VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

FACULTY OF FUNDAMENTAL SCIENCES

DEPARTMENT OF INFORMATION SYSTEMS

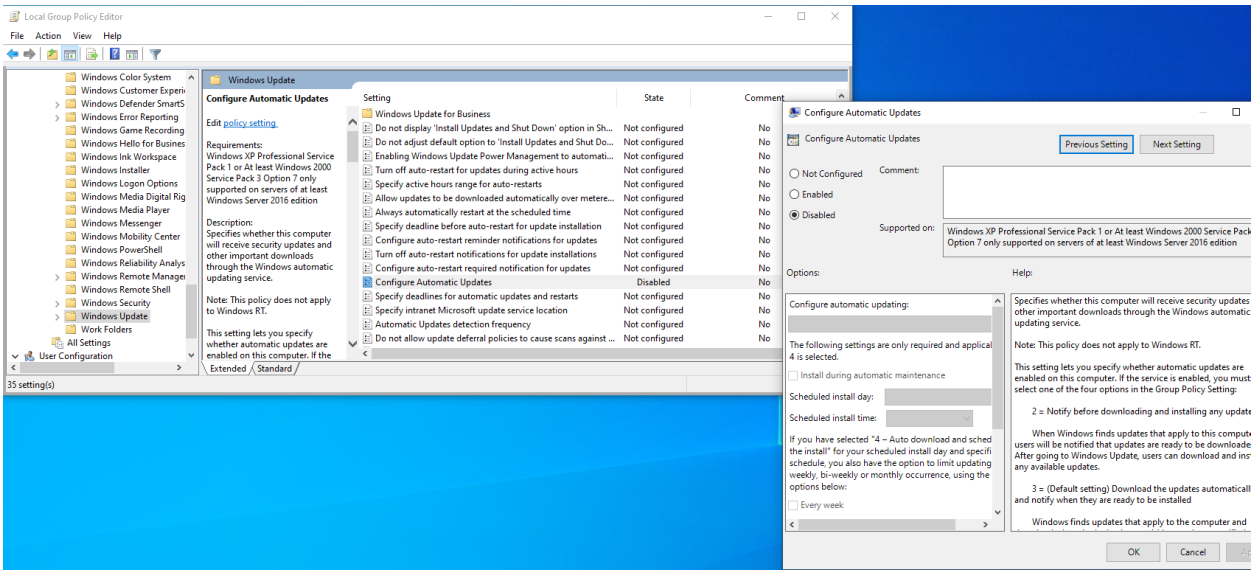
STATIC MALWARE ANALYSIS

Prepared by: Simonas Riška

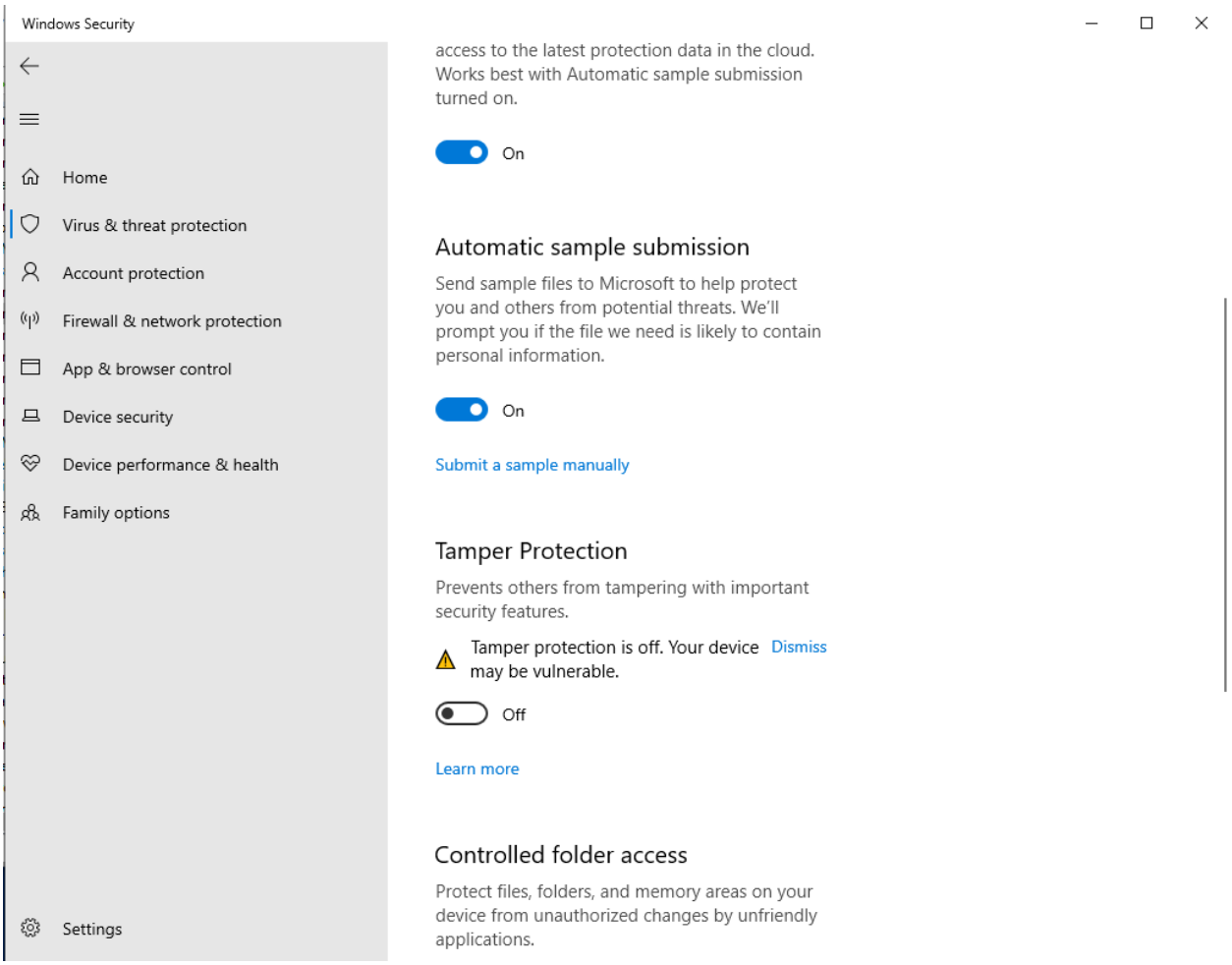
Checked by: lect. [redacted]

VILNIUS 2025

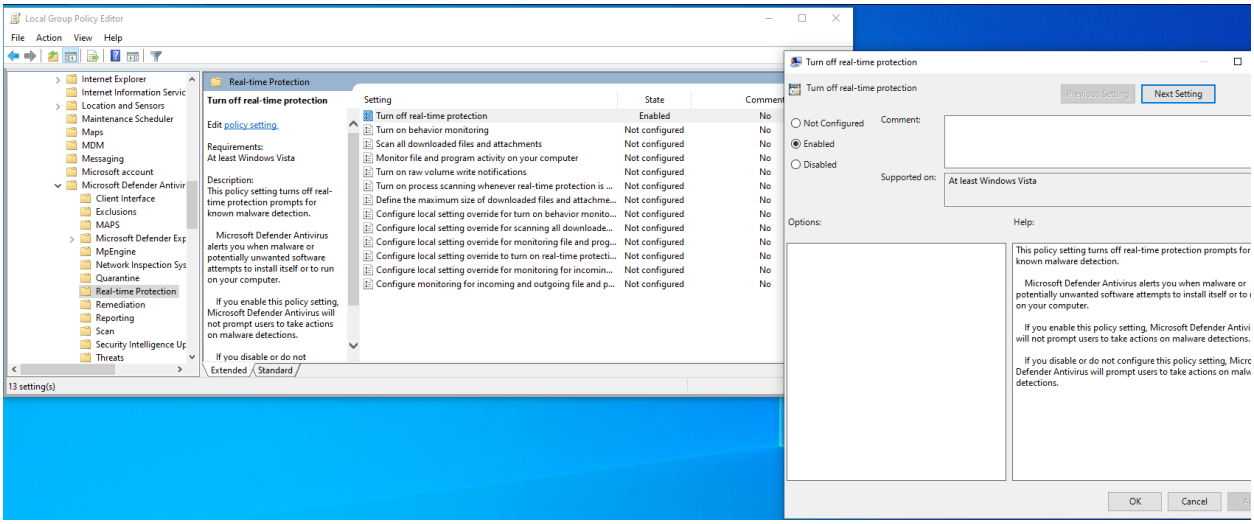
At first, to successfully prepare Malware Analysis Lab, I used this resource – https://www.windowscentral.com/how-stop-updates-installing-automatically-windows-10 to configure and disable automatic updates.



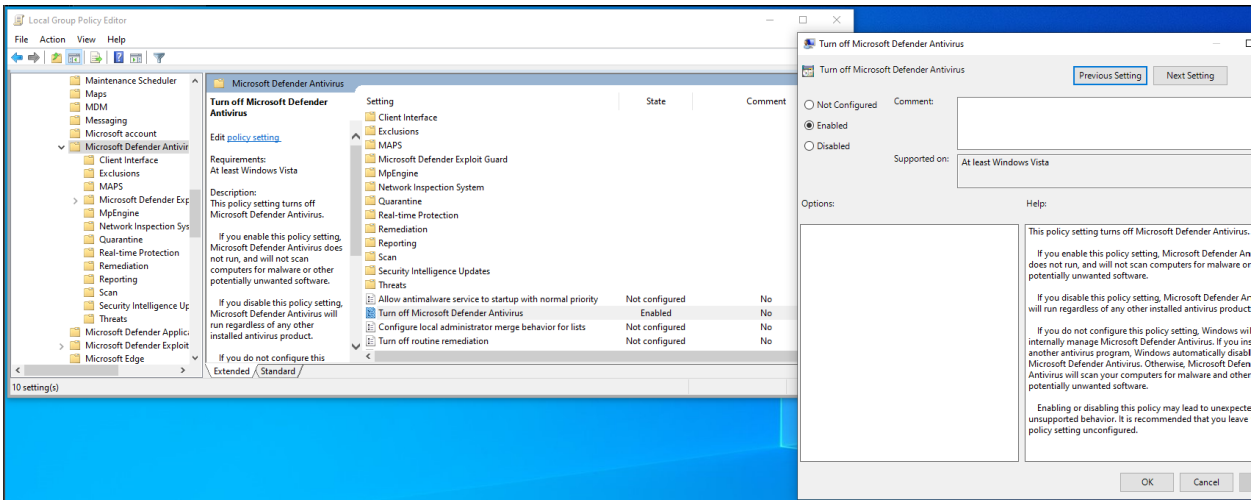
Also, installing Flare VM required to disable Windows Defende. I used this guide https://superuser.com/questions/1757339/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo. I had to turn off tamper protection setting.



Also, I also disabled real-time protection.



Lastly, I turned off Microsoft Defender Antivirus.



Then, using the instructions of Flare VM here - https://github.com/mandiant/flare-vm, I installed Flare VM.

```
PS C:\Windows\system32> (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/mai
n/install.ps1',"$([Environment]::GetFolderPath("Desktop"))\install.ps1")
PS C:\Windows\system32> cd C:\Users\simon\Desktop
PS C:\Users\simon\Desktop> Unblock-File .\install.ps1
PS C:\Users\simon\Desktop> Set-ExecutionPolicy Unrestricted -Force
PS C:\Users\simon\Desktop> .\install.ps1 -password Password123 -noWait -noGui
```

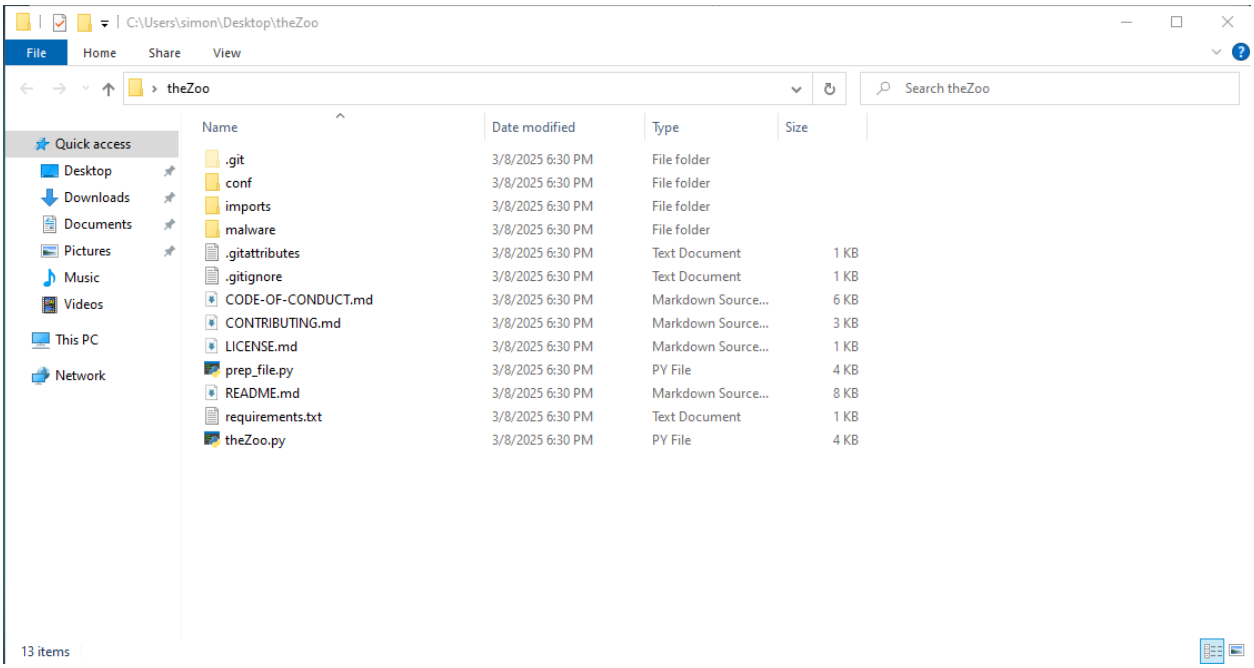
Also, I used REMnux documentation and installed REMnux on Linux using this article https://docs.remnux.org/install-distro/install-from-scratch

```
simon@ubuntu:~$ wget https://REMnux.org/remnux-cli
--2025-03-08 05:17:27--  https://remnux.org/remnux-cli
Resolving remnux.org (remnux.org)... 185.199.108.153, 185.199.109.153, 185.199.110.153, ...
Connecting to remnux.org (remnux.org)|185.199.108.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 82407294 (79M) [application/octet-stream]
Saving to: ‘remnux-cli’

remnux-cli          100%[===================>]  78.59M  11.3MB/s    in 7.0s

2025-03-08 05:17:36 (11.2 MB/s) - ‘remnux-cli’ saved [82407294/82407294]

simon@ubuntu:~$ sha256sum remnux-cli
c8c6d6830cfeb48c9ada2b49c76523c8637d95dc41d00aac345282fb47021f8e  remnux-cli
simon@ubuntu:~$ mv remnux-cli remnux
simon@ubuntu:~$ chmod +x remnux
simon@ubuntu:~$ sudo mv remnux /usr/local/bin
[sudo] password for simon:
```

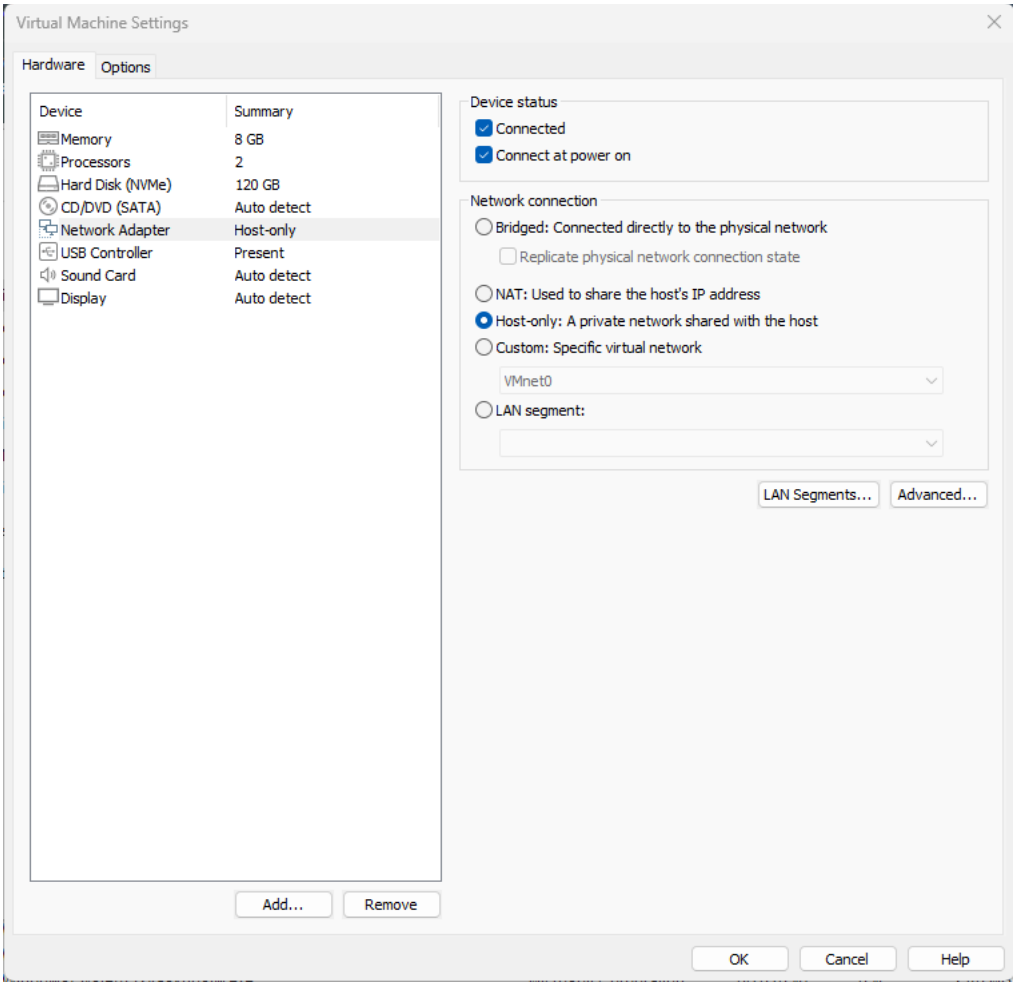
```
simon@ubuntu:~$ sudo remnux install
```

```
simon@ubuntu: ~
>> Running: /etc/apt/apt.conf.d/20auto-upgrades
>> Running: systemd-timesyncd
>> Running: bluetooth
>> Running: docker
>> Running: /usr/local/bin/docker
>> Running: apt-get autoremove -y
>> Running: /etc/ssh/sshd_config
>> Running: /etc/ssh/sshd_config
>> Running: /etc/ssh/sshd_config
>> Running: /etc/ssh/sshd_config
>> Running: /etc/ssh/sshd_config
>> Running: /etc/ssh/sshd_config
>> Running: away-from-the-dog
>> Running: echo "wireshark-common wireshark-common/install-setuid select True"| debconf-set-selections; dpkg-reconfigure -f noninteractive wireshark-common
>> Running: wireshark
>> Running: remnux-theme
>> Running: ssh
>> Running: remnux-dedicated

>> COMPLETED SUCCESSFULLY! Success: 806, Failure: 0


>> Please reboot to make sure all settings go into effect.
simon@ubuntu:~$
```

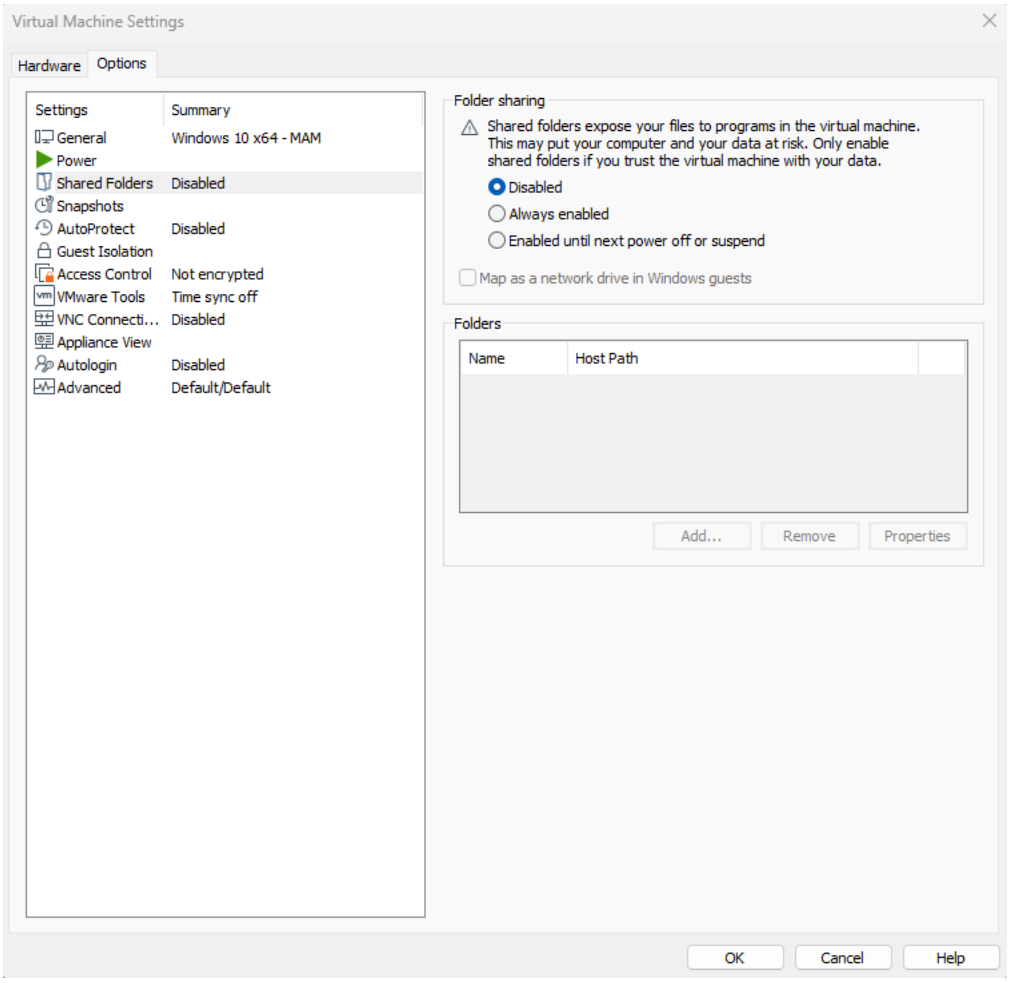
To obtain malware samples I cloned the Zoo repository from this link
https://github.com/ytisf/theZoo



