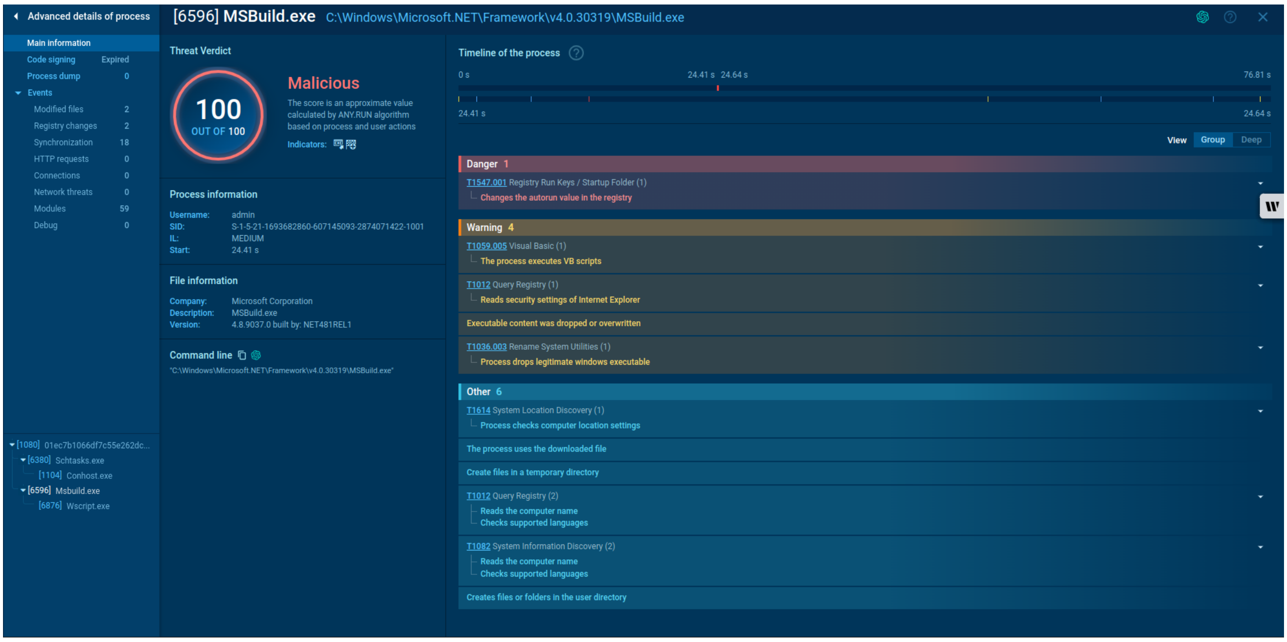
24.31 s 24.39 s

View Group Deep

No data

```
[1080] 01ec7b1066df7c55e262dc...
  [6380] Schtasks.exe
    [1104] Conhost.exe
  [6596] Msbuild.exe
    [6876] Wscript.exe
```

- fourth process:



Advanced details of process

[6596] MSBuild.exe C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Main information

Code signing Expired

Process dump 0

Events

Modified files 2

Registry changes 2

Synchronization 18

HTTP requests 0

Connections 0

Network threats 0

Modules 59

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-1-5-21-1693682860-607145093-2874071422-1001
IL: MEDIUM
Start: 24.41 s

File information

Company: Microsoft Corporation
Description: MSBuild.exe
Version: 4.8.9037.0 built by: NET481REL1

Command line

```
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"
```

Timeline of the process

0 s 24.41 s 24.64 s 76.81 s

24.41 s 24.64 s

View Group Deep

Danger 1

T1547.001 Registry Run Keys / Startup Folder (1)
└ Changes the autorun value in the registry

Warning 4

T1059.005 Visual Basic (1)
└ The process executes VB scripts

T1012 Query Registry (1)
└ Reads security settings of Internet Explorer

Executable content was dropped or overwritten

T1036.003 Rename System Utilities (1)
└ Process drops legitimate windows executable