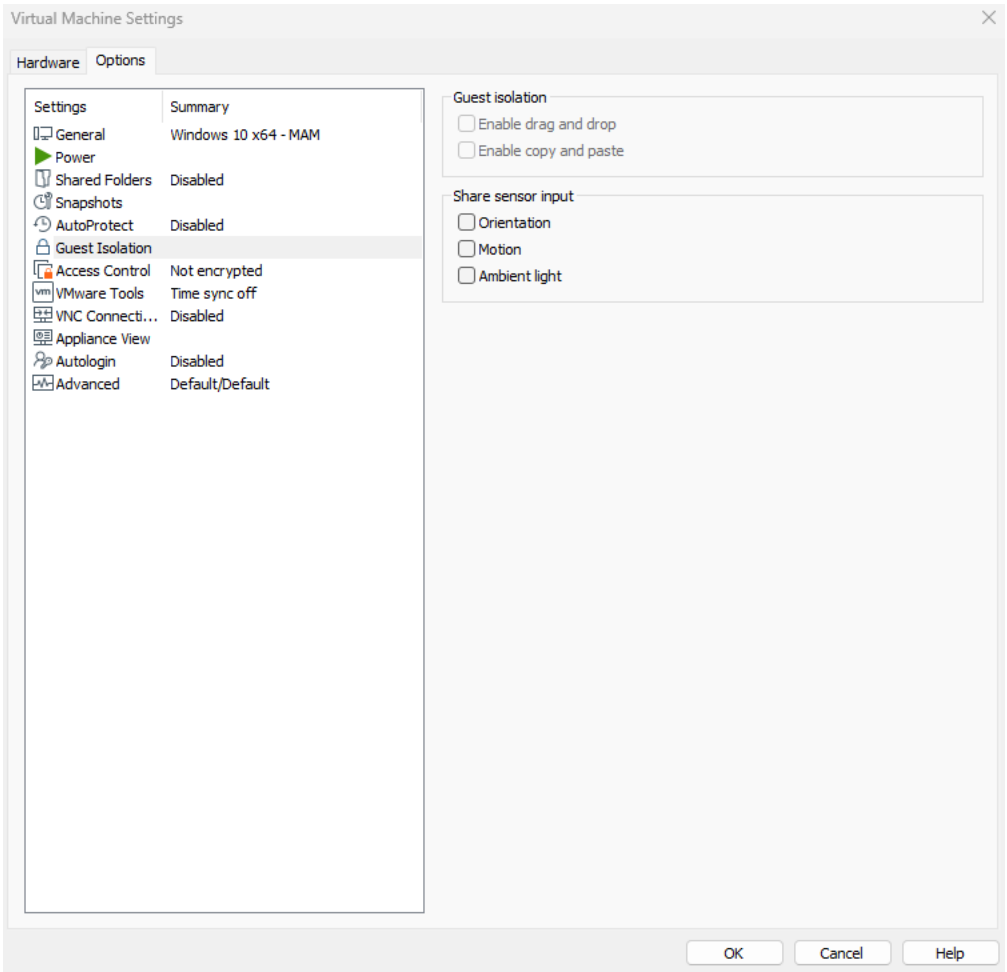
Before running malware I put it to Host-only



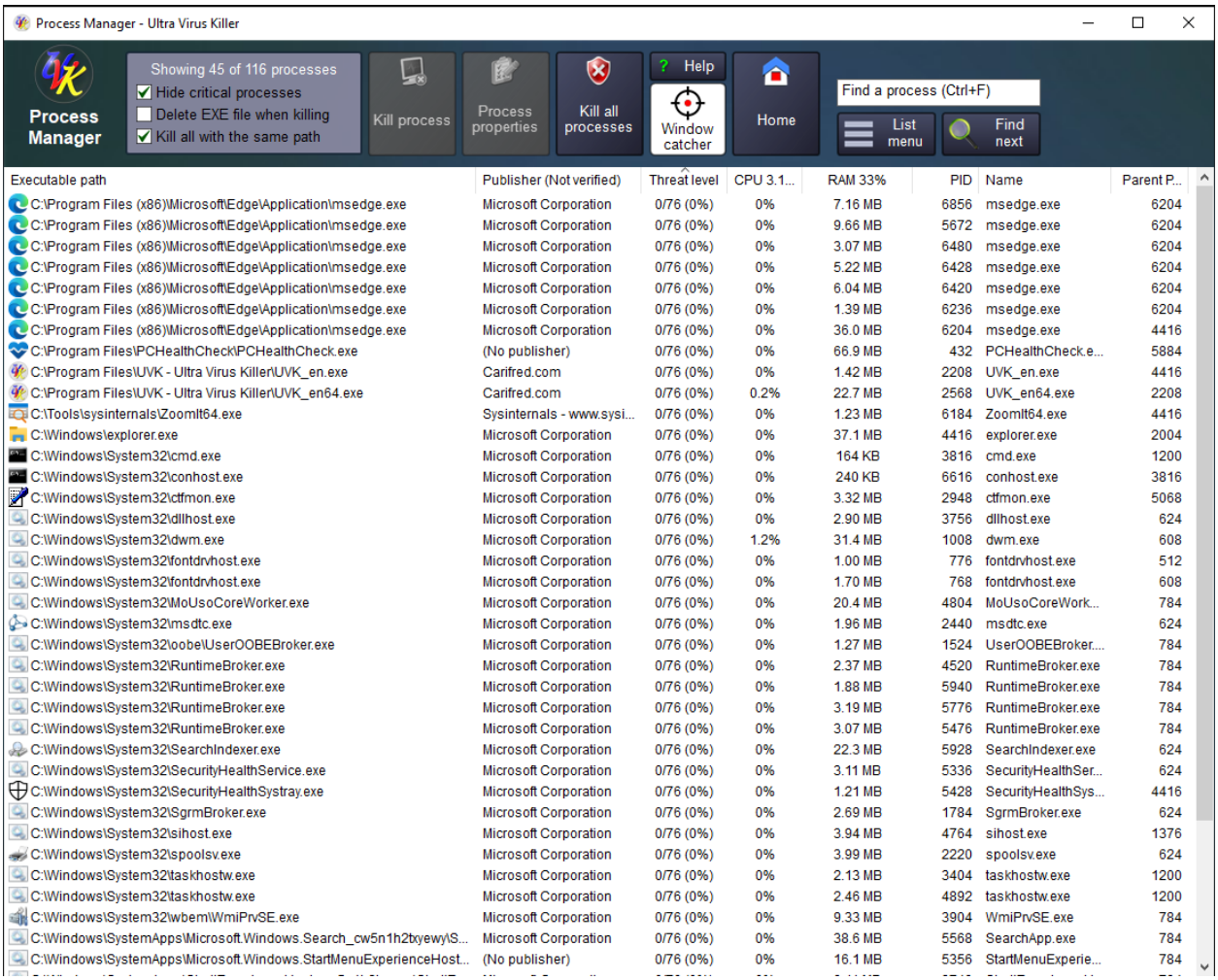
Also, I disabled shared folders.



And also did guest isolation – no drag and drop and no clipboard.

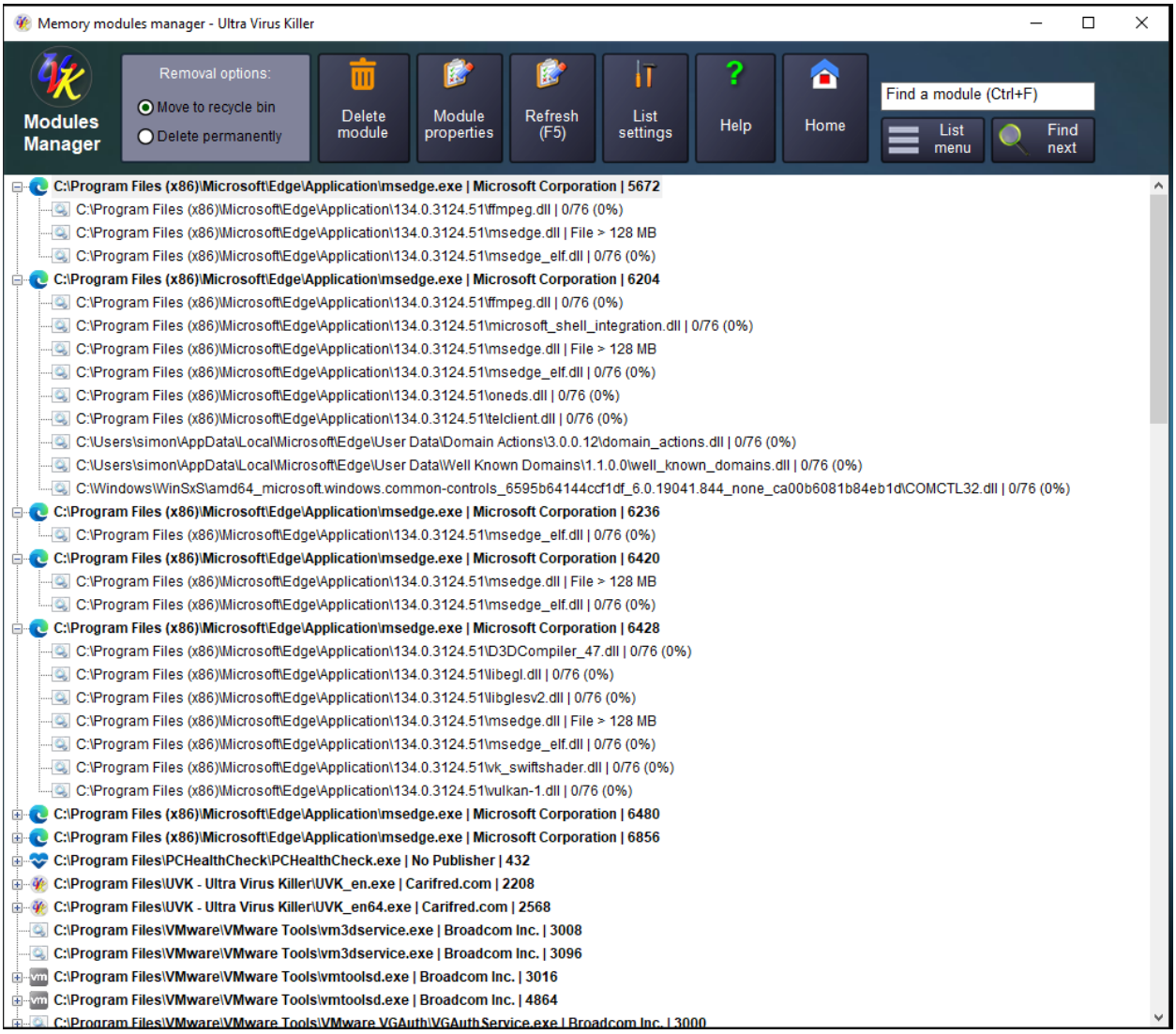

Virtual Machine Settings
Hardware
Options
Settings
Summary
General
Windows 10 x64 - MAM
Power
Shared Folders
Disabled
Snapshots
AutoProtect
Disabled
Guest Isolation
Access Control
Not encrypted
VMware Tools
Time sync off
VNC Connecti...
Disabled
Appliance View
Autologin
Disabled
Advanced
Default/Default
Guest isolation
Enable drag and drop
Enable copy and paste
Share sensor input
Orientation
Motion
Ambient light
OK
Cancel
Help

Then, I downloaded UVK and used UVK's Process Manager and Memory Modules Manager modules to check how they can used to identify malware. The test involves checking for threats when malware is stationary (not executed) versus when it is actively running.

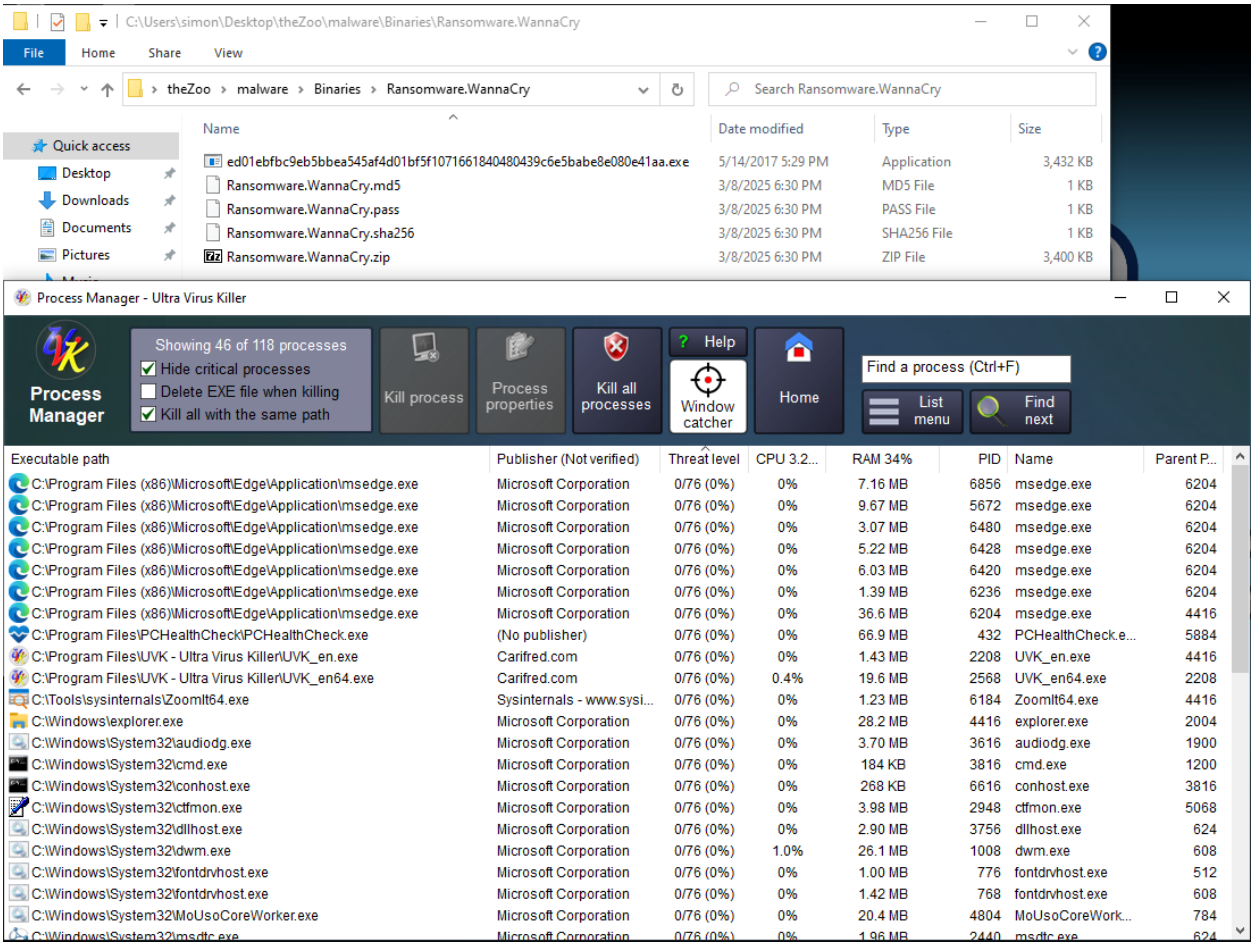


Executable path	Publisher (Not verified)	Threat level	CPU 3.1...	RAM 33%	PID	Name	Parent P...
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	7.16 MB	6856	msedge.exe	6204
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	9.66 MB	5672	msedge.exe	6204
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	3.07 MB	6480	msedge.exe	6204
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	5.22 MB	6428	msedge.exe	6204
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	6.04 MB	6420	msedge.exe	6204
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	1.39 MB	6236	msedge.exe	6204
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	36.0 MB	6204	msedge.exe	4416
C:\Program Files\PCHealthCheck\PCHealthCheck.exe	(No publisher)	0/76 (0%)	0%	66.9 MB	432	PCHealthCheck.e...	5884
C:\Program Files\UVK - Ultra Virus Killer\UVK_en.exe	Carifred.com	0/76 (0%)	0%	1.42 MB	2208	UVK_en.exe	4416
C:\Program Files\UVK - Ultra Virus Killer\UVK_en64.exe	Carifred.com	0/76 (0%)	0.2%	22.7 MB	2568	UVK_en64.exe	2208
C:\Tools\sysinternals\Zoomlt64.exe	Sysinternals - www.sysi...	0/76 (0%)	0%	1.23 MB	6184	Zoomlt64.exe	4416
C:\Windows\explorer.exe	Microsoft Corporation	0/76 (0%)	0%	37.1 MB	4416	explorer.exe	2004
C:\Windows\System32\cmd.exe	Microsoft Corporation	0/76 (0%)	0%	164 KB	3816	cmd.exe	1200
C:\Windows\System32\conhost.exe	Microsoft Corporation	0/76 (0%)	0%	240 KB	6616	conhost.exe	3816
C:\Windows\System32\ctfmon.exe	Microsoft Corporation	0/76 (0%)	0%	3.32 MB	2948	ctfmon.exe	5068
C:\Windows\System32\dllhost.exe	Microsoft Corporation	0/76 (0%)	0%	2.90 MB	3756	dllhost.exe	624
C:\Windows\System32\dwm.exe	Microsoft Corporation	0/76 (0%)	1.2%	31.4 MB	1008	dwm.exe	608
C:\Windows\System32\fontdrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.00 MB	776	fontdrvhost.exe	512
C:\Windows\System32\fontdrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.70 MB	768	fontdrvhost.exe	608
C:\Windows\System32\MoUsoCoreWorker.exe	Microsoft Corporation	0/76 (0%)	0%	20.4 MB	4804	MoUsoCoreWork...	784
C:\Windows\System32\msdtc.exe	Microsoft Corporation	0/76 (0%)	0%	1.96 MB	2440	msdtc.exe	624
C:\Windows\System32\oobe\UserOOBEBroker.exe	Microsoft Corporation	0/76 (0%)	0%	1.27 MB	1524	UserOOBEBroker....	784
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	2.37 MB	4520	RuntimeBroker.exe	784
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	1.88 MB	5940	RuntimeBroker.exe	784
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	3.19 MB	5776	RuntimeBroker.exe	784
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	3.07 MB	5476	RuntimeBroker.exe	784
C:\Windows\System32\SearchIndexer.exe	Microsoft Corporation	0/76 (0%)	0%	22.3 MB	5928	SearchIndexer.exe	624
C:\Windows\System32\SecurityHealthService.exe	Microsoft Corporation	0/76 (0%)	0%	3.11 MB	5336	SecurityHealthSer...	624
C:\Windows\System32\SecurityHealthSystray.exe	Microsoft Corporation	0/76 (0%)	0%	1.21 MB	5428	SecurityHealthSys...	4416
C:\Windows\System32\SgrmBroker.exe	Microsoft Corporation	0/76 (0%)	0%	2.69 MB	1784	SgrmBroker.exe	624
C:\Windows\System32\sihost.exe	Microsoft Corporation	0/76 (0%)	0%	3.94 MB	4764	sihost.exe	1376
C:\Windows\System32\spoolsv.exe	Microsoft Corporation	0/76 (0%)	0%	3.99 MB	2220	spoolsv.exe	624
C:\Windows\System32\taskhostw.exe	Microsoft Corporation	0/76 (0%)	0%	2.13 MB	3404	taskhostw.exe	1200
C:\Windows\System32\taskhostw.exe	Microsoft Corporation	0/76 (0%)	0%	2.46 MB	4892	taskhostw.exe	1200
C:\Windows\System32\wbem\WmiPrvSE.exe	Microsoft Corporation	0/76 (0%)	0%	9.33 MB	3904	WmiPrvSE.exe	784
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\S...	Microsoft Corporation	0/76 (0%)	0%	38.6 MB	5568	SearchApp.exe	784
C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost...	(No publisher)	0/76 (0%)	0%	16.1 MB	5356	StartMenuExperie...	784

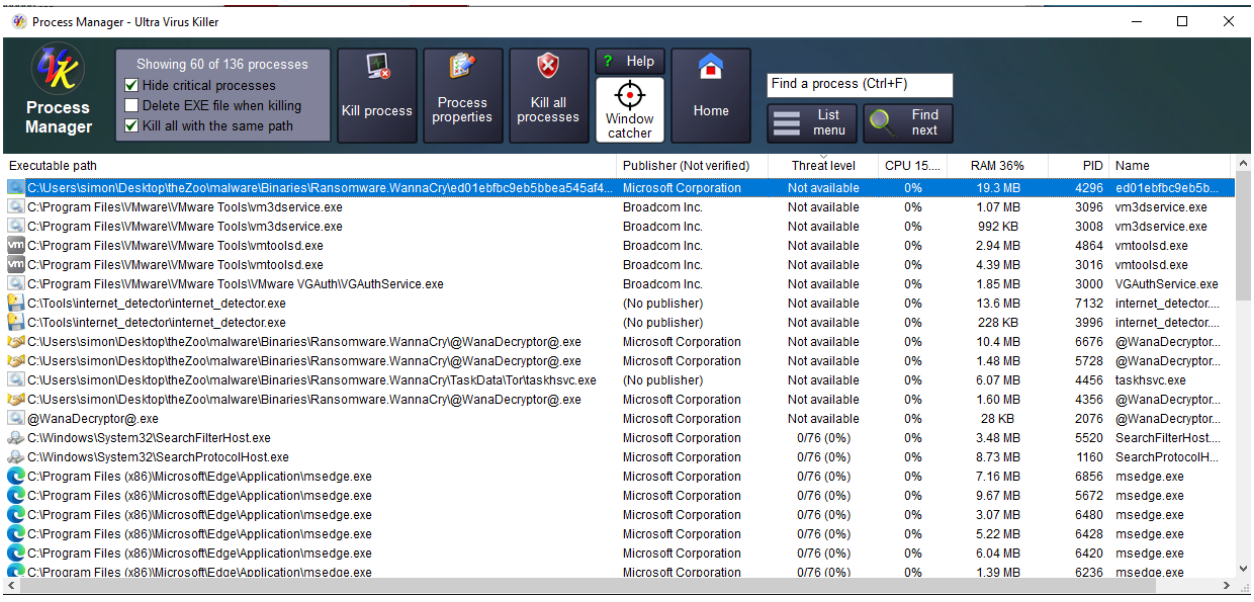
UVK assigns a Threat Level to processes, but no suspicious processes are detected in this stage when malware is stationary. The same goes to memory modules.



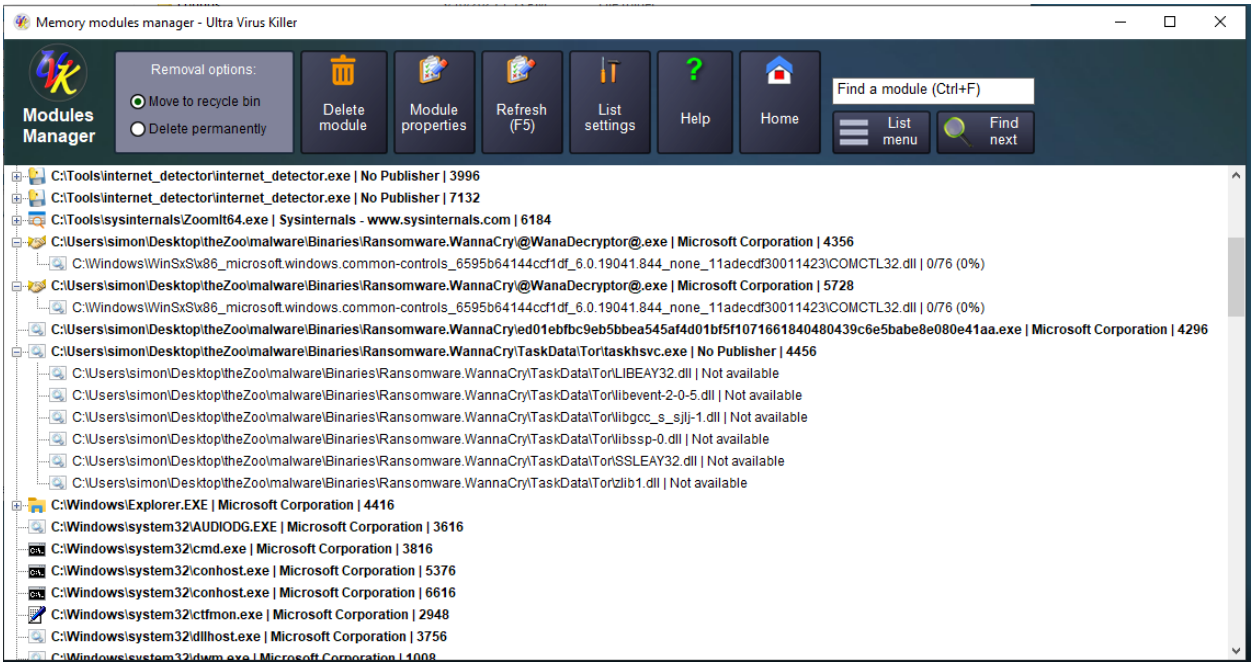
I navigated to WannaCry ransomware in Zoo binaries folder using File Explorer. UVK does not detect it as a running threat because it is not yet executed. UVK is more focused on running processes, so likely it won't detect the malware at this stage. UVK does not flag stationary malware in its Process Manager because it appears it does not actively scan files on disk.



I launched the application. The WannaCry executable appeared in the process list. Multiple new processes related to WannaCry spawned. No immediate threat level was assigned, but the process was unverified. The process used 19.3 MB RAM, which indicates it was running.

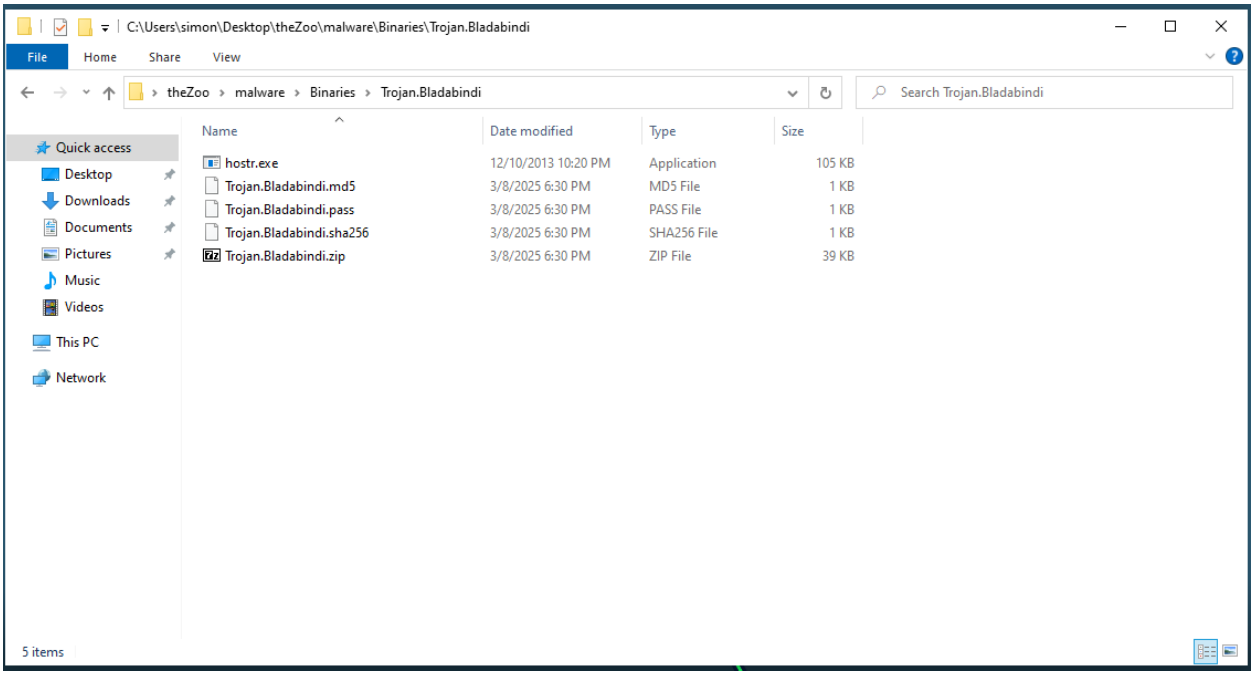


Multiple new DLLs were loaded into memory. Some DLLs were from Tor, suggesting WannaCry's network activity. Microsoft-signed DLLs were also loaded, probably an evasion technique.



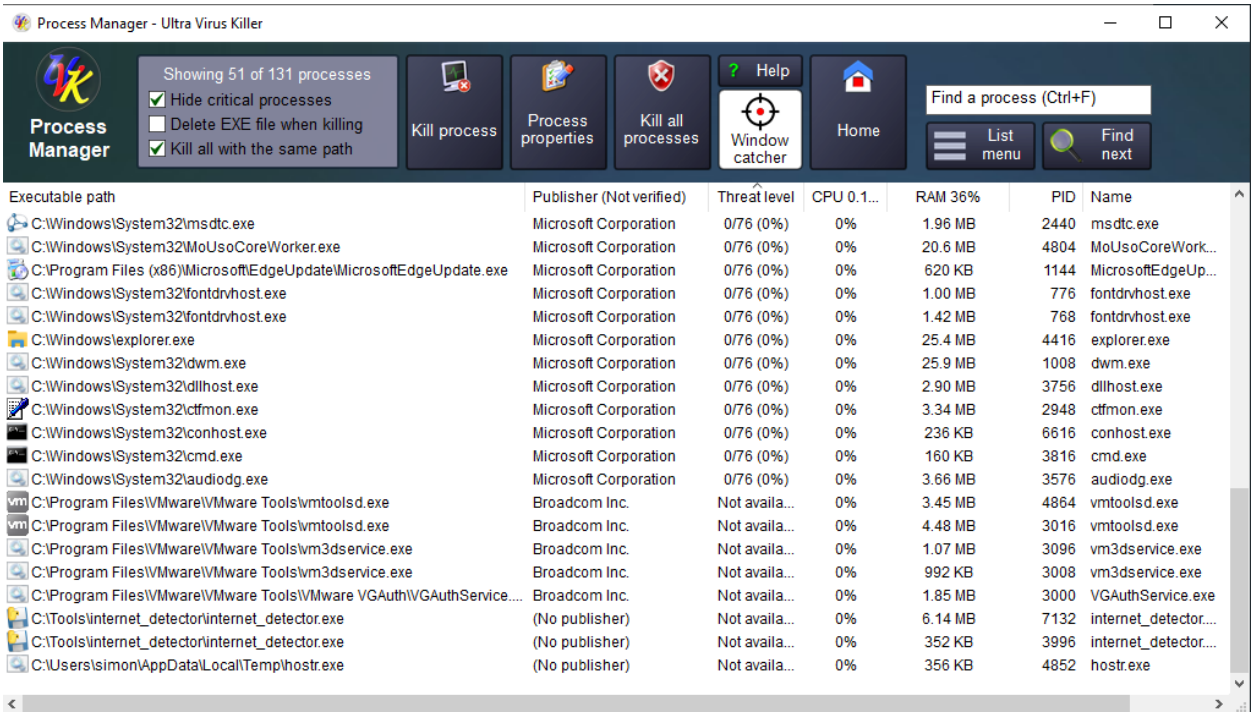
UVK detected the running malware but did not assign a threat level. Memory modules analysis revealed injected and loaded DLLs.

I also analyzed Trojan.Bladabindi. Before execution, the malware file hostr.exe was stored in the folder: C:\Users\simon\Desktop\theZoo\malware\Binaries\Trojan.Bladabindi\



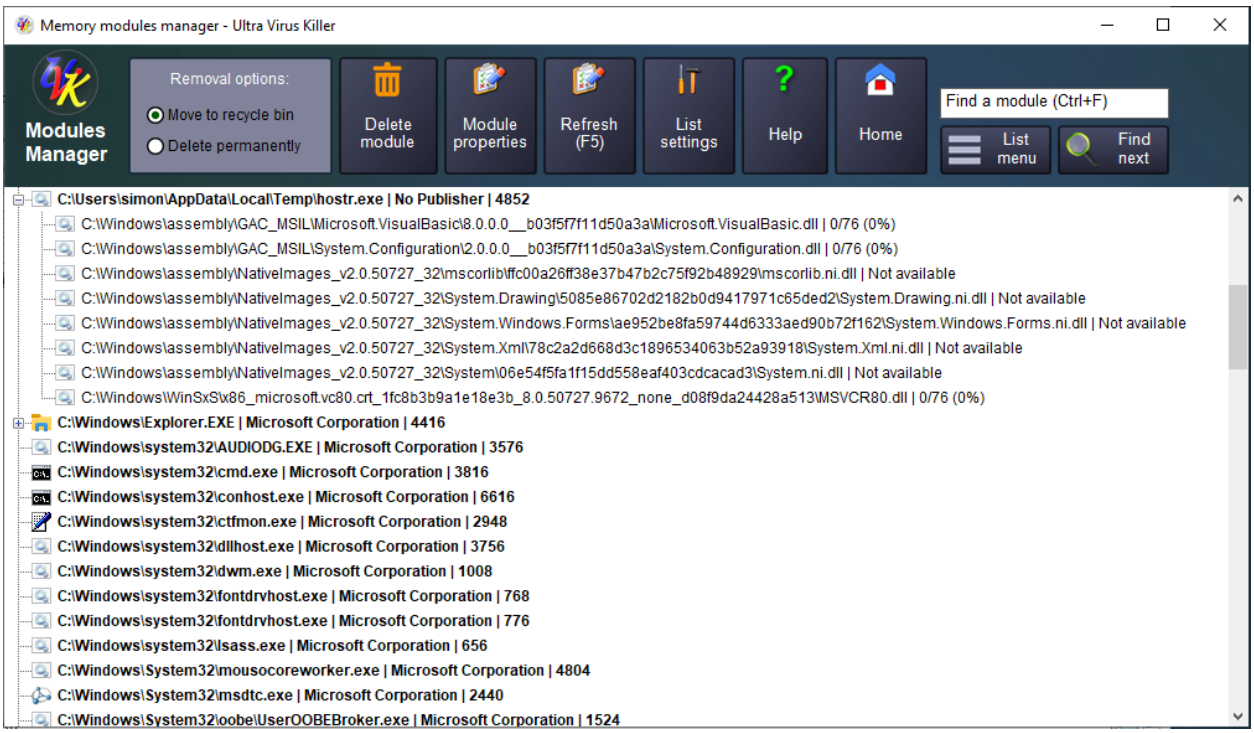
UVK did not detect it as a threat while it was in a not launched state. This confirms that UVK does not scan files on disk for malware. UVK's Process Manager and Memory Modules Manager focus on active processes and memory, not static file scanning.

After executing hostr.exe, I checked UVK's Process Manager.



A new process named hostr.exe appeared. No threat level was assigned by UVK. The process was running from C:\Users\simon\AppData\Local\Temp\, which is a suspicious location often used by malware. The process had a low RAM footprint (356 KB). Unlike WannaCry, this malware runs with a small memory footprint, making it harder to detect based on CPU/memory usage alone.

Using Memory Modules Manager, I observed the following:

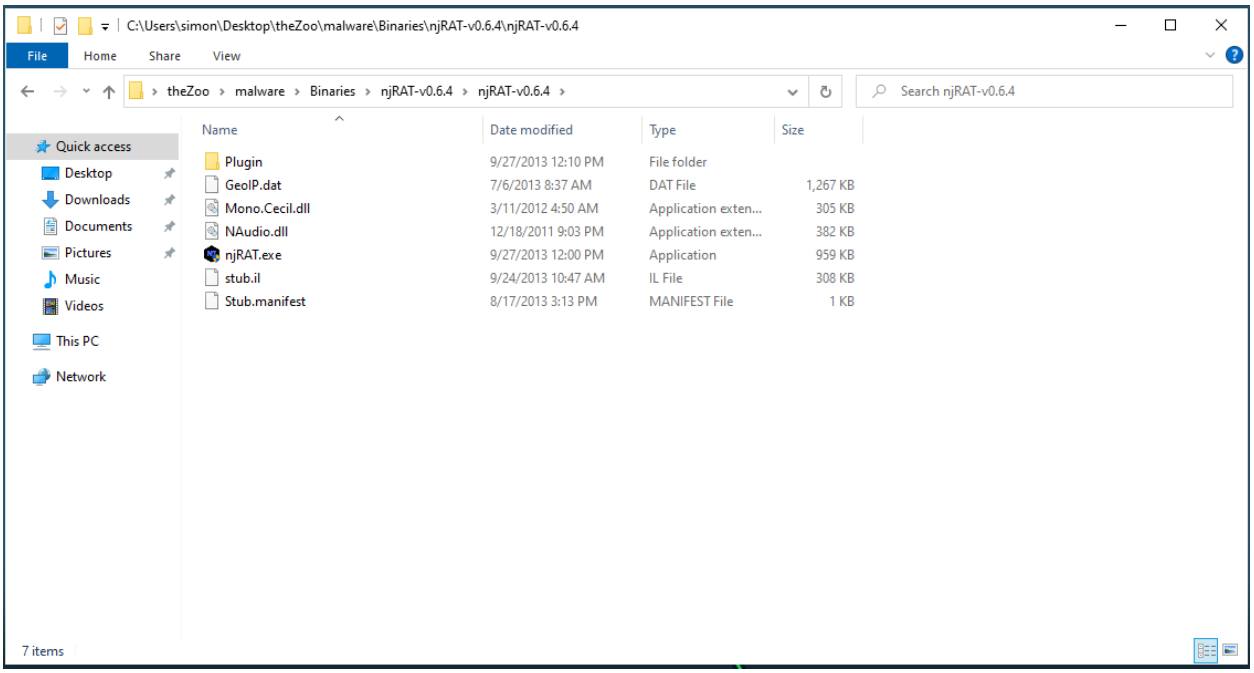


hostr.exe loaded several modules, including Visual Basic DLLs (Microsoft.VisualBasic.dll). It also loaded common .NET framework DLLs (System.Configuration.dll, System.Drawing.dll).

No direct signs of persistence mechanisms were detected in this scan. Unlike WannaCry, it does not load Tor DLLs or create multiple child processes.

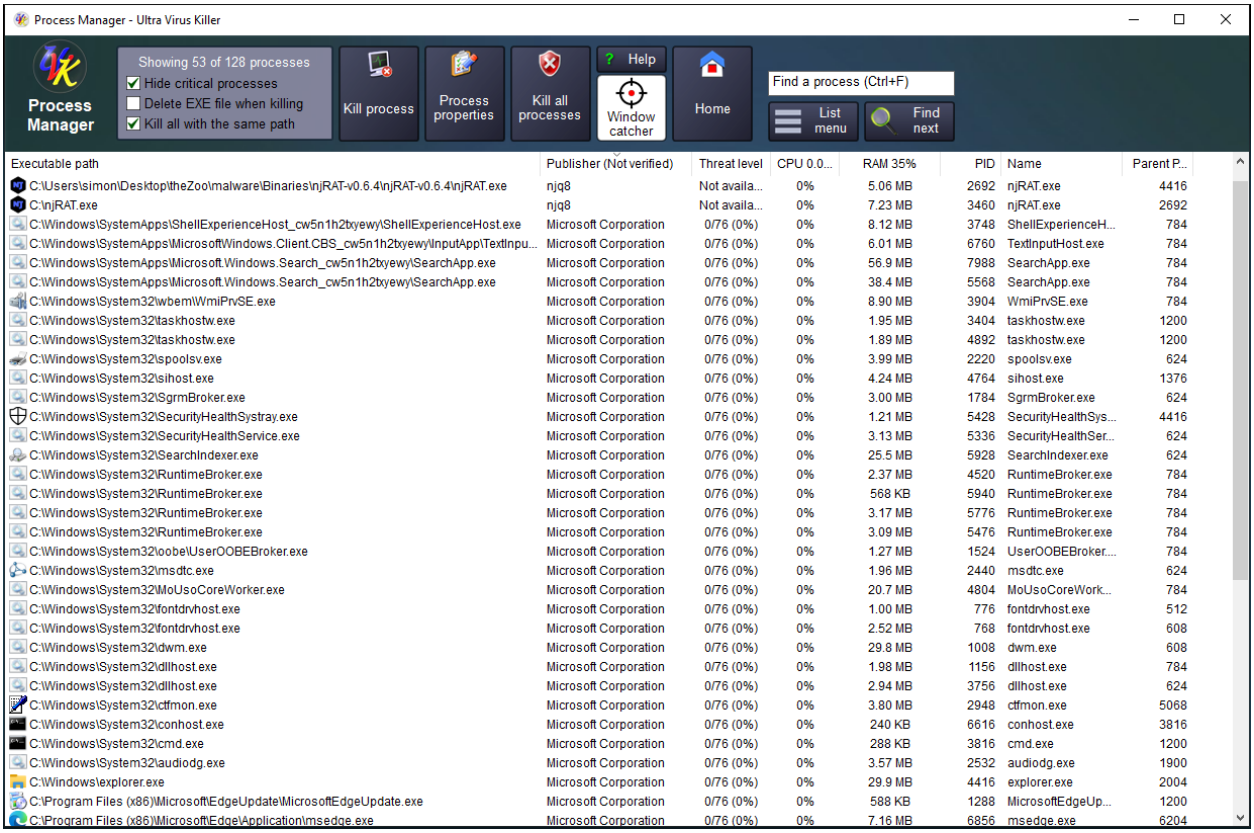
WannaCry is more aggressive, spawning multiple processes. Bladabindi is stealthier, using low memory and hiding in Temp folders. Both evaded UVK's threat scoring, showing the limitations of heuristic-based detection.