Other 6

T1614 System Location Discovery (1)
└ Process checks computer location settings

The process uses the downloaded file

Create files in a temporary directory

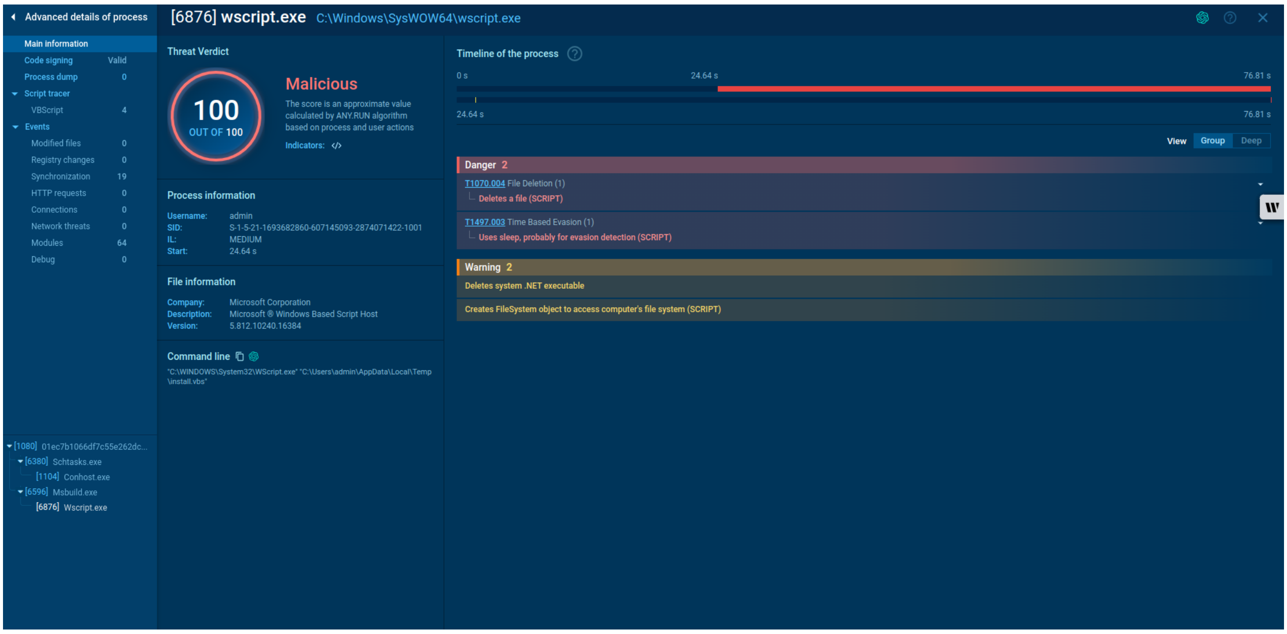
T1012 Query Registry (2)
├ Reads the computer name
└ Checks supported languages

T1082 System Information Discovery (2)
├ Reads the computer name
└ Checks supported languages

Creates files or folders in the user directory

```
[1080] 01ec7b1066df7c55e262dc...
  [6380] Schtasks.exe
    [1104] Conhost.exe
  [6596] Msbuild.exe
    [6876] Wscript.exe
```

- 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	
VBScript	4
Events	
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-1-5-21-1693682860-607145093-2874071422-1001
IL: 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\install.vbs"
```