The third sample – njRAT executable was stored in C:\Users\simon\Desktop\theZoo\malware\Binaries\njRAT-v0.6.4\



Again, UVK did not detect njRAT while it was stationary. No threat levels were assigned since the malware was not running. This behavior confirms UVK does not scan files for malware unless executed.

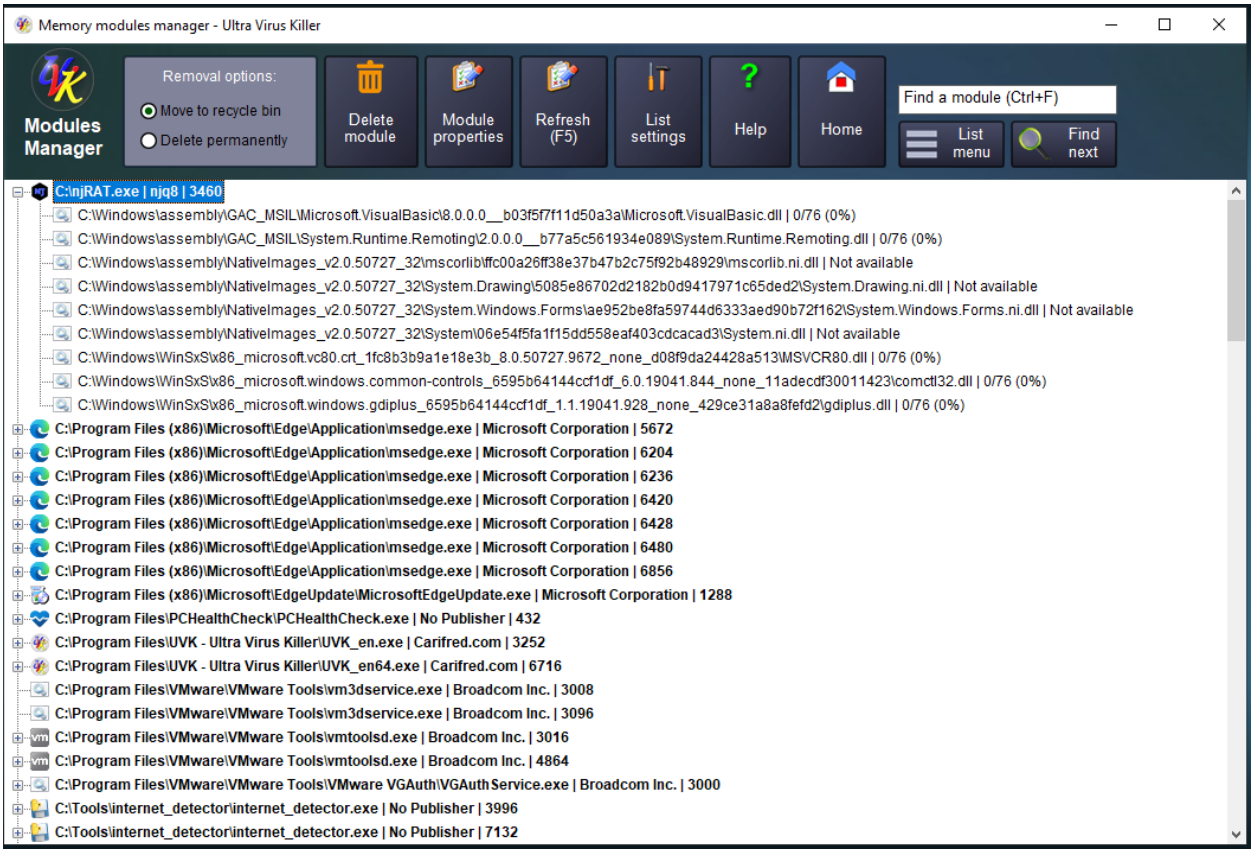
After executing njRAT.exe, UVK's Process Manager displayed new activity.



Executable path	Publisher (Not verified)	Threat level	CPU 0.0...	RAM 35%	PID	Name	Parent P...
C:\Users\simon\Desktop\theZoo\malware\Binaries\njRAT-v0.6.4\njRAT-v0.6.4\njRAT.exe	njq8	Not availa...	0%	5.06 MB	2692	njRAT.exe	4416
C:\njRAT.exe	njq8	Not availa...	0%	7.23 MB	3460	njRAT.exe	2692
C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	Microsoft Corporation	0/76 (0%)	0%	8.12 MB	3748	ShellExperienceH...	784
C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInpu...	Microsoft Corporation	0/76 (0%)	0%	6.01 MB	6760	TextInputHost.exe	784
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe	Microsoft Corporation	0/76 (0%)	0%	56.9 MB	7988	SearchApp.exe	784
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe	Microsoft Corporation	0/76 (0%)	0%	38.4 MB	5568	SearchApp.exe	784
C:\Windows\System32\wbem\WmiPrvSE.exe	Microsoft Corporation	0/76 (0%)	0%	8.90 MB	3904	WmiPrvSE.exe	784
C:\Windows\System32\taskhostw.exe	Microsoft Corporation	0/76 (0%)	0%	1.95 MB	3404	taskhostw.exe	1200
C:\Windows\System32\taskhostw.exe	Microsoft Corporation	0/76 (0%)	0%	1.89 MB	4892	taskhostw.exe	1200
C:\Windows\System32\spoolsv.exe	Microsoft Corporation	0/76 (0%)	0%	3.99 MB	2220	spoolsv.exe	624
C:\Windows\System32\sihost.exe	Microsoft Corporation	0/76 (0%)	0%	4.24 MB	4764	sihost.exe	1376
C:\Windows\System32\SgrmBroker.exe	Microsoft Corporation	0/76 (0%)	0%	3.00 MB	1784	SgrmBroker.exe	624
C:\Windows\System32\SecurityHealthSystray.exe	Microsoft Corporation	0/76 (0%)	0%	1.21 MB	5428	SecurityHealthSys...	4416
C:\Windows\System32\SecurityHealthService.exe	Microsoft Corporation	0/76 (0%)	0%	3.13 MB	5336	SecurityHealthSer...	624
C:\Windows\System32\SearchIndexer.exe	Microsoft Corporation	0/76 (0%)	0%	25.5 MB	5928	SearchIndexer.exe	624
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	2.37 MB	4520	RuntimeBroker.exe	784
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	568 KB	5940	RuntimeBroker.exe	784
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	3.17 MB	5776	RuntimeBroker.exe	784
C:\Windows\System32\RuntimeBroker.exe	Microsoft Corporation	0/76 (0%)	0%	3.09 MB	5476	RuntimeBroker.exe	784
C:\Windows\System32\oobe\UserOOBEBroker.exe	Microsoft Corporation	0/76 (0%)	0%	1.27 MB	1524	UserOOBEBroker....	784
C:\Windows\System32\msdtc.exe	Microsoft Corporation	0/76 (0%)	0%	1.96 MB	2440	msdtc.exe	624
C:\Windows\System32\MoUsoCoreWorker.exe	Microsoft Corporation	0/76 (0%)	0%	20.7 MB	4804	MoUsoCoreWork...	784
C:\Windows\System32\fontdrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.00 MB	776	fontdrvhost.exe	512
C:\Windows\System32\fontdrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	2.52 MB	768	fontdrvhost.exe	608
C:\Windows\System32\dwm.exe	Microsoft Corporation	0/76 (0%)	0%	29.8 MB	1008	dwm.exe	608
C:\Windows\System32\dllhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.98 MB	1156	dllhost.exe	784
C:\Windows\System32\dllhost.exe	Microsoft Corporation	0/76 (0%)	0%	2.94 MB	3756	dllhost.exe	624
C:\Windows\System32\ctfmon.exe	Microsoft Corporation	0/76 (0%)	0%	3.80 MB	2948	ctfmon.exe	5068
C:\Windows\System32\conhost.exe	Microsoft Corporation	0/76 (0%)	0%	240 KB	6616	conhost.exe	3816
C:\Windows\System32\cmd.exe	Microsoft Corporation	0/76 (0%)	0%	288 KB	3816	cmd.exe	1200
C:\Windows\System32\audiodg.exe	Microsoft Corporation	0/76 (0%)	0%	3.57 MB	2532	audiodg.exe	1900
C:\Windows\explorer.exe	Microsoft Corporation	0/76 (0%)	0%	29.9 MB	4416	explorer.exe	2004
C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Microsoft Corporation	0/76 (0%)	0%	588 KB	1288	MicrosoftEdgeUp...	1200
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	7.16 MB	6856	msedge.exe	6204

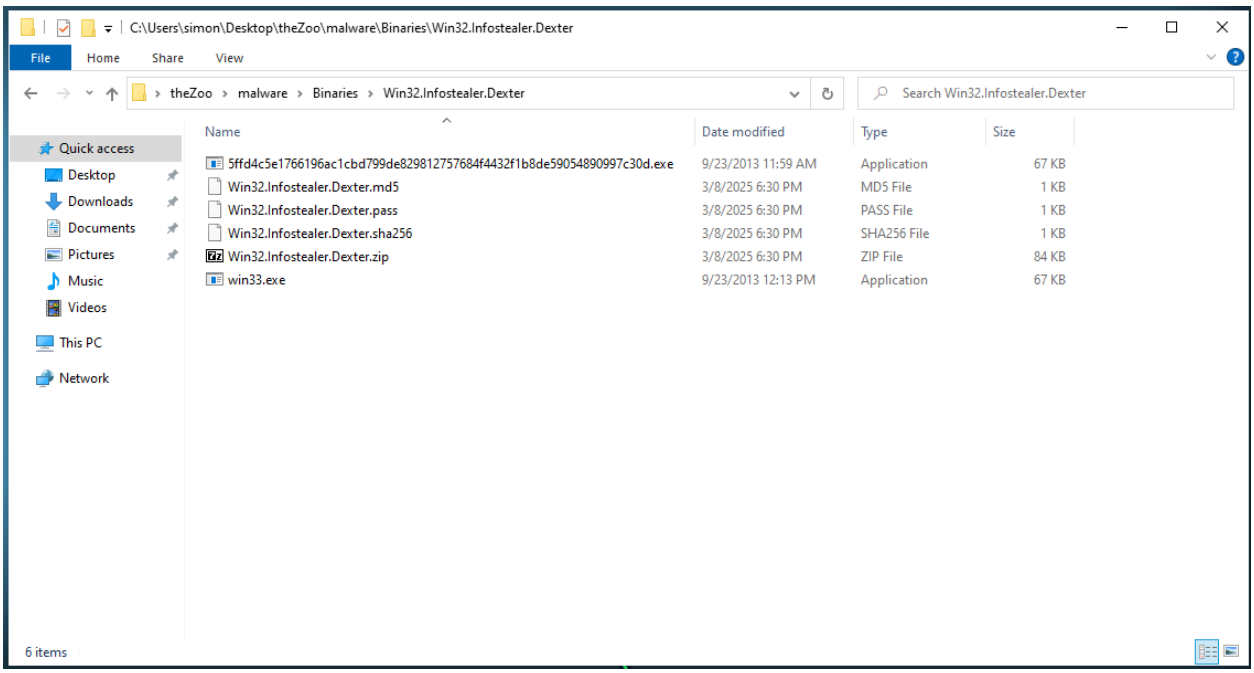
A new process named njRAT.exe appeared in the process list. No threat level was assigned by UVK. The process was running from the same directory where it was executed (C:\Users\simon\Desktop\theZoo\malware\Binaries\njRAT-v0.6.4\). RAM Usage (about 5 MB) is low, making it stealthier than WannaCry but higher than Bladabindi.

Using Memory Modules Manager, the following observations were made:

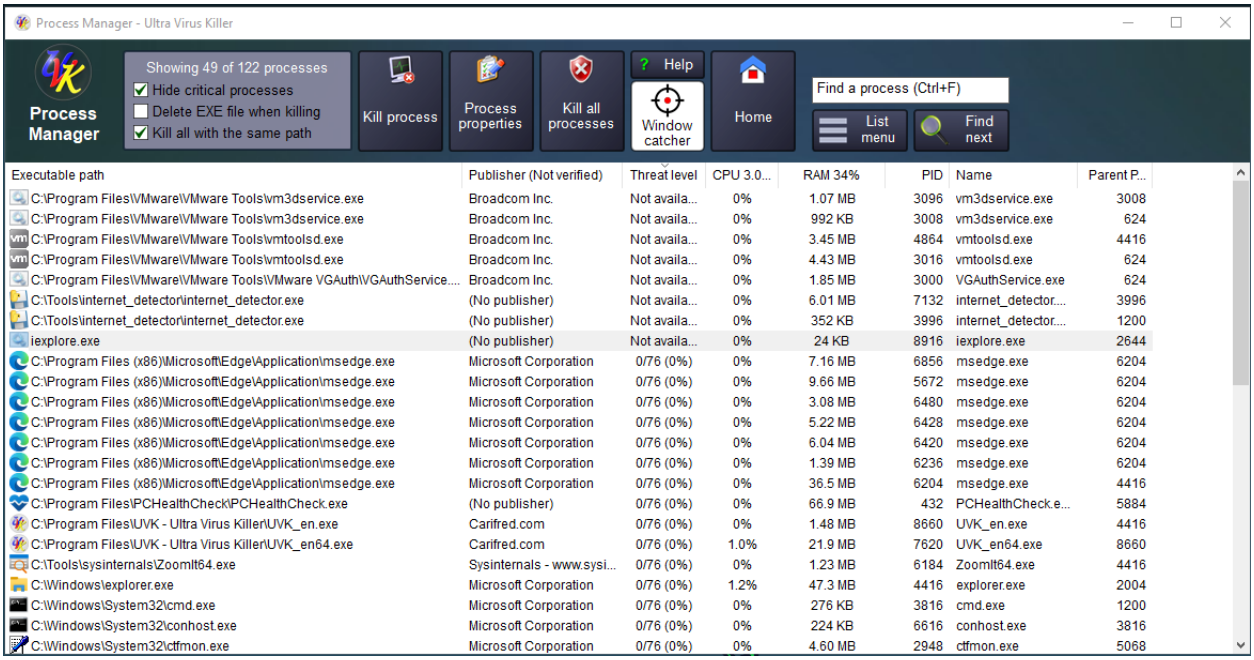


njRAT loaded several Microsoft .NET-related DLLs, including: Microsoft.VisualBasic.dll, System.Runtime.Remoting.dll, System.Drawing.dll. These libraries suggest that njRAT is built on the .NET framework, like Bladabindi. No direct signs of process injection, but its dependencies indicate it may rely on remote connections

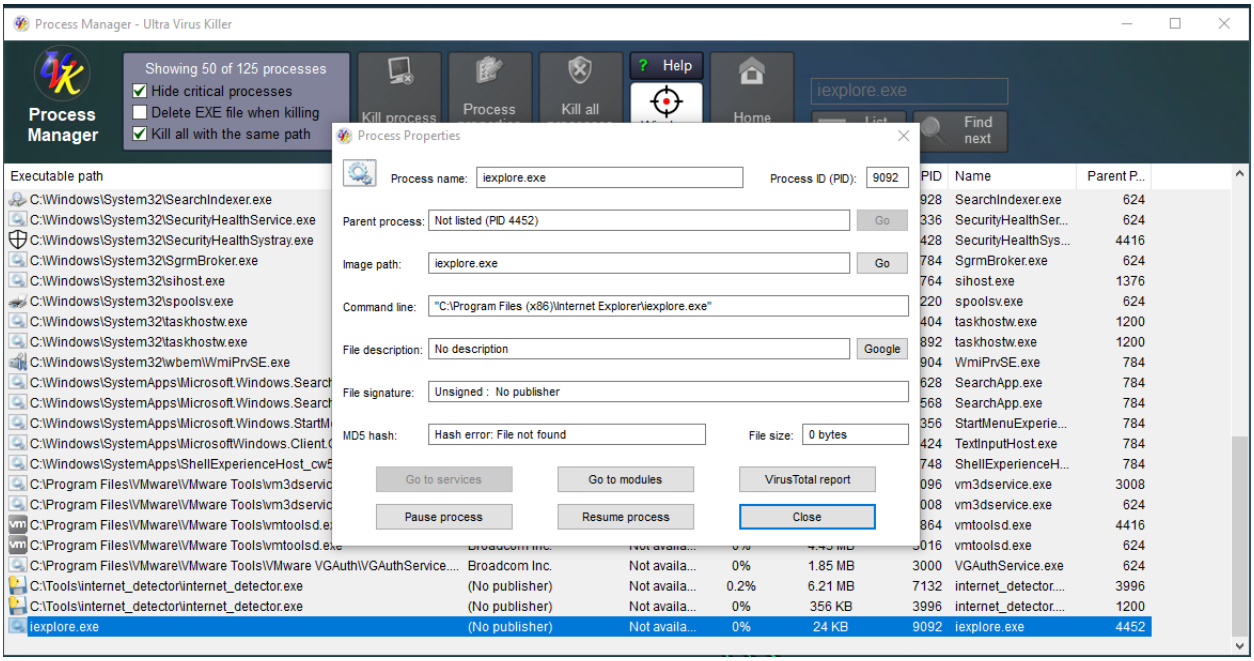
Then, I extracted Win32.Infostealer.Dexter.zip and launched .exe files.



When I checked UVK I identified new process, which is named iexplore.exe.

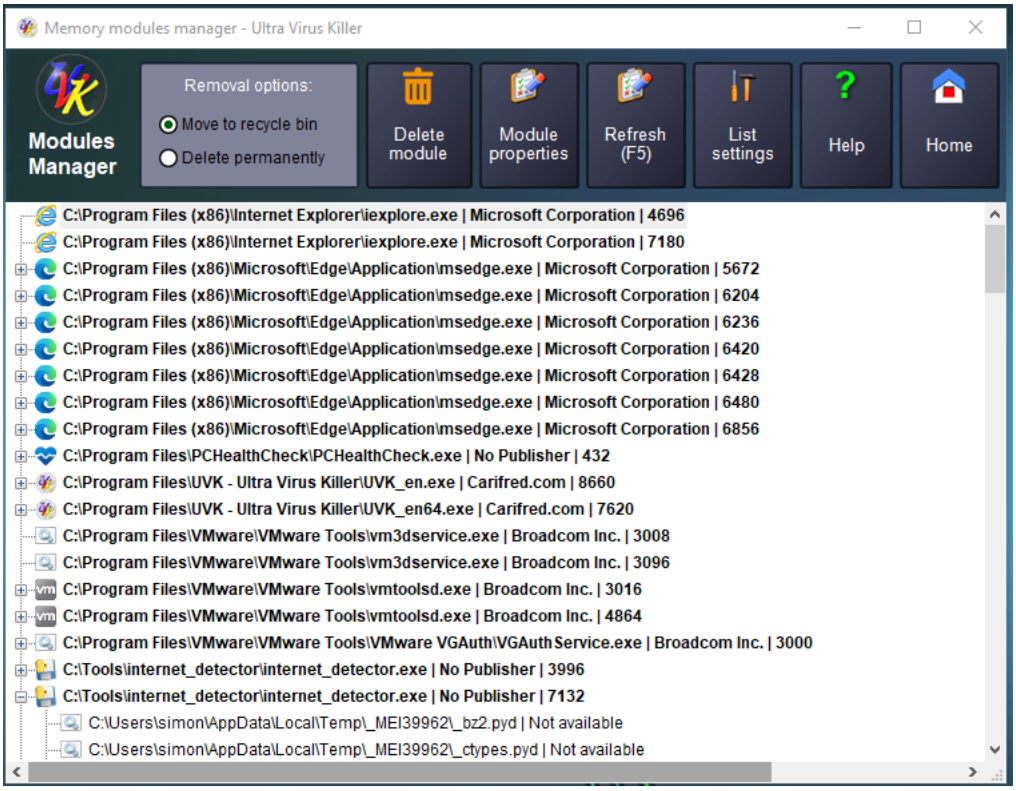


It had executable Path: C:\Program Files (x86)\Internet Explorer\iexplore.exe. Parent Process: Not listed (PID 4452) (Unusual behavior). File Signature: Unsigned - No Publisher. File Size: 0 bytes. CPU and RAM Usage: Minimal, indicating stealthy execution.



iexplore.exe was spawned unexpectedly, likely by Dexter, meaning the malware used process injection. The process being unsigned and having 0 bytes in size suggests it was modified in-memory. The lack of a proper parent process indicates that it was not started normally by the user.

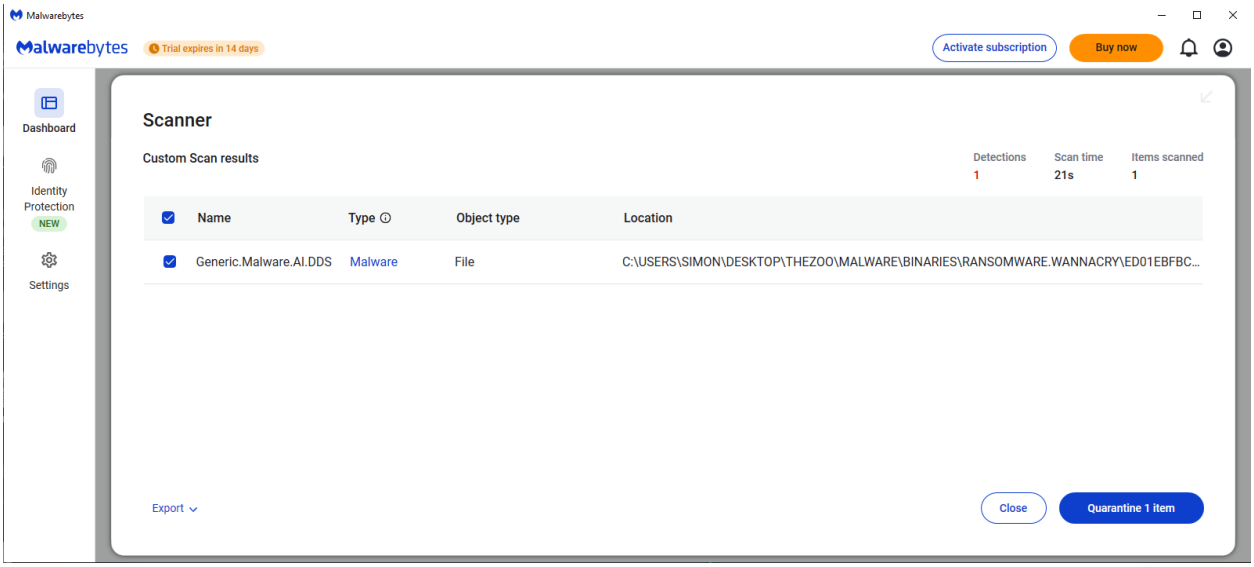
Then, I checked memory modules.



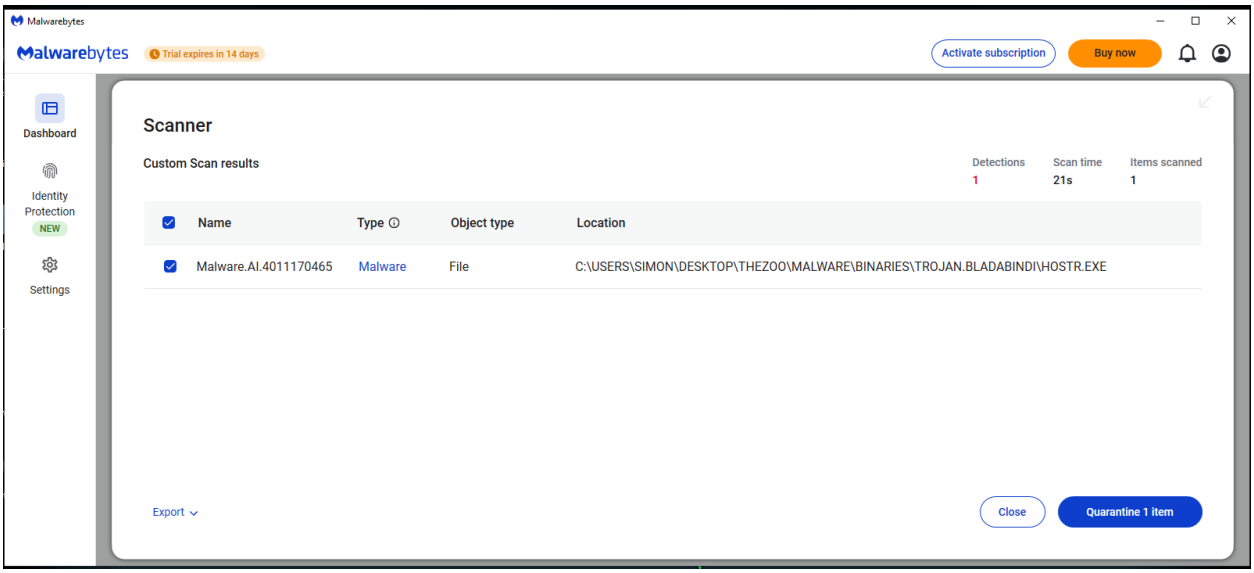
iexplore.exe Instances (PIDs: 4696, 7180) suggest multiple browser injections. Dexter uses process injection to operate inside iexplore.exe, avoiding detection. This is consistent with credential-stealing malware behavior, which hooks into web browsers. I confirmed it by reading about it – https://en.wikipedia.org/wiki/Dexter_(malware).

Conclusions – Stationary malware (not executed) is not detected by UVK's Process Manager or Memory Modules Manager. Running malware spawns processes and injects memory modules, which can be identified using UVK. Process verification & threat levels are limited in UVK, so additional tools like VirusTotal, or dynamic analysis tools are needed. Manual analysis is necessary, as UVK does not automatically classify threats.

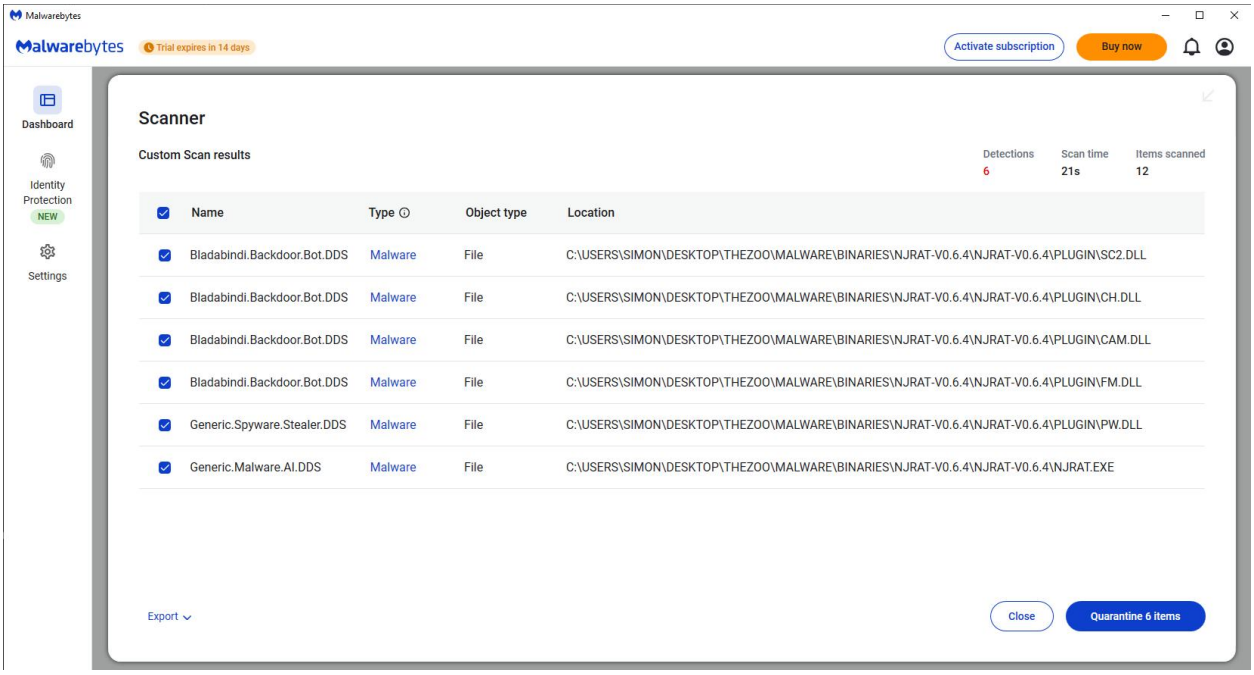
Malwarebytes identified a file from the WannaCry ransomware sample as a generic malware threat using AI-based detection.



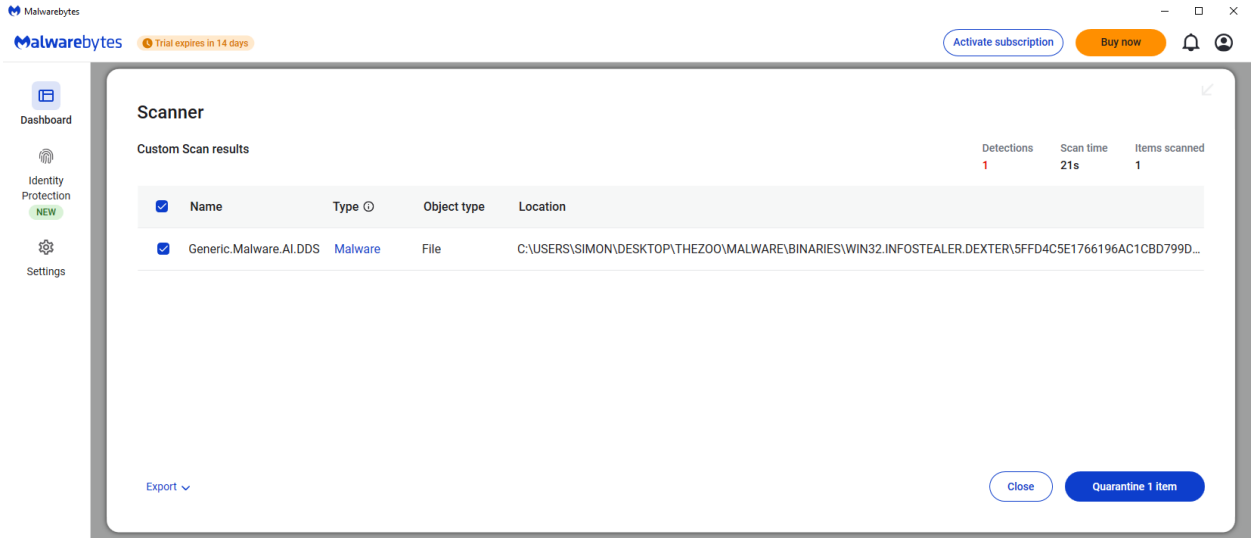
Malwarebytes flagged the Bladabindi trojan (also known as njRAT) as an AI-detected malware.



Malwarebytes detected njRAT and its components as backdoor trojans and spyware.

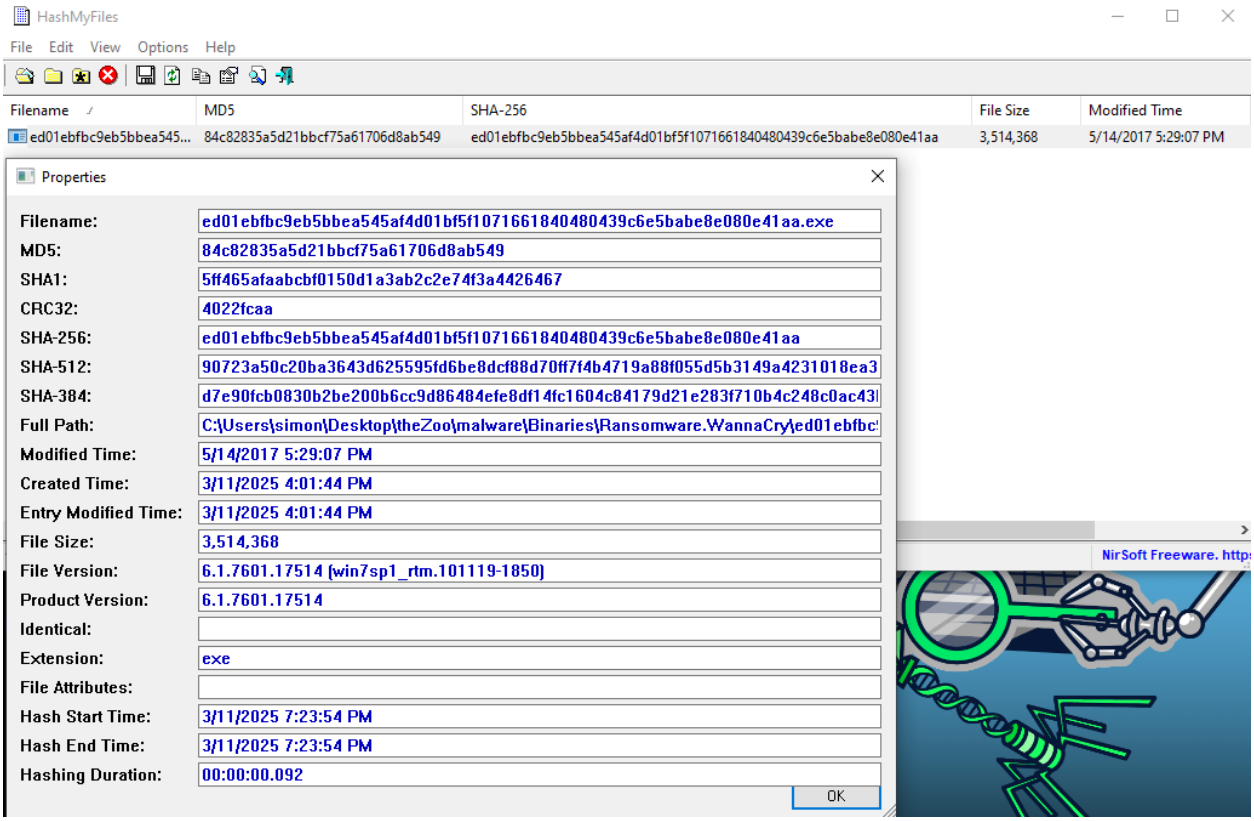


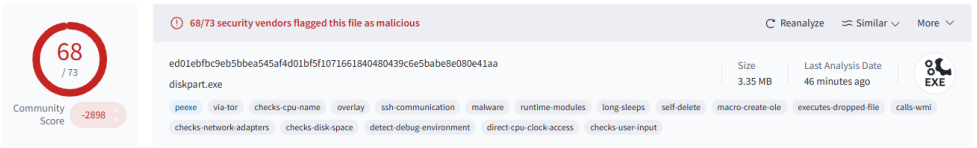
Malwarebytes identified a sample from the Dexter infostealer family as a generic malware threat.



I checked file hashes for each of the malware and put it to VirusTotal.

WannaCry was detected by many anti malware tools.





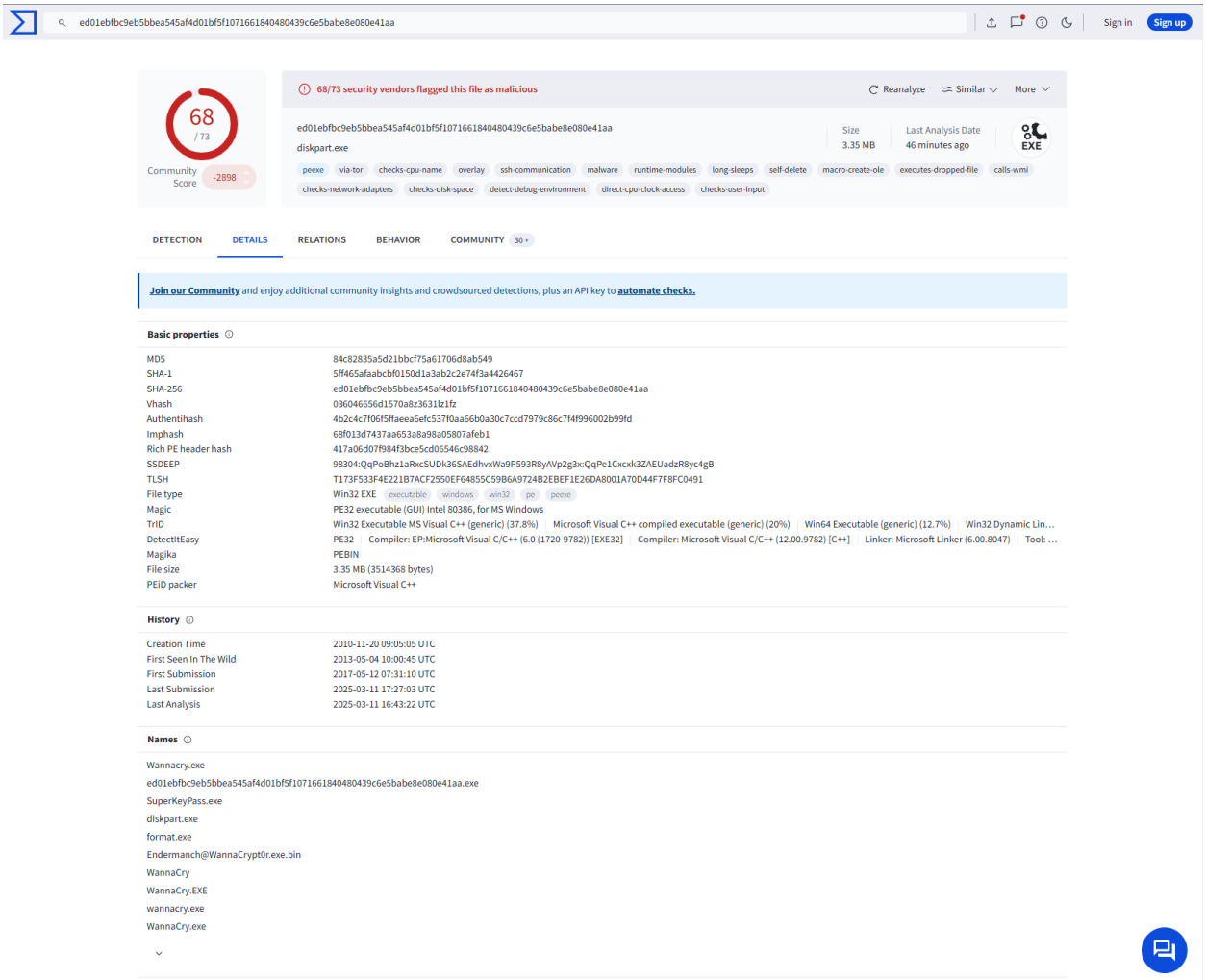
DETECTION DETAILS RELATIONS COMMUNITY

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

Popular threat label ransomware.wannacry/wannacryptor **Threat categories** ransomware trojan **Family labels** wannacry wannacryptor wanna

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.WannaCryptor.R200571	Alibaba	Ransom:Win32/WannaCry.ali1020010
AliCloud	RansomWare	ALYac	Trojan.Ransom.WannaCryptor
Antiy-AVL	Trojan[Ransom]/Win32.Wanna	Arcabit	Trojan.Ransom.WannaCryptor.A
Avast	Win32:WanaCry-A [Trj]	AVG	Win32:WanaCry-A [Trj]
Avira (no cloud)	TR/Ransom.JB	Baidu	Win32.Trojan.WannaCry.c
BitDefender	Trojan.Ransom.WannaCryptor.A	Bkav Pro	W32.Common.74B07FDA
ClamAV	Win.Ransomware.Wannacryptor-994018…	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.ransomware.wannacry	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Encoder.11432	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Ransom.WannaCryptor.A (B)	eScan	Trojan.Ransom.WannaCryptor.A
ESET-NOD32	Win32/Filecoder.WannaCryptor.D	Fortinet	W32/WannaCryptor.6F87!tr.ransom
GData	Win32.Trojan-Ransom.WannaCry.A	Gridinsoft (no cloud)	Malware.Win32.Gen.bot!se54409
Huorong	Ransom/Wannacry.j	Ikarus	Trojan-Ransom.WannaCry
Jiangmin	Trojan.Wanna.eo	K7AntiVirus	Trojan (0050d7171)
K7GW	Trojan (0050d7171)	Kaspersky	Trojan-Ransom.Win32.Wanna.zbu
Kingsoft	Win32.Troj.Undef.a	Lionic	Trojan.Win32.Wanna.toNn
Malwarebytes	Generic.Malware.AI.DDS	MaxSecure	Trojan.Ransom.Wanna.d



Trojan.Bladabindi:

HashMyFiles

File Edit View Options Help

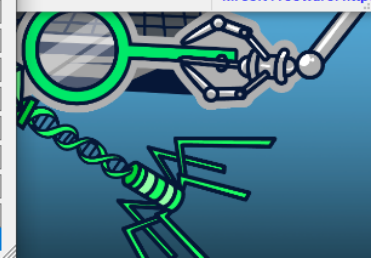
Filename	MD5	SHA-256	File Size	Modified Time
hostr.exe	5a559b6d223c79f3736dc52794636cfd	6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1	107,520	12/10/2013 10:20:53 PM

Properties

Filename:	hostr.exe
MD5:	5a559b6d223c79f3736dc52794636cfd
SHA1:	5c4676b37fcd49990d21960a2df57af72ceef29a
CRC32:	3006edd4
SHA-256:	6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1
SHA-512:	7a12510fe2104a1860bccdd12d96449eb8b02e30f9757bf3fbb4aef3373c710afbaef380ac
SHA-384:	0b53eaa96e75ead888f5b39b675fb9531d38adacc7e001023bb3562f298ef505d7467712
Full Path:	C:\Users\simon\Desktop\theZoo\malware\Binaries\Trojan.Bladabindi\hostr.exe
Modified Time:	12/10/2013 10:20:53 PM
Created Time:	12/11/2014 6:56:24 AM
Entry Modified Time:	3/11/2025 4:03:57 PM
File Size:	107,520
File Version:	0.0.0.0
Product Version:	0.0.0.0
Identical:	
Extension:	exe
File Attributes:	A
Hash Start Time:	3/11/2025 7:22:11 PM
Hash End Time:	3/11/2025 7:22:11 PM
Hashing Duration:	00:00:00.006

OK

NirSoft Freeware. http



6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1

Sign in Sign up

64 / 72

Community Score -93

64/72 security vendors flagged this file as malicious

Reanalyze Similar More

6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1

max.exe

Size 105.00 KB

Last Analysis Date 9 days ago

EXE

peexe direct-cpu-clock-access assembly long-sleeps detect-debug-environment via-tor persistence runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 15+