```
[1080] 01ec7b1066df7c55e262dc...
  [6380] Schtasks.exe
    [1104] Conhost.exe
  [6596] Msbuild.exe
    [6876] Wscript.exe
```

Timeline of the process

Danger 2

T1070.004 File Deletion (1)
└ Deletes a file (SCRIPT)

T1497.003 Time Based Evasion (1)
└ Uses sleep, probably for evasion detection (SCRIPT)

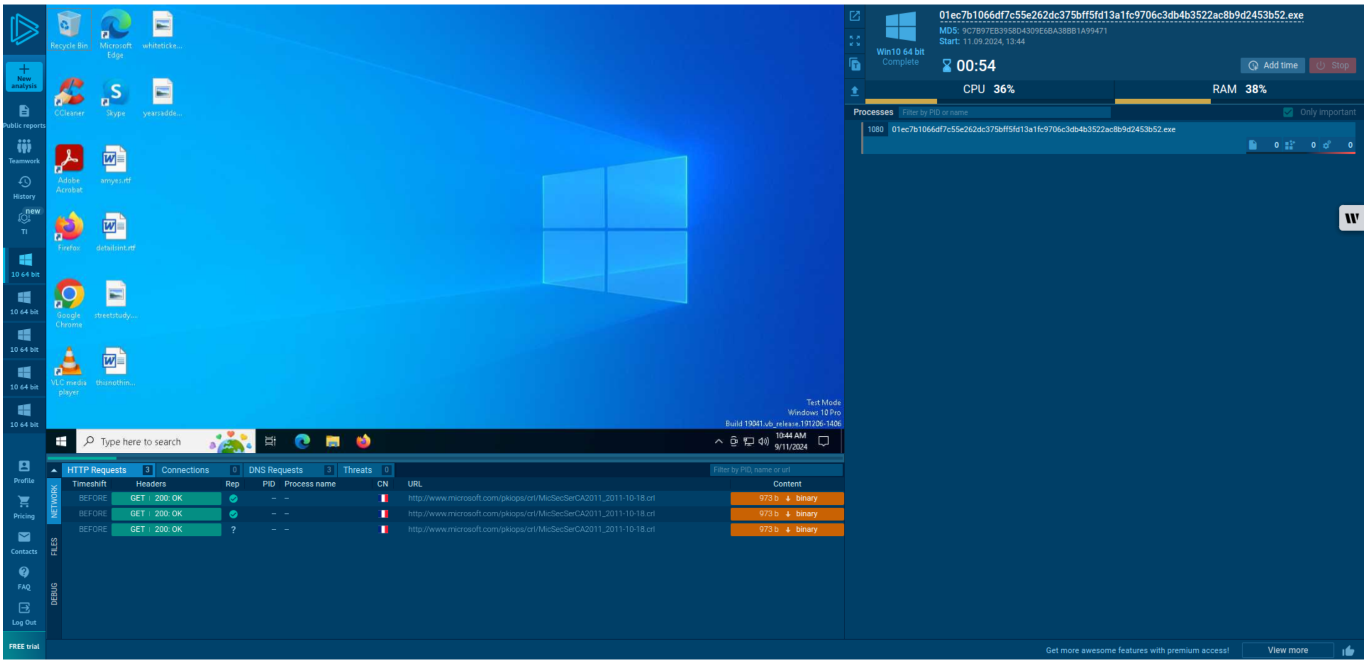
Warning 2

Deletes system .NET executable

Creates FileSystem object to access computer's file system (SCRIPT)

---

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



Test Mode
Windows 10 Pro
Build 19041.vb_release.191206-1406

10:44 AM
9/11/2024

01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe
MD5: 9C7B97EB3958D4309E6BA38BB1A99471
Start: 11.09.2024, 13:44

Win10 64 bit
Complete

00:54

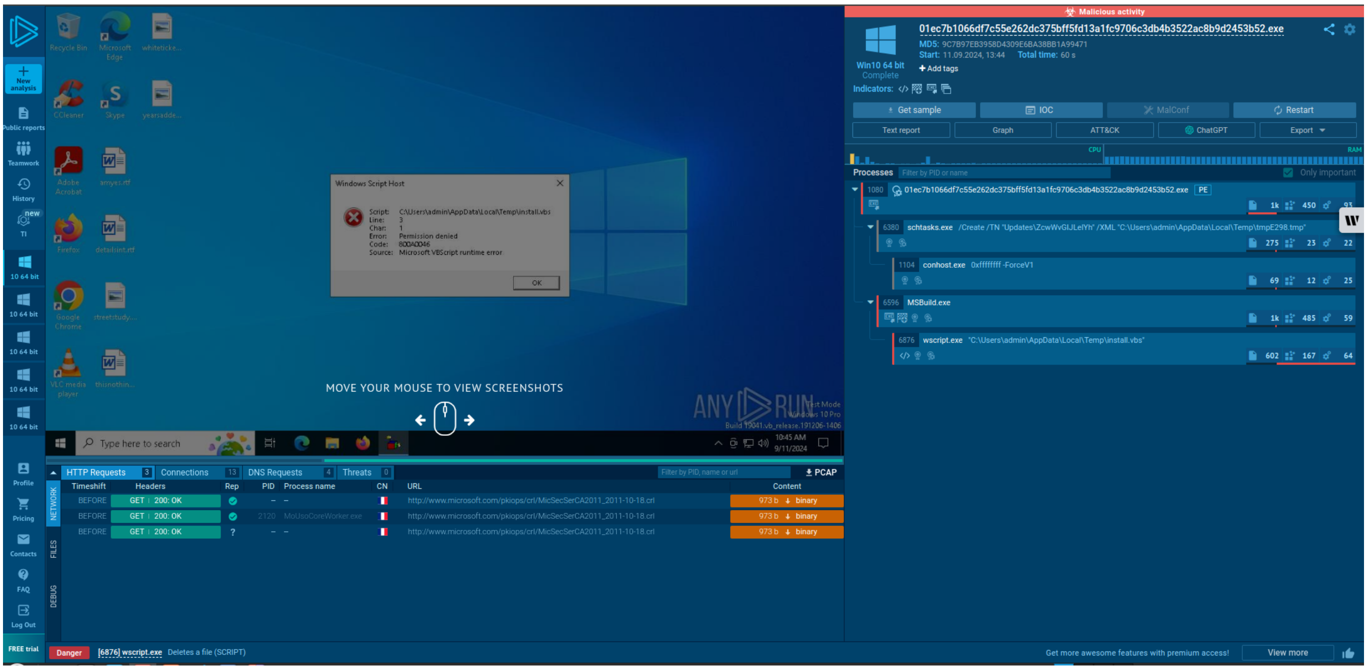
CPU 36%   RAM 38%

Processes   Filter by PID or name   ☑ Only important

1080 01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe   0 0 0

HTTP Requests 3   Connections 0   DNS Requests 3   Threats 0   Filter by PID, name or url

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	–	–	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary
BEFORE	GET 200: OK	✓	–	–	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary
BEFORE	GET 200: OK	?	–	–	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b ↓ binary



Malicious activity

01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe

MD5: 9C7B97EB3958D4309E6BA38BB1A99471

Start: 11.09.2024, 13:44 Total time: 60 s

Win10 64 bit Complete