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

Popular threat label trojan.msil/bladabindi

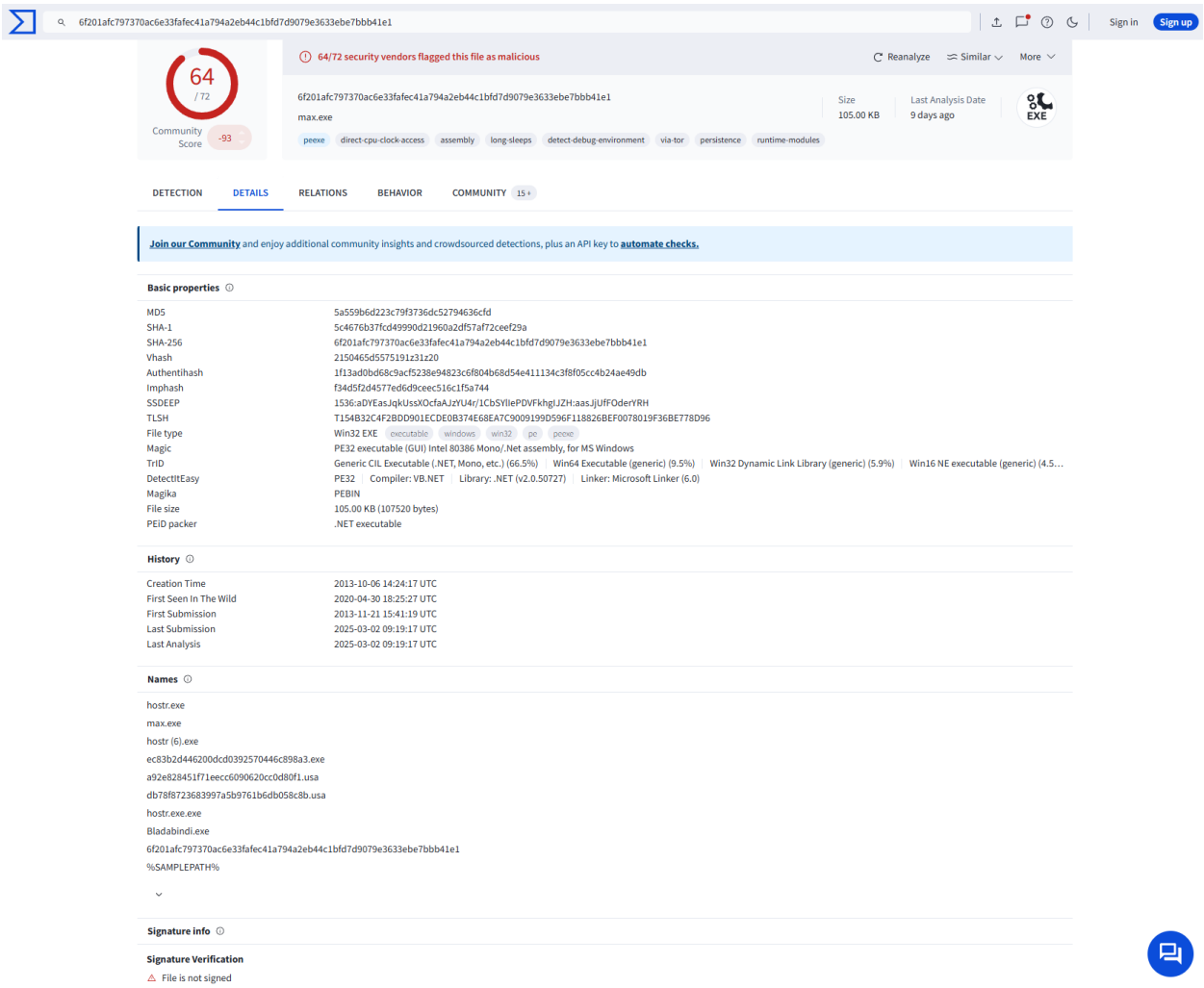
Threat categories trojan

Family labels msil bladabindi msilperseus

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R88176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSILPerseus.25588	Antiy-AVL	Trojan/Win32.Pakes
Arcabit	Trojan.MSILPerseus.D63F4	Avast	Win32:RATX-gen [Trj]
AVG	Win32:RATX-gen [Trj]	Avira (no cloud)	TR/Barys.10755412
BitDefender	Gen:Variant.MSILPerseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan.Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msil	Cylance	Unsafe
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Bifrost.19762
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.MSILPerseus.25588 (B)
eScan	Gen:Variant.MSILPerseus.25588	ESET-NOD32	MSIL/Bladabindi.O
Fortinet	MSIL/Generic.AP.EA844!tr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.ba!s1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingsoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.lLPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LS!5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml



Win32.Infostealer.Dexter:

HashMyFiles

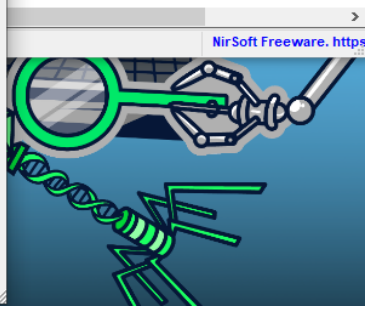
File Edit View Options Help

Filename	MD5	SHA-256	File Size	Modified Time
win33.exe	140d24af0c2b3a18529df12dfbc5f6de	4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92	68,096	9/23/2013 12:13:50 PM

Properties

Filename:	win33.exe
MD5:	140d24af0c2b3a18529df12dfbc5f6de
SHA1:	e8db5ad2b7ffede3e41b9c3adb24f3232d764931
CRC32:	604aca49
SHA-256:	4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
SHA-512:	a2ead649f155555ec3e55800494f833d18cea68afe736807ec23b5991242928a0853e451
SHA-384:	032208310f37895806f4e4fc2daa521f507ddd2c5bef57573460ff6101db2bb4445082f622
Full Path:	C:\Users\simon\Desktop\theZoo\malware\Binaries\Win32.Infostealer.Dexter\win33.exe
Modified Time:	9/23/2013 12:13:50 PM
Created Time:	3/11/2025 4:07:27 PM
Entry Modified Time:	3/11/2025 4:07:27 PM
File Size:	68,096
File Version:	
Product Version:	
Identical:	
Extension:	exe
File Attributes:	A
Hash Start Time:	3/11/2025 7:20:24 PM
Hash End Time:	3/11/2025 7:20:24 PM
Hashing Duration:	00:00:00.000

OK



4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92

Sign in Sign up

66 / 72

Community Score -480

66/72 security vendors flagged this file as malicious

Reanalyze Similar More

4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92

win33.exe

Size 66.50 KB

Last Analysis Date 7 days ago

EXE

peexe checks-user-input malware spreader persistence detect-debug-environment runtime-modules checks-network-adapters via-tor direct-cpu-clock-access

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 23+

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

Popular threat label trojan.dexter/sydg

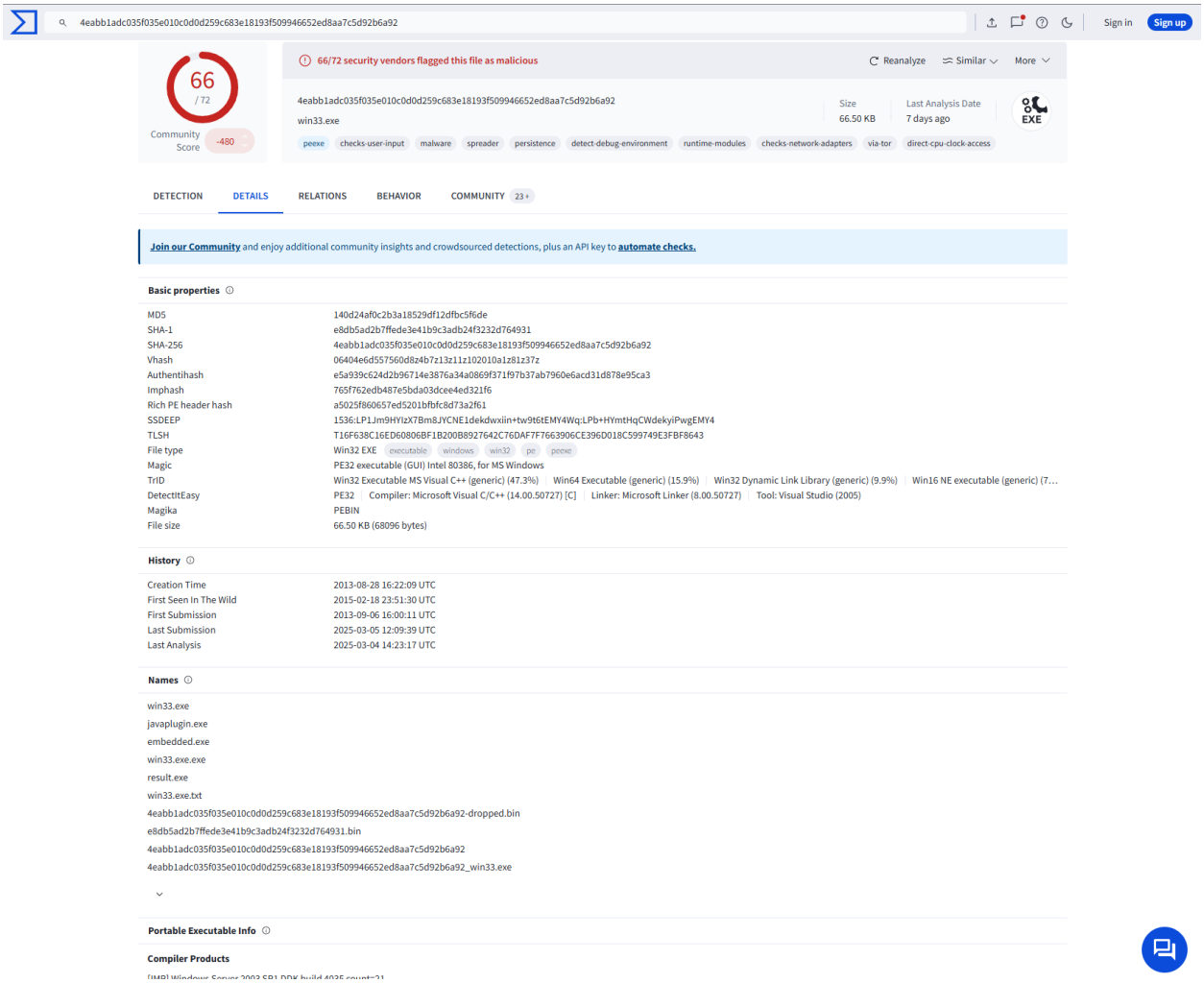
Threat categories trojan

Family labels dexter sydg poxters

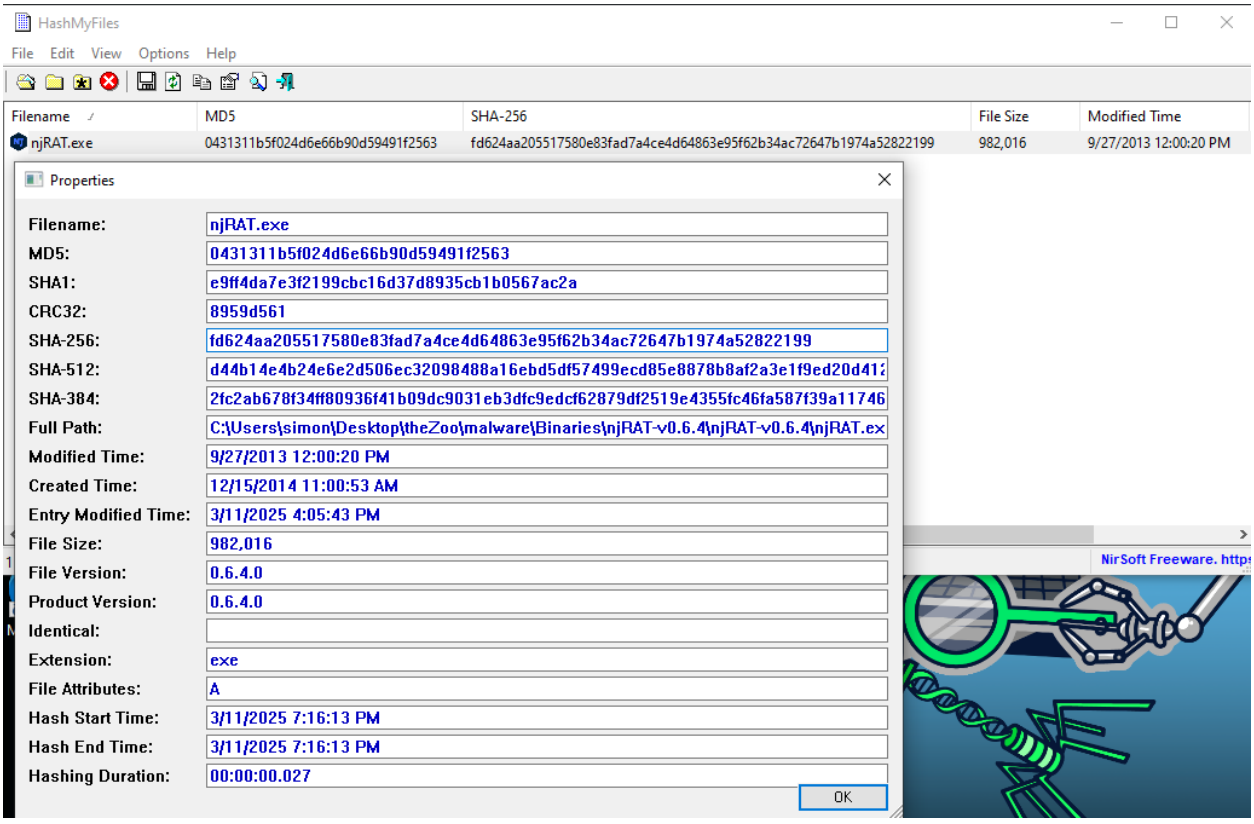
Security vendors' analysis

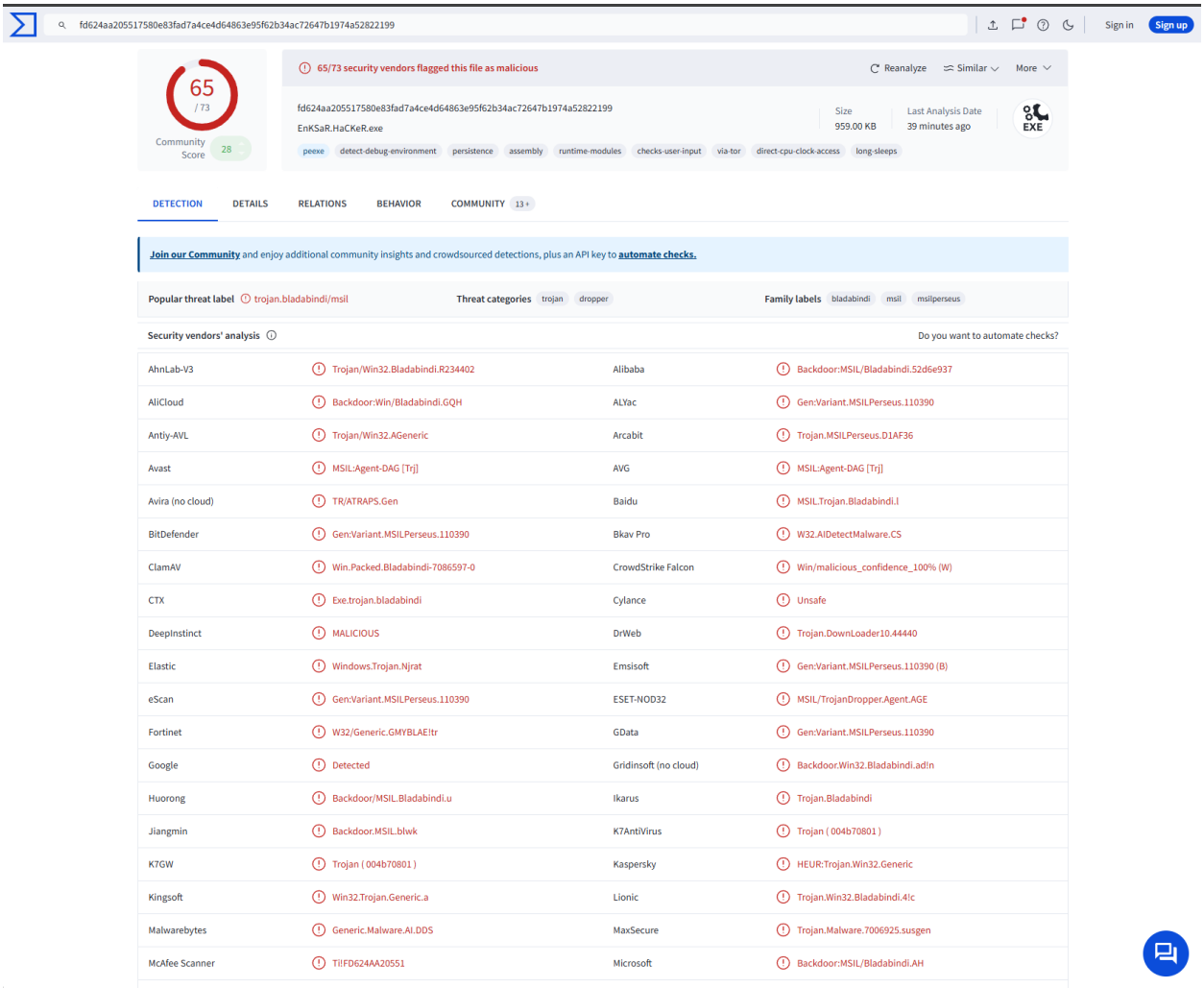
Do you want to automate checks?

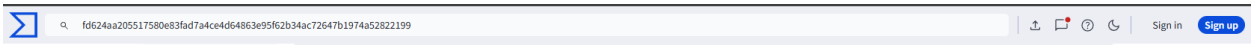
AhnLab-V3	Trojan/Win32.Agent.R66523	Alibaba	TrojanPSW:Win32/Dexter.8c5ba213
AliCloud	Trojan:Win/Agent!AID.JBCM	ALYac	Spyware.Infostealer.Dexter
Antiy-AVL	Trojan/Win32.Invader	Arcabit	Generic.Malware.SYdg.D7A4AFFF
Avast	Win32:Dexter-I [Trj]	AVG	Win32:Dexter-I [Trj]
Avira (no cloud)	TR/Hijacker.Gen	BitDefender	Dropped:Generic.Malware.SYdg.1956AFFF
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Malware.Dexter-9654223-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.dexter
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Packed.21724
Elastic	Malicious (high Confidence)	Emsisoft	Dropped:Generic.Malware.SYdg.1956AF…
eScan	Dropped:Generic.Malware.SYdg.1956AFFF	ESET-NOD32	A Variant Of Win32/Poxters.E
Fortinet	W32/Poxters.E!tr	GData	Dropped:Generic.Malware.SYdg.1956AFFF
Google	Detected	Gridinsoft (no cloud)	PWS.Win32.Dexter.cc!s3
Huorong	Trojan/Agent.aid	Ikarus	Trojan.Win32.Poxters
Jiangmin	Trojan/Pincav.scs	K7AntiVirus	Trojan (004b9fa61)
K7GW	Trojan (004b9fa61)	Kaspersky	HEUR:Trojan.Win32.Generic
Kingsoft	Win32.Trojan.Generic.a	Lionic	Trojan.Win32.Generic.IVqc
Malwarebytes	Generic.Malware.AI.DDS	McAfee Scanner	Real Protect-LS!140D24AF0C2B
Microsoft	PWS:Win32/Dexter.A	NANO-Antivirus	Trojan.Win32.Hijacker.ftgjac


4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
Sign in
Sign up
66
/ 72
Community Score
-480
66/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
win33.exe
Size
66.50 KB
Last Analysis Date
7 days ago
EXE
peexe
checks-user-input
malware
spreader
persistence
detect-debug-environment
runtime-modules
checks-network-adapters
via-tor
direct-cpu-clock-access
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 23+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 140d24af0c2b3a18529df12dfbc5f6de
SHA-1 e8db5ad2b7ffede3e41b9c3adb24f3232d764931
SHA-256 4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
Vhash 06404e6d557560d8z4b7z13z11z102010a1z81z37z
Authentihash e5a939c624d2b96714e3876a34a0869f371f97b37ab7960e6acd31d878e95ca3
Imphash 765f762edb487e5bda03dcee4ed321f6
Rich PE header hash a5025f860657ed5201bfbfc8d73a2f61
SSDEEP 1536:LP1Jm9HYIzX7Bm8JYCNE1dekdwxiin+tw9t6tEMY4Wq:LPb+HYmtHqCWdekyiPwgEMY4
TLSH T16F638C16ED60806BF1B200B8927642C76DAF7F7663906CE396D018C599749E3FBF8643
File type Win32 EXE executable windows win32 pe peexe
Magic PE32 executable (GUI) Intel 80386, for MS Windows
TrID Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (7…
DetectItEasy PE32 Compiler: Microsoft Visual C/C++ (14.00.50727) [C] Linker: Microsoft Linker (8.00.50727) Tool: Visual Studio (2005)
Magika PEBIN
File size 66.50 KB (68096 bytes)
History
Creation Time 2013-08-28 16:22:09 UTC
First Seen In The Wild 2015-02-18 23:51:30 UTC
First Submission 2013-09-06 16:00:11 UTC
Last Submission 2025-03-05 12:09:39 UTC
Last Analysis 2025-03-04 14:23:17 UTC
Names
win33.exe
javaplugin.exe
embedded.exe
win33.exe.exe
result.exe
win33.exe.txt
4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92-dropped.bin
e8db5ad2b7ffede3e41b9c3adb24f3232d764931.bin
4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92_win33.exe
Portable Executable Info
Compiler Products

njRAT:


HashMyFiles
File Edit View Options Help
Filename MD5 SHA-256 File Size Modified Time
njRAT.exe 0431311b5f024d6e66b90d59491f2563 fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199 982,016 9/27/2013 12:00:20 PM
Properties
Filename: njRAT.exe
MD5: 0431311b5f024d6e66b90d59491f2563
SHA1: e9ff4da7e3f2199cbc16d37d8935cb1b0567ac2a
CRC32: 8959d561
SHA-256: fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199
SHA-512: d44b14e4b24e6e2d506ec32098488a16ebd5df57499ecd85e8878b8af2a3e1f9ed20d41
SHA-384: 2fc2ab678f34ff80936f41b09dc9031eb3dfc9edcf62879df2519e4355fc46fa587f39a11746
Full Path: C:\Users\simon\Desktop\theZoo\malware\Binaries\njRAT-v0.6.4\njRAT-v0.6.4\njRAT.ex
Modified Time: 9/27/2013 12:00:20 PM
Created Time: 12/15/2014 11:00:53 AM
Entry Modified Time: 3/11/2025 4:05:43 PM
File Size: 982,016
File Version: 0.6.4.0
Product Version: 0.6.4.0
Identical:
Extension: exe
File Attributes: A
Hash Start Time: 3/11/2025 7:16:13 PM
Hash End Time: 3/11/2025 7:16:13 PM
Hashing Duration: 00:00:00.027
OK
NirSoft Freeware. http


fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199
Sign in
Sign up
65
/ 73
Community Score
28
65/73 security vendors flagged this file as malicious
Reanalyze
Similar
More
fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199
EnKSaR.HaCKeR.exe
peexe
detect-debug-environment
persistence
assembly
runtime-modules
checks-user-input
via-tor
direct-cpu-clock-access
long-sleeps
Size
959.00 KB
Last Analysis Date
39 minutes ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 13+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.bladabindi/msil
Threat categories trojan dropper
Family labels bladabindi msil msilperseus
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Trojan/Win32.Bladabindi.R234402
Alibaba Backdoor:MSIL/Bladabindi.52d6e937
AliCloud Backdoor:Win/Bladabindi.GQH
ALYac Gen:Variant.MSILPerseus.110390
Antiy-AVL Trojan/Win32.AGeneric
Arcabit Trojan.MSILPerseus.D1AF36
Avast MSIL:Agent-DAG [Trj]
AVG MSIL:Agent-DAG [Trj]
Avira (no cloud) TR/ATRAPS.Gen
Baidu MSIL.Trojan.Bladabindi.l
BitDefender Gen:Variant.MSILPerseus.110390
Bkav Pro W32.AIDetectMalware.CS
ClamAV Win.Packed.Bladabindi-7086597-0
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.bladabindi
Cylance Unsafe
DeepInstinct MALICIOUS
DrWeb Trojan.DownLoader10.44440
Elastic Windows.Trojan.Njrat
Emsisoft Gen:Variant.MSILPerseus.110390 (B)
eScan Gen:Variant.MSILPerseus.110390
ESET-NOD32 MSIL/TrojanDropper.Agent.AGE
Fortinet W32/Generic.GMYBLA!tr
GData Gen:Variant.MSILPerseus.110390
Google Detected
Gridinsoft (no cloud) Backdoor.Win32.Bladabindi.ad!n
Huorong Backdoor/MSIL.Bladabindi.u
Ikarus Trojan.Bladabindi
Jiangmin Backdoor.MSIL.blwk
K7AntiVirus Trojan (004b70801)
K7GW Trojan (004b70801)
Kaspersky HEUR:Trojan.Win32.Generic
Kingsoft Win32.Trojan.Generic.a
Lionic Trojan.Win32.Bladabindi.4!c
Malwarebytes Generic.Malware.AI.DDS
MaxSecure Trojan.Malware.7006925.susgen
McAfee Scanner Ti!FD624AA20551
Microsoft Backdoor:MSIL/Bladabindi.AH



65 / 73

Community Score 28

65/73 security vendors flagged this file as malicious

Reanalyze Similar More

fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199

EnKSaR.HaCKeR.exe

Size 959.00 KB

Last Analysis Date 59 minutes ago

EXE

peexe detect-debug-environment persistence assembly runtime-modules checks-user-input via-tor direct-cpu-clock-access long-sleeps

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13+

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

Basic properties

MD5	0431311b5f024d6e66b90d59491f2563
SHA-1	e9ff4da7e3f2199cbc16d37d8935cb1b0567ac2a
SHA-256	fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199
Vhash	2950465d15151ff0101fc3952314100
Authentihash	d6fdee461f0fecbe955f1cd6d5b1453c3c687876de8033be739927f86f09bfc4
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	12288:+O9vE3J7JO+xEPuc//9wivAmv6SAbnzmip2hGnadIFM4ZHOT2:+eXuczPCSGnzVjad1
TLSH	T1D4252A233744FC28C03971F6A0858FD481A24F1E95B645F925B173BAF5FA6C2AC4A3D9
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Generic CIL Executable (.NET, Mono, etc.) (51.8%) | Win32 Executable MS Visual C++ (generic) (22.1%) | Win64 Executable (generic) (7.4%) | Win32 Dynamic Link Library (…
DetectItEasy	PE32 | Protector: Eazfuscator | Compiler: VB.NET | Library: .NET (v4.0.30319) | Linker: Microsoft Linker (11.0)
Magika	PEBIN
File size	959.00 KB (982016 bytes)
PEiD packer	.NET executable

History

Creation Time	2013-09-27 08:00:20 UTC
First Seen In The Wild	2013-09-27 08:00:20 UTC
First Submission	2013-10-27 11:15:27 UTC
Last Submission	2025-03-07 17:52:28 UTC
Last Analysis	2025-03-11 16:38:39 UTC

Names

EnKSaR.HaCKeR.exe
njRAT.exe
njRAT.exe.v
njRAT.bin
PIG Nobulink 1 June 2024.exe
qq.exe
njRATexe.exe
fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199.rat
fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199.exe
RegClear.exe

Signature info

Signature Verification

⚠ File is not signed

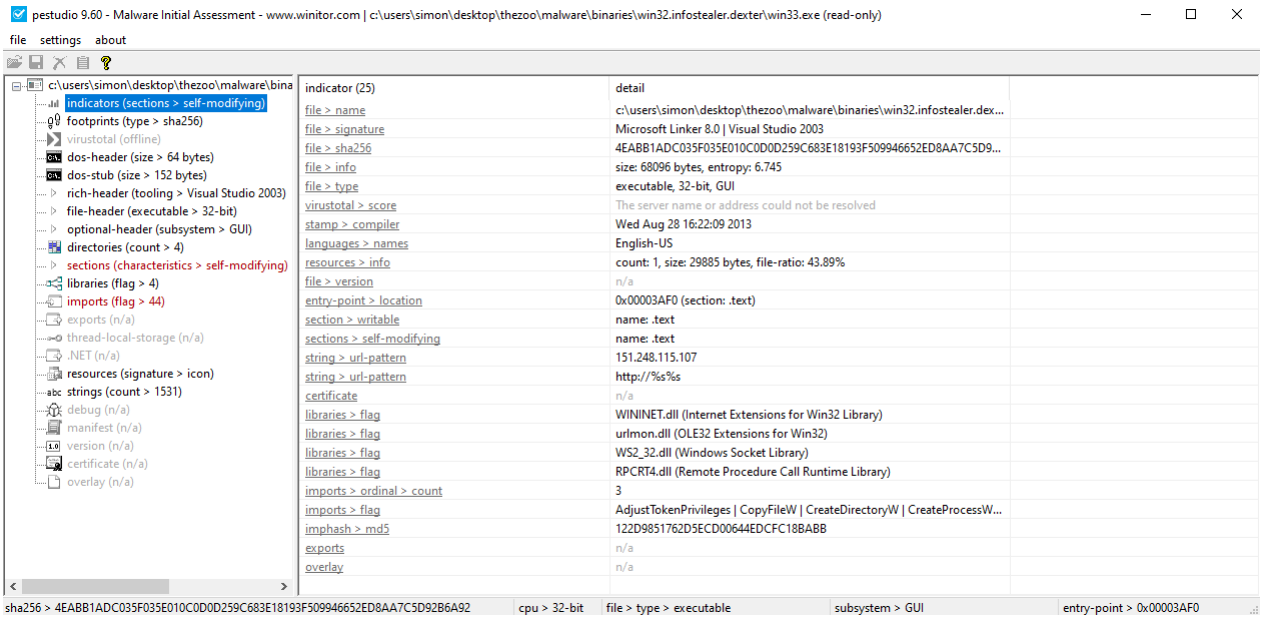
The analysis of malware samples using UVK, Malwarebytes, and VirusTotal revealed differences in detection capabilities and methodologies – each tool employs a distinct approach, because UVK focuses on runtime behavior (when malware is executed), Malwarebytes relies on signature and scanning, while VirusTotal combines detections from multiple antivirus engines based on file hashes – these variations resulted in different detection outcomes, emphasizing the need for a multi-faceted approach when analyzing malware.

UVK used during malware execution, did not assign threat levels but successfully identified new processes and memory modules spawned by each malware sample – this confirms that the malware was actively running, modifying system memory and potentially interacting with the operating system, however, since UVK does not classify threats or detects it, it does not provide information on the malware's type or severity. Instead, it is useful for observing real-time system modifications caused by the executed malware.

Malwarebytes detected the malware samples and classified them. The results often identified the files with generic names, such as Generic.Malware.AI.DDS, Trojan, or Backdoor.Bot.DDS. This suggests that Malwarebytes relies on known malware signatures but also employs machine learning techniques for unknown threats. Malware bytes can identify malicious files, however it does not provide deeper insights into the malware's behavior unless executed.

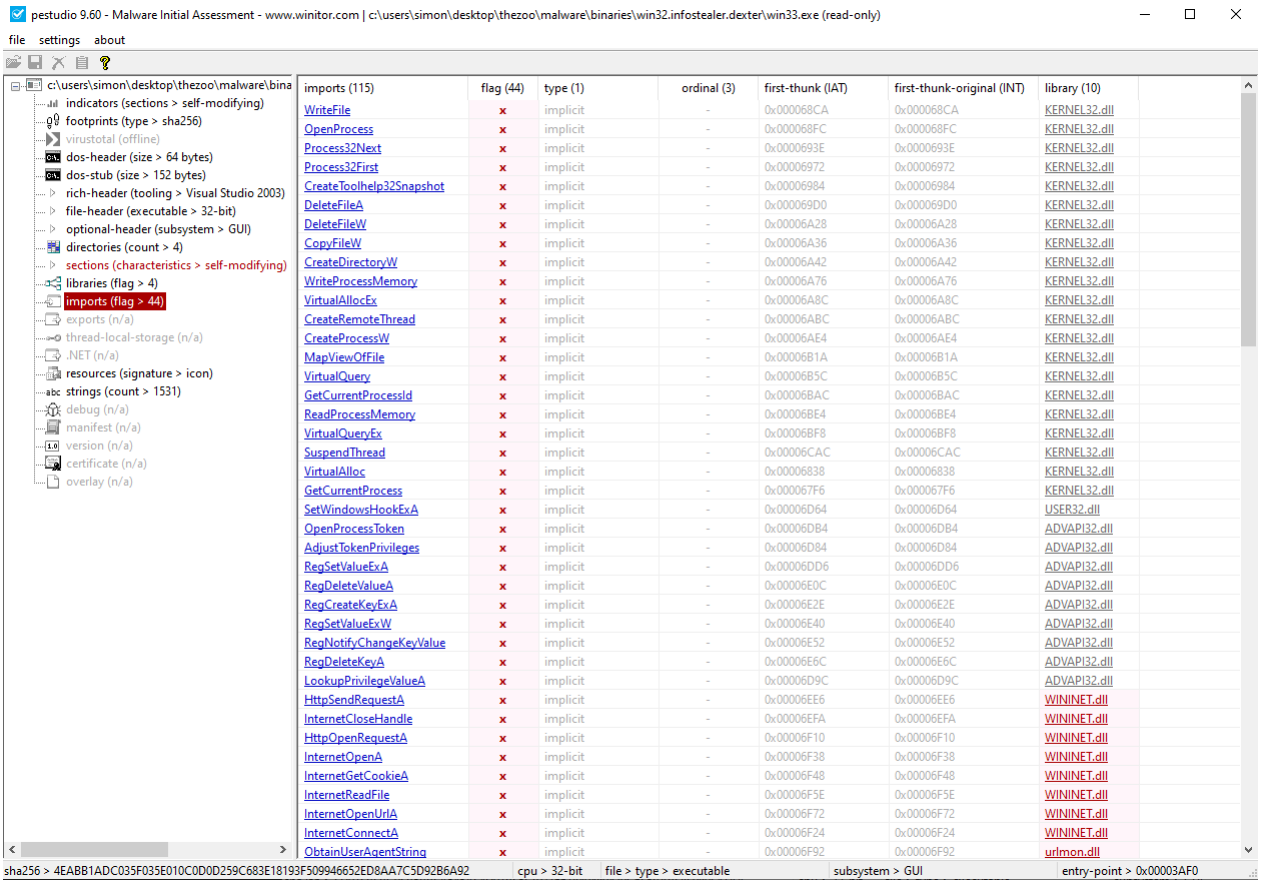
VirusTotal produced the most extensive classification of malware. It checked file hashes against multiple antivirus databases. Since VirusTotal relies entirely on previously known file hashes, it excels in identifying widely distributed malware but may provide limited results for modified, obfuscated, or newly compiled samples. Also, the detection rate varied between samples, with most being recognized by a majority of AV vendors, confirming that the analyzed samples were well-documented threats.

Static analysis of win33.exe (Win32.Infostealer.Dexter) using PeStudio revealed multiple characteristics indicative of malicious behavior. The tool flagged the executable as self-modifying, which suggests that the file has the capability to alter its own structure at runtime to avoid being detected. Absence of a digital signature further supports the likelihood that this is an unauthorized or malicious executable. Since the system was offline, PeStudio was unable to retrieve VirusTotal results, preventing immediate confirmation from external databases.

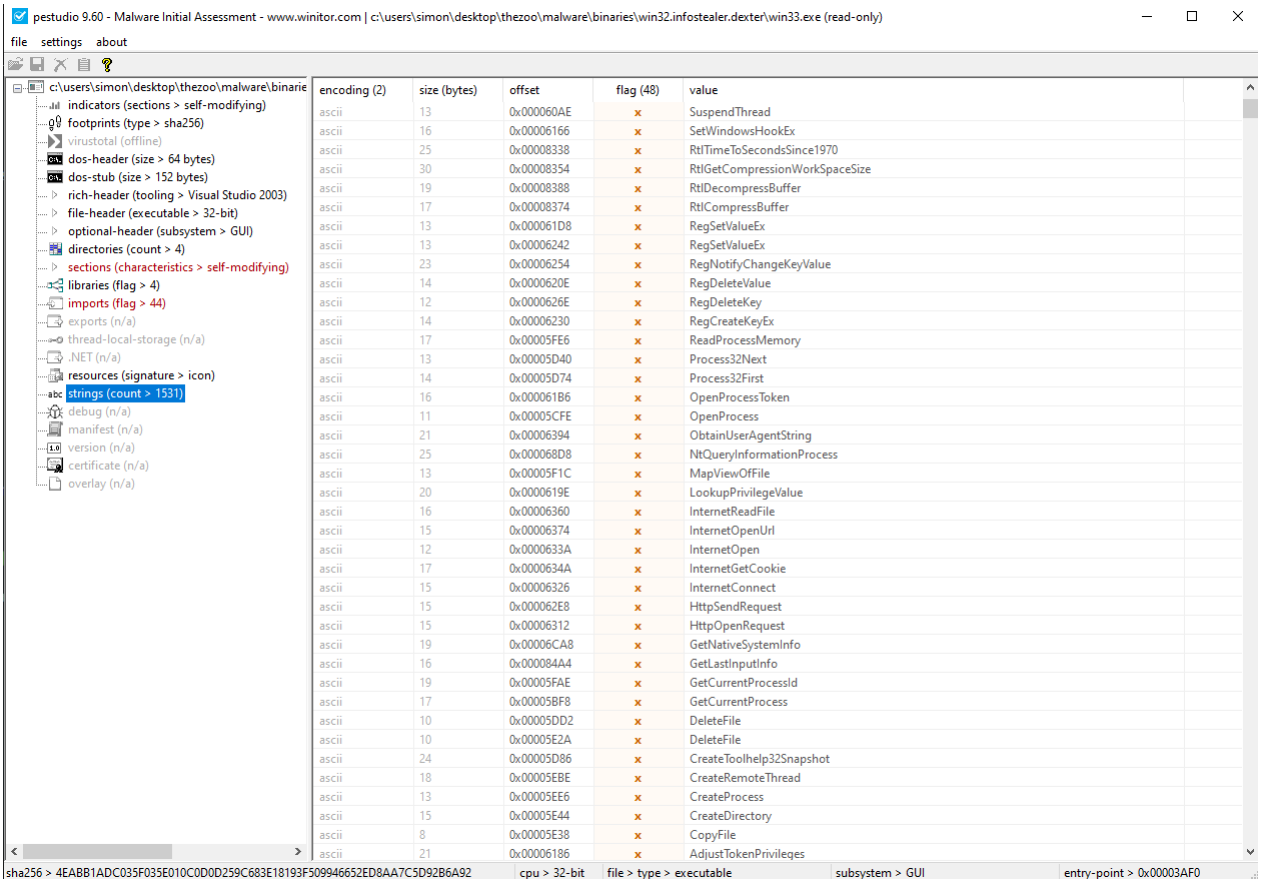


A look into the imported API functions provides insight into the malware's potential capabilities. Functions like VirtualAllocEx (https://learn.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtualallocex), CreateRemoteThread (https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createremotethread), and WriteProcessMemory (https://learn.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-writeprocessmemory) indicate that the malware can manipulate other processes, likely for injection purposes. Calls to AdjustTokenPrivileges (https://learn.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-adjusttokenprivileges), SetWindowsHookEx (https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-setwindowshookexa), and CreateProcessW (https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessw) suggest that it may attempt to escalate privileges or establish persistence. The presence of networking-related functions such as InternetOpenA (https://learn.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopena), HttpSendRequestA (https://learn.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-httpsendrequesta), and InternetConnect (https://learn.microsoft.com/en-us/previous-versions/windows/embedded/ms918351(v=msdn.10)) confirms that the malware is designed to communicate with external servers, potentially exfiltrating stolen data. Additionally, functions like DeleteFileW (https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-deletefilew), CopyFileW (https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-copyfilew), RegCreateKeyEx (https://help.intervalzero.com/product_help/RTX64_4/Content/Topics/SDK/RtRegistryAPIs/Reg

CreateKeyEx.htm), and RegSetValueEx (https://learn.microsoft.com/en-us/previous-versions/ms942534(v=msdn.10)) show that the malware is capable of modifying system files and registry entries, reinforcing its potential to establish persistence and alter system configurations.



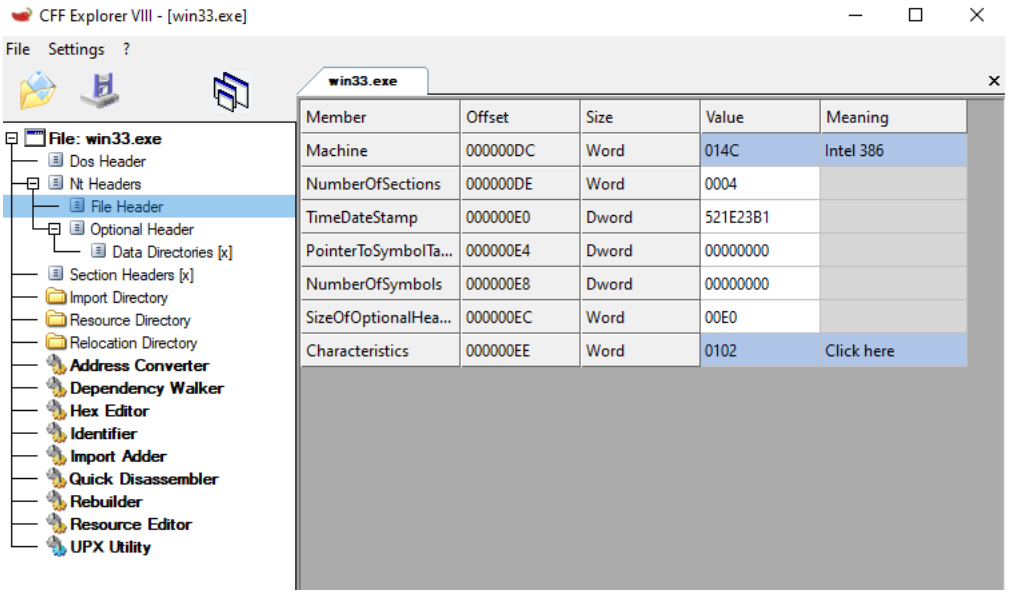
An examination of embedded strings within the executable further tells about its malicious intent – the file contains over 1500 embedded strings, many of which include HTTP requests and network-related instructions, suggesting that the malware is programmed to send or retrieve data from remote sources. Also, several registry modification commands appear in the strings, which aligns with its potential ability to alter system settings for persistence. Additionally, references to file system and process management functions indicate that the malware may engage in data theft, execution of additional payloads, or manipulation of system components to evade detection.