```
1080  01ec7b1066df7c55e262dc375bff5fd13a1fc9706c3db4b3522ac8b9d2453b52.exe  PE     1k  450  93
  6380  schtasks.exe  /Create /TN "Updates\ZcwWvGIJLelYh" /XML "C:\Users\admin\AppData\Local\Temp\tmpE298.tmp"   275  23  22
    1104  conhost.exe  0xffffffff -ForceV1                                            69  12  25
  6596  MSBuild.exe                                                                   1k  485  59
    6876  wscript.exe  "C:\Users\admin\AppData\Local\Temp\install.vbs"                 602  167  64
```

Windows Script Host

```
Script:   C:\Users\admin\AppData\Local\Temp\install.vbs
Line:     3
Char:     1
Error:    Permission denied
Code:     800A0046
Source:   Microsoft VBScript runtime error
```

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	–	–	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
BEFORE	GET 200: OK	✓	2120	MoUsoCoreWorker.exe	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
BEFORE	GET 200: OK	?	–	–	🇫🇷	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary

Danger [6876] wscript.exe Deletes a file (SCRIPT)

---

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.

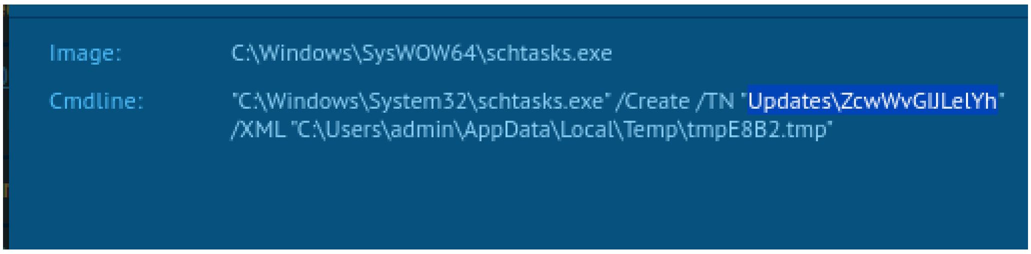
> Note that generic recommendations will not be accepted. You need to suggest very specific steps that align with the results from your analysis.

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 ❌

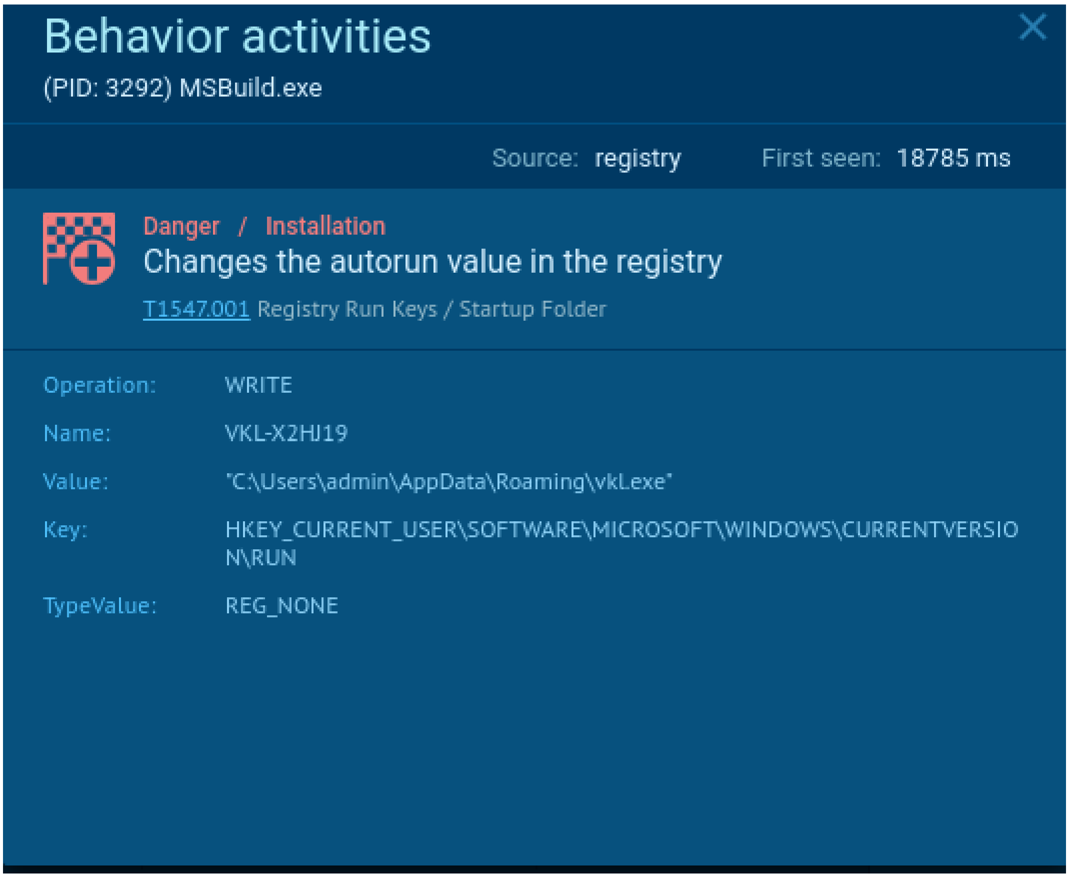
Solution:

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



```
Image:      C:\Windows\SysWOW64\schtasks.exe
Cmdline:    "C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZcwWvGIJLelYh"
            /XML "C:\Users\admin\AppData\Local\Temp\tmpE8B2.tmp"
```

3. restart the configuration C:\Users\admin\AppData\Roaming\vkl.exe" to its previous value or defualt one.



Behavior activities

(PID: 3292) MSBuild.exe

Source: registry First seen: 18785 ms

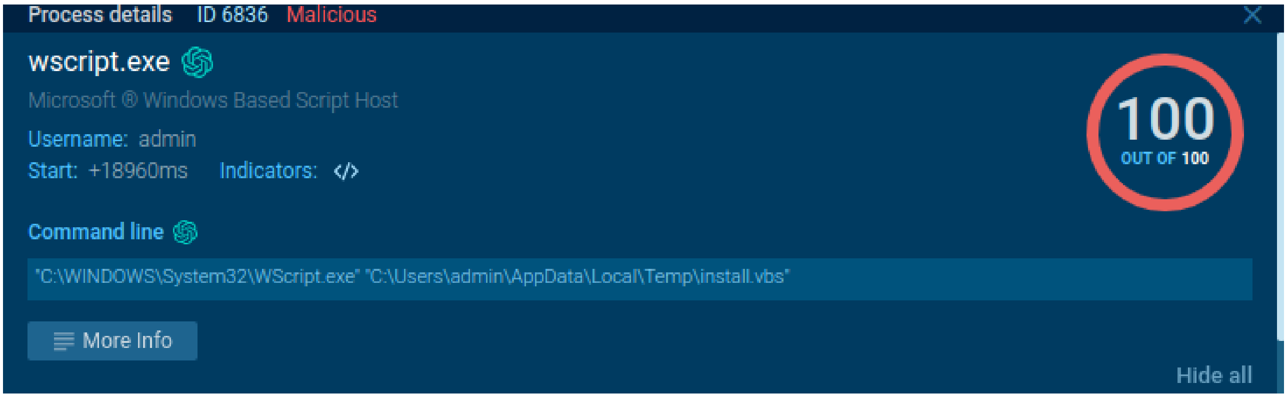
Danger / Installation

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\vkl.exe"
Key:        HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSIO
            N\RUN
TypeValue:  REG_NONE
```