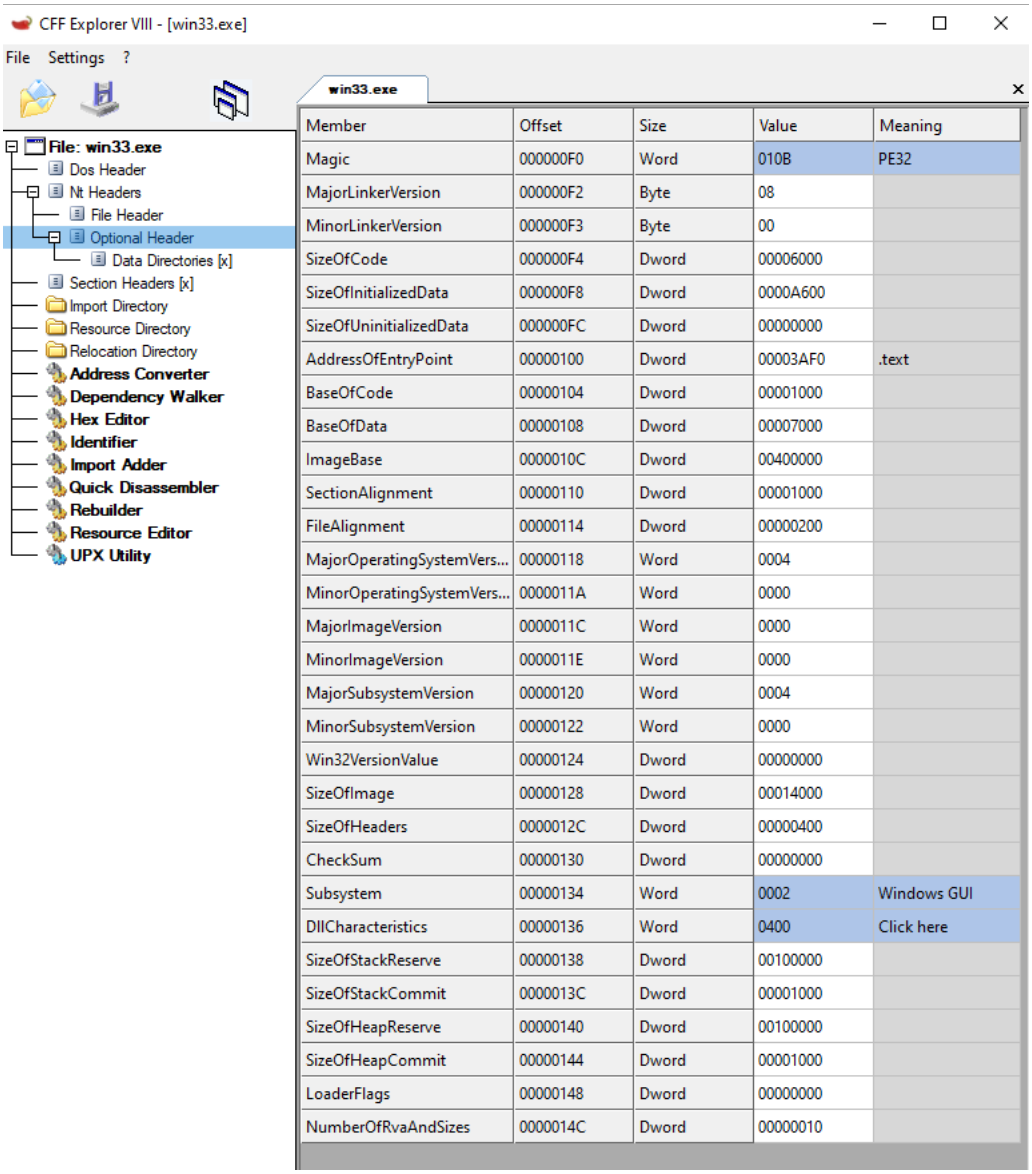
The results of this manual analysis confirm that Win32.Infostealer.Dexter is structured to perform credential theft, interact with external servers, and modify system behavior for persistence. Its API imports and embedded strings suggest that it could be part of a larger malware campaign targeting sensitive user information.

The win33.exe sample was analyzed using CFF Explorer to examine its PE structure, including headers, sections, and imported libraries. This analysis provides insights into the executable's architecture, entry point, and potential indicators of malicious intent.

File Headers reveal that the executable is a 32-bit PE file, compiled for the Intel 386 architecture. The TimeDateStamp value (0x521E23B1) corresponds to August 28, 2013, which suggests that the binary has not been altered since that time, however, timestamps can be manually modified by malware authors to mislead analysis. The characteristics field indicates that this is a standard executable file.

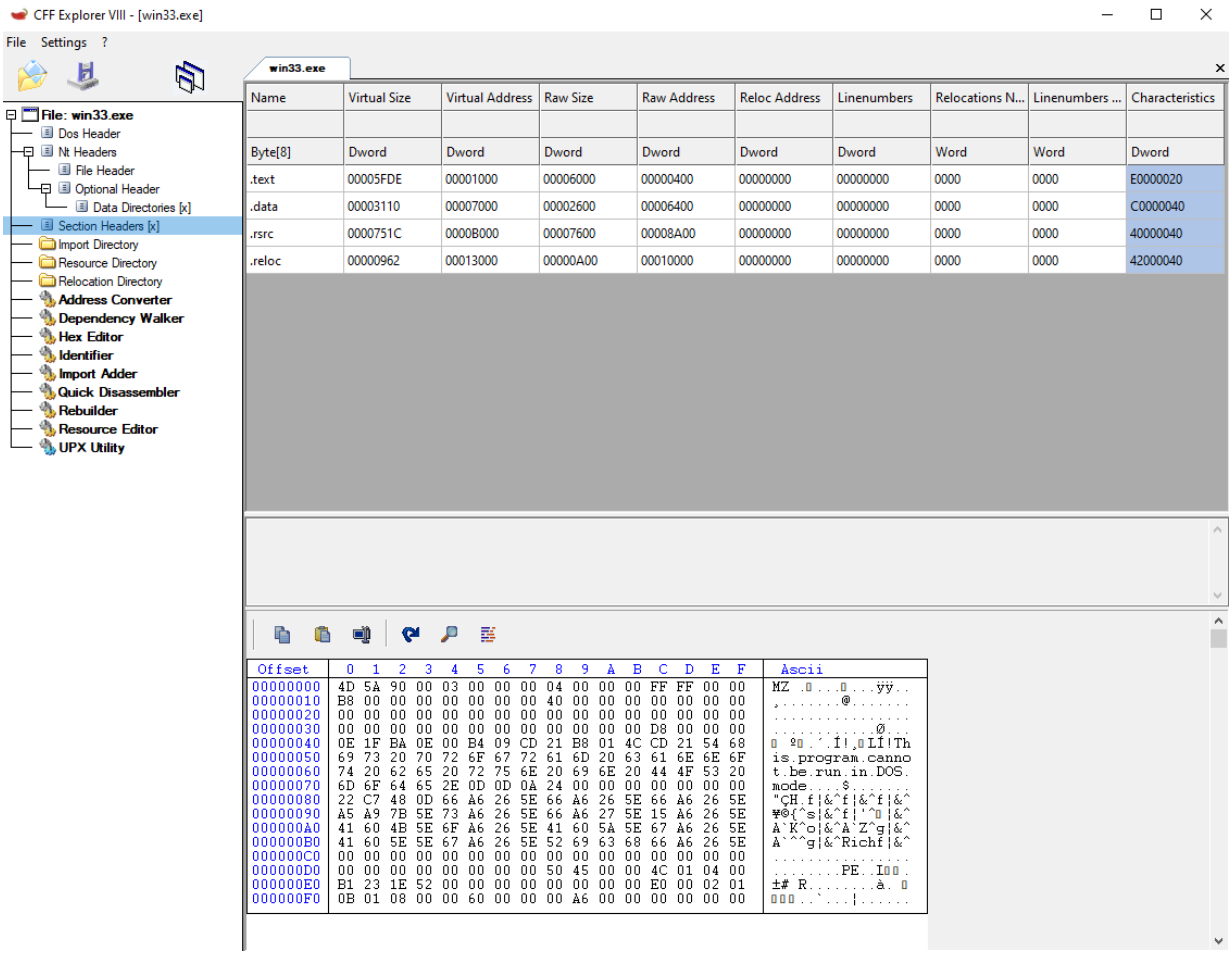


Optional Header provides additional metadata, including the Address of Entry Point (0x00003AF0), which is the location where execution begins. The Subsystem value (0x0002) confirms that this is a Windows GUI application.

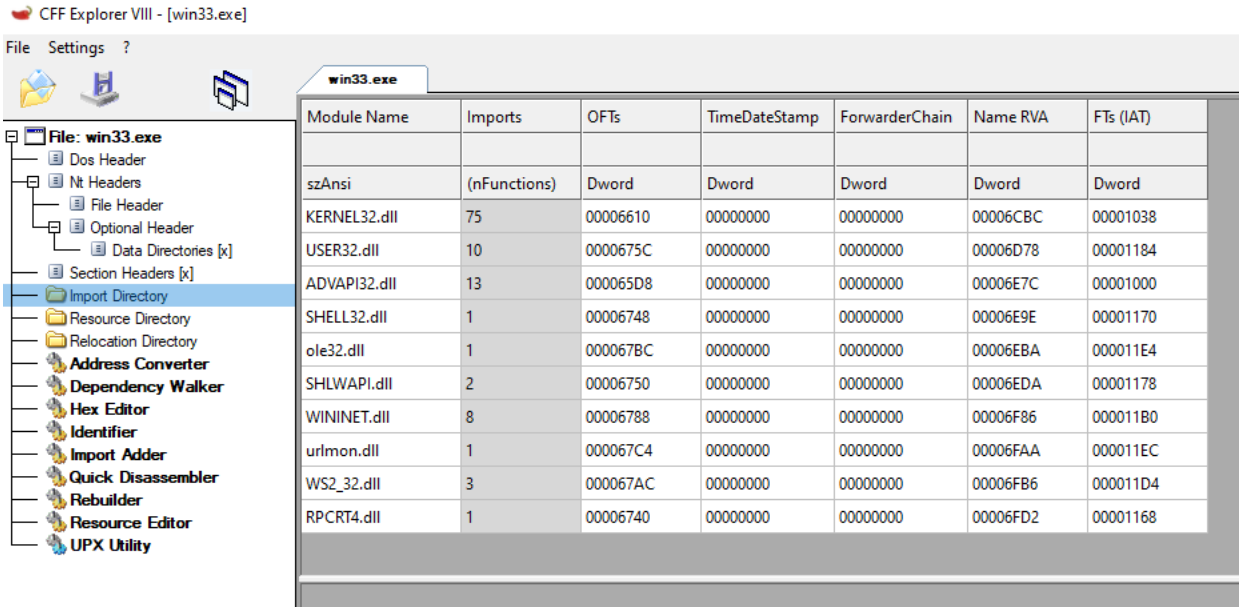


Member	Offset	Size	Value	Meaning
Magic	000000F0	Word	010B	PE32
MajorLinkerVersion	000000F2	Byte	08	
MinorLinkerVersion	000000F3	Byte	00	
SizeOfCode	000000F4	Dword	00006000	
SizeOfInitializedData	000000F8	Dword	0000A600	
SizeOfUninitializedData	000000FC	Dword	00000000	
AddressOfEntryPoint	00000100	Dword	00003AF0	.text
BaseOfCode	00000104	Dword	00001000	
BaseOfData	00000108	Dword	00007000	
ImageBase	0000010C	Dword	00400000	
SectionAlignment	00000110	Dword	00001000	
FileAlignment	00000114	Dword	00000200	
MajorOperatingSystemVers...	00000118	Word	0004	
MinorOperatingSystemVers...	0000011A	Word	0000	
MajorImageVersion	0000011C	Word	0000	
MinorImageVersion	0000011E	Word	0000	
MajorSubsystemVersion	00000120	Word	0004	
MinorSubsystemVersion	00000122	Word	0000	
Win32VersionValue	00000124	Dword	00000000	
SizeOfImage	00000128	Dword	00014000	
SizeOfHeaders	0000012C	Dword	00000400	
CheckSum	00000130	Dword	00000000	
Subsystem	00000134	Word	0002	Windows GUI
DllCharacteristics	00000136	Word	0400	Click here
SizeOfStackReserve	00000138	Dword	00100000	
SizeOfStackCommit	0000013C	Dword	00001000	
SizeOfHeapReserve	00000140	Dword	00100000	
SizeOfHeapCommit	00000144	Dword	00001000	
LoaderFlags	00000148	Dword	00000000	
NumberOfRvaAndSizes	0000014C	Dword	00000010	

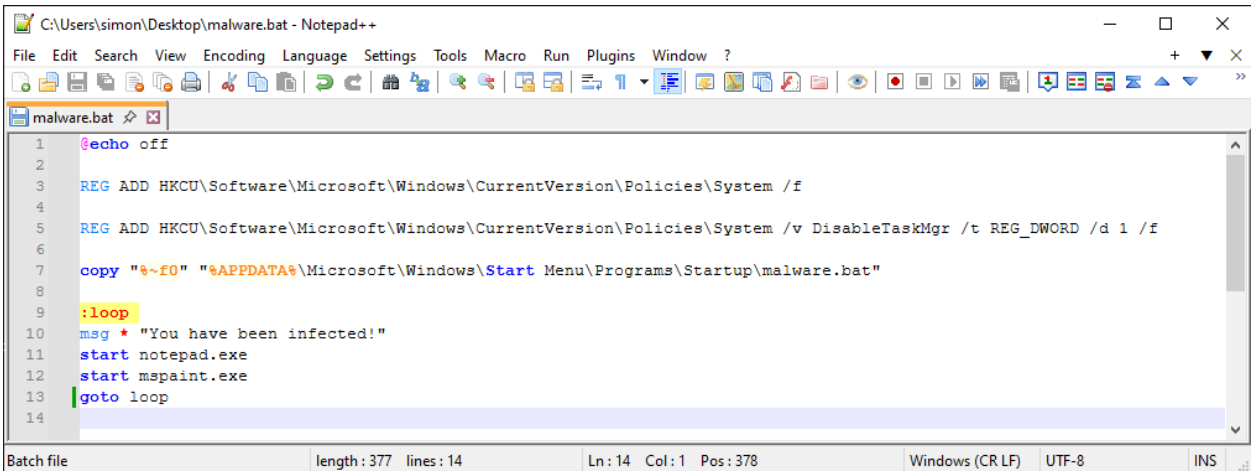
Examining the Section Headers, the executable contains standard PE sections, including .text, .data, .rdata, and .reloc. The .text section is marked as executable (E0000020), meaning it contains the program's core instructions.

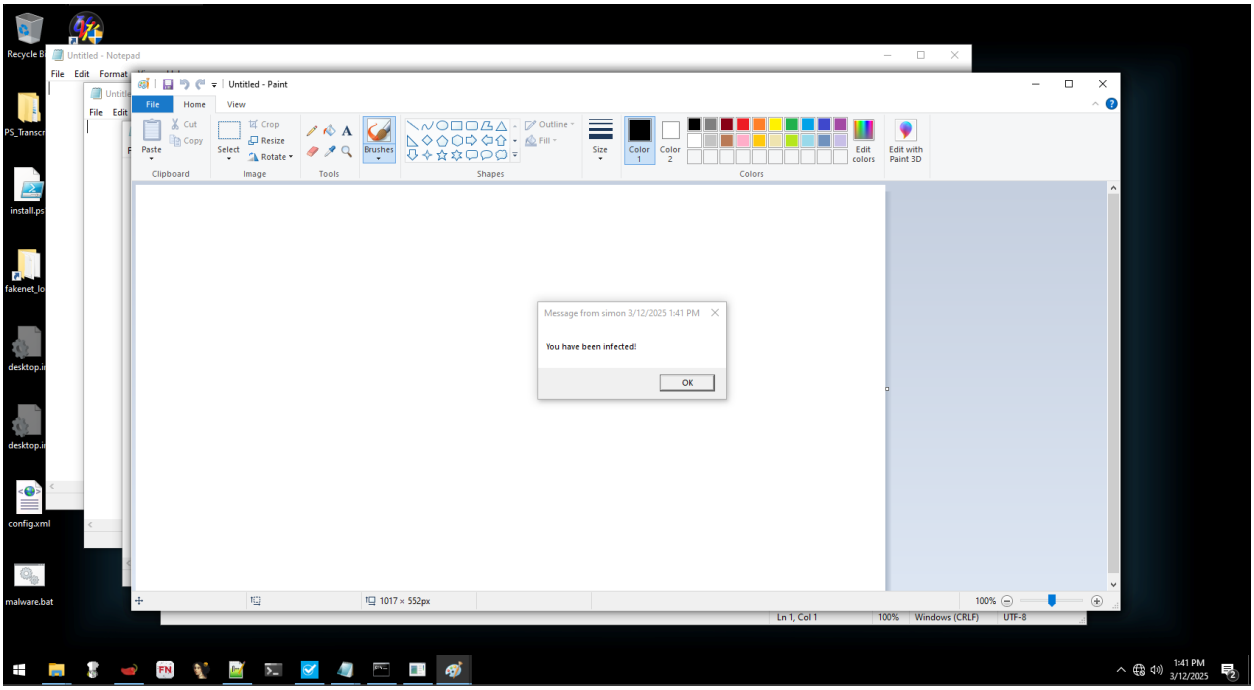


The Import Directory lists DLLs that the malware interacts with – the presence of KERNEL32.dll, USER32.dll, WININET.dll, WS2_32.dll, and ADVAPI32.dll indicates that the executable interacts with system processes, manages user input, and establishes network connections. The inclusion of WININET.dll (https://learn.microsoft.com/en-us/windows/win32/wininet/about-wininet) suggests the malware may perform HTTP-based communication.

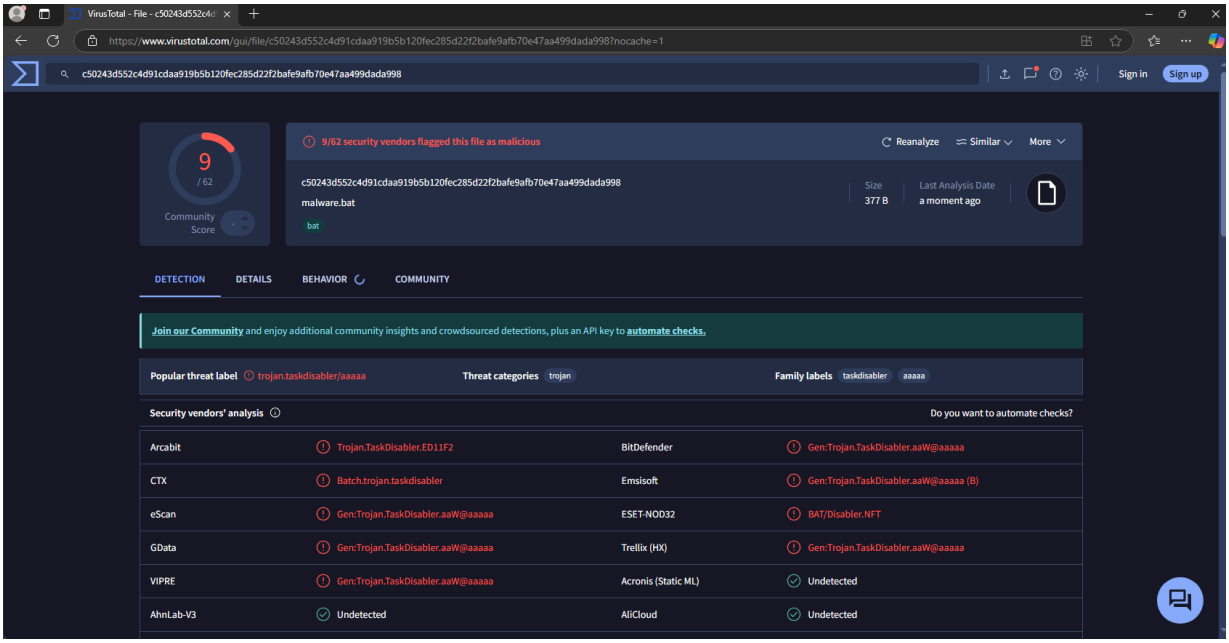


I created malware.bat file which adds to regedit settings to disable task manager https://winaero.com/how-to-disable-task-manager-in-windows-10/ (to prevent it being disconnected), also it would start to startup and that would spam pop-ups, that the user is infected and would open up Notepad and MS Paint many times (in the loop).





I checked it with VirusTotal and 9 security vendors flagged this file as malicious. It identified as Trojan TaskDisabler.



Then I tried obfuscation techniques and ran it again via VirusTotal. It gave result that no security vendor flagged this file as malicious.