4. Remove the script files "C:\Users\admin\AppData\Local\Temp\install.vbs"



Process details ID 6836 Malicious

wscript.exe

Microsoft ® Windows Based Script Host

Username: admin

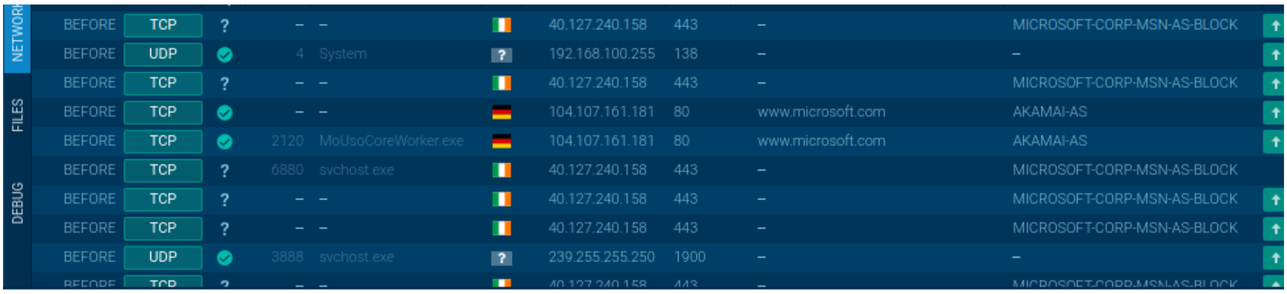
Start: +18960ms Indicators: </>

100 OUT OF 100

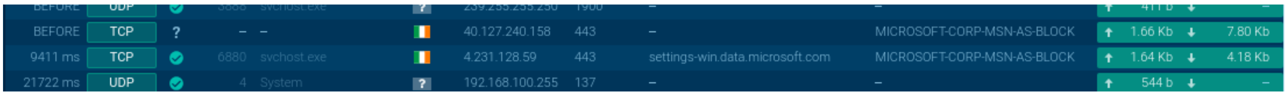
Command line

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

5. Create a rule on the network firewall to block IP address 40.127.240.158 which has unkown Rep with proccess name: svchost.exe or null

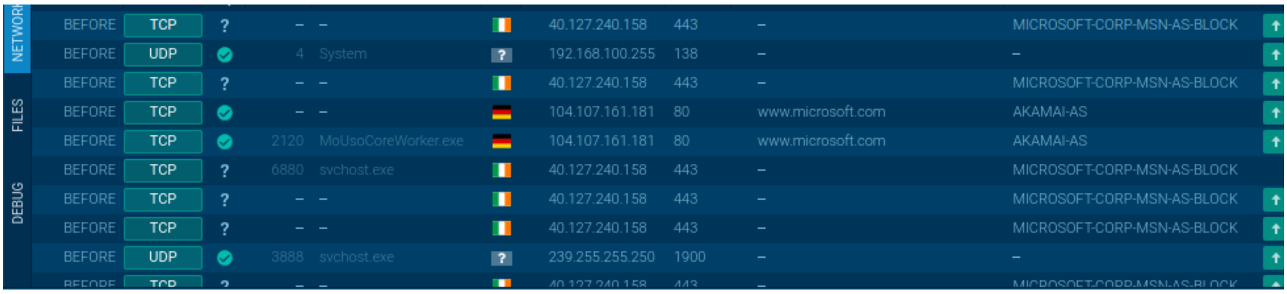


BEFORE	TCP	?	–	–		40.127.240.158	443	–	MICROSOFT-CORP-MSN-AS-BLOCK	↑
BEFORE	UDP	✓	4	System	?	192.168.100.255	138	–	–	↑
BEFORE	TCP	?	–	–		40.127.240.158	443	–	MICROSOFT-CORP-MSN-AS-BLOCK	↑
BEFORE	TCP	✓	–	–		104.107.161.181	80	www.microsoft.com	AKAMAI-AS	↑
BEFORE	TCP	✓	2120	MoUsoCoreWorker.exe		104.107.161.181	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	↑

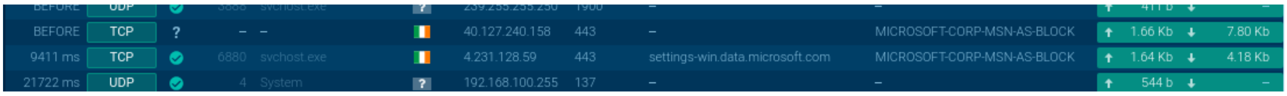


BEFORE	UDP	✓	3888	svchost.exe	?	239.255.255.250	1900	–	–	↑	411 b ↓	–
BEFORE	TCP	?	–	–		40.127.240.158	443	–	MICROSOFT-CORP-MSN-AS-BLOCK	↑	1.66 Kb ↓	7.80 Kb
9411 ms	TCP	✓	6880	svchost.exe		4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑	1.64 Kb ↓	4.18 Kb
21722 ms	UDP	✓	4	System	?	192.168.100.255	137	–	–	↑	544 b ↓	–

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



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	↑



BEFORE	UDP	✓	3888	svchost.exe	?	239.255.255.250	1900	–	–	↑	411 b ↓	–
BEFORE	TCP	?	–	–		40.127.240.158	443	–	MICROSOFT-CORP-MSN-AS-BLOCK	↑	1.66 Kb ↓	7.80 Kb
9411 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 ↓	–