Rafael Angelo Christianto

njRAT-v0.6.4
DYNAMIC MALWARE ANALYSIS WITH WINDOWS 10 + FLARE VM

Introduction

From this project of malware analysis, I get to know in more detail how malware infects systems, hides, steals data, and persists. This can come in crucial especially for incident response, this project lets me understand the malware and its capabilities to the system. I will be able to spot suspicious APIs, abnormal system behaviour, suspicious strings, and I will be quick to identify threats. This can be useful for further projects like YARA/SIEM detections, and improve IDS tools by real malware behaviour.

I will be demonstrating and doing the malware analysis only on a safe isolated virtual machine. Why virtual machines are used:

- Isolation: VMs provide an isolated environment, preventing the malware from infecting the host computer or the network.
- Snapshots: i can create a snapshot of the VM before running the malware and revert to that clean state after the analysis is complete.
- Disable shared folders to ensure the malware is prevented from intervening with my host system’s file system
- Disable clipboard and drag’n’drop to prevent data exfiltration from the VM to the host since many malware abuses clipboard
- The network should be Host-Only set in the virtual machine settings to let it not go out to the network I am connected to. Therefore, also meaning the malware I choose is better to not have any network level interactions, since there will be no signal inside the virtual machine.

The files being used in this malware analysis project such as the TXT files, procmon files, procexp files, PCAP file, since it is coming from a VM with actual malware, and spreading them would spread the malware too.

Rafael Angelo Christianto

Methodology

For the sample of virus that I will be analyzing in this project, I will be taking it TheZoo. The zoo contains live malware samples with source code. I will be picking the binaries type since it is best for dynamic malware analysis and I will be analyzing the njRAT-v0.6.4 malware, which can be found and downloaded through the link below:
https://github.com/ytisf/theZoo/tree/master/malware/Binaries/njRAT-v0.6.4
We only need to take the zip file containing the live malware sample, the others are:

- njRAT-v0.6.4.pass which contains the password when unzipping the zip file, but usually the same for all theZoo malware samples, which is "infected".
- njRAT-v0.6.4.md5 is a file used for checking file integrity with hashing with md5, not an executable
- njRAT-v0.6.4.sha256 is just another hash value used for stronger integrity check with sha256

I first downloaded Windows 10 ISO and loaded it as a virtual machine in Virtual Box, and did the initial settings. Then I will choose to use FlareVM, which is a Windows-based security distribution created by Mandiant, and automatically install 300 malware tools. It is available to download from GitHub. It will come with these following tools:

- ProcMon
- Wireshark
- Process Explorer
- Autoruns
- x64dbg
- Ghidra
- IDA Free
- FakeNet-NG
- Regshot
- PE-sieve
- Capa

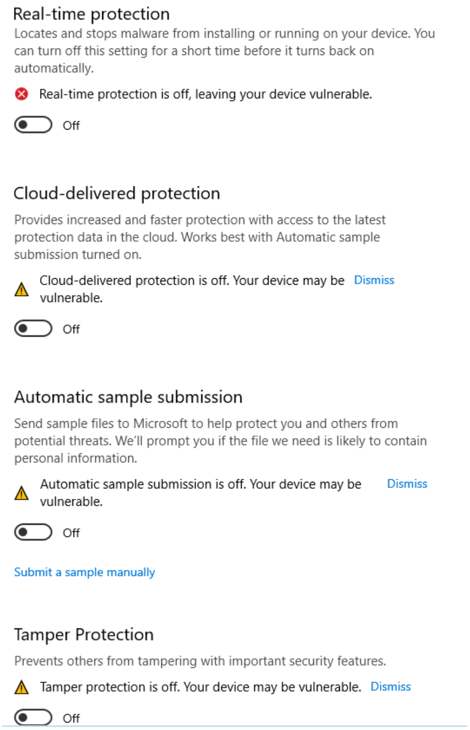
It also configures:

- Firewall rules

- System hardening for safe malware testing
- PATH shortcuts for all tools

The Setup

The first setup is to disable real-time protection and Firewalls that would stop the Malware from being run.



Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

✖ Real-time protection is off, leaving your device vulnerable.

○ Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

⚠ Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

○ Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

⚠ Automatic sample submission is off. Your device may be vulnerable. Dismiss

○ Off

Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

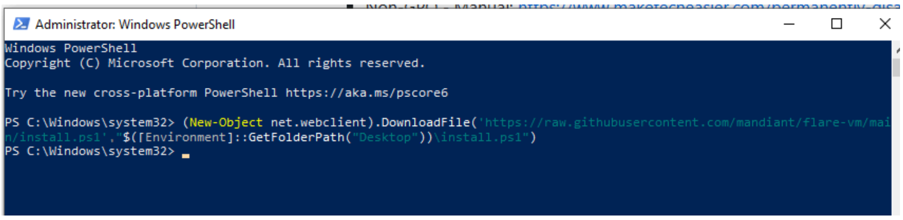
⚠ Tamper protection is off. Your device may be vulnerable. Dismiss

○ Off

After that, given the instructions from the official GitHub repository of the FlareVM, which the link is given below:

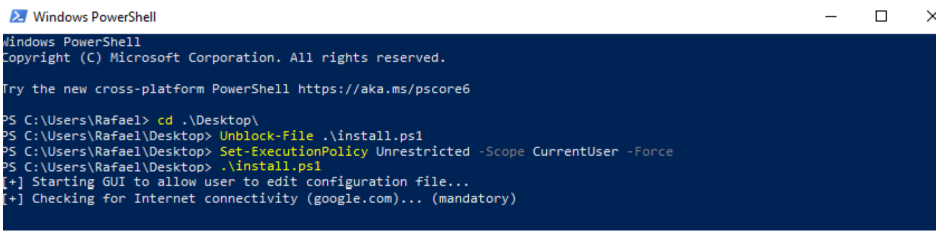
https://github.com/mandiant/flare-vm

Installing the ./install.ps1 will take some time since it is around 60GB.



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> (New-Object net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/mai
n/install.ps1',"$([Environment]::GetFolderPath("Desktop"))\install.ps1")
PS C:\Windows\system32> _
```

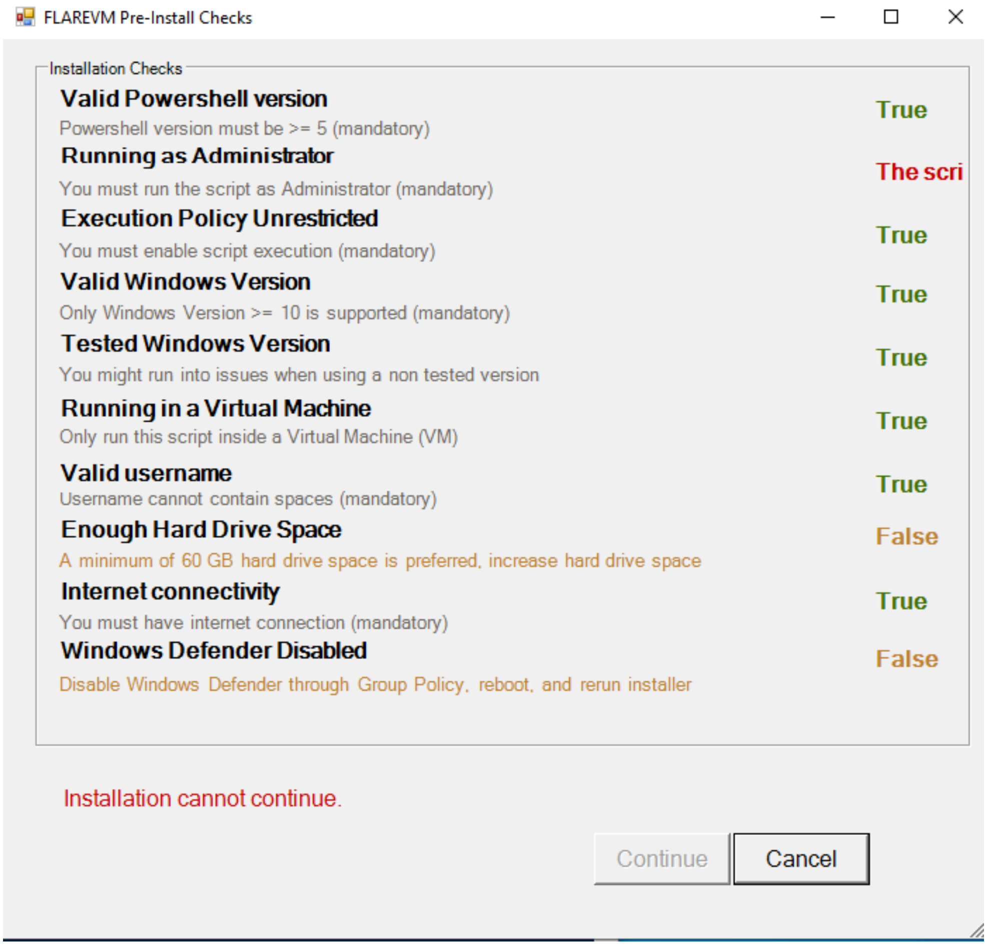


Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Rafael> cd .\Desktop\
PS C:\Users\Rafael\Desktop> Unblock-File .\install.ps1
PS C:\Users\Rafael\Desktop> Set-ExecutionPolicy Unrestricted -Scope CurrentUser -Force
PS C:\Users\Rafael\Desktop> .\install.ps1
[+] Starting GUI to allow user to edit configuration file...
[+] Checking for Internet connectivity (google.com)... (mandatory)
```

Rafael Angelo Christianto

The screenshot below shows the requirements needed to install FlareVM.



Valid Powershell version — True
Powershell version must be >= 5 (mandatory)

Running as Administrator — The scri
You must run the script as Administrator (mandatory)

Execution Policy Unrestricted — True
You must enable script execution (mandatory)

Valid Windows Version — True
Only Windows Version >= 10 is supported (mandatory)

Tested Windows Version — True
You might run into issues when using a non tested version

Running in a Virtual Machine — True
Only run this script inside a Virtual Machine (VM)

Valid username — True
Username cannot contain spaces (mandatory)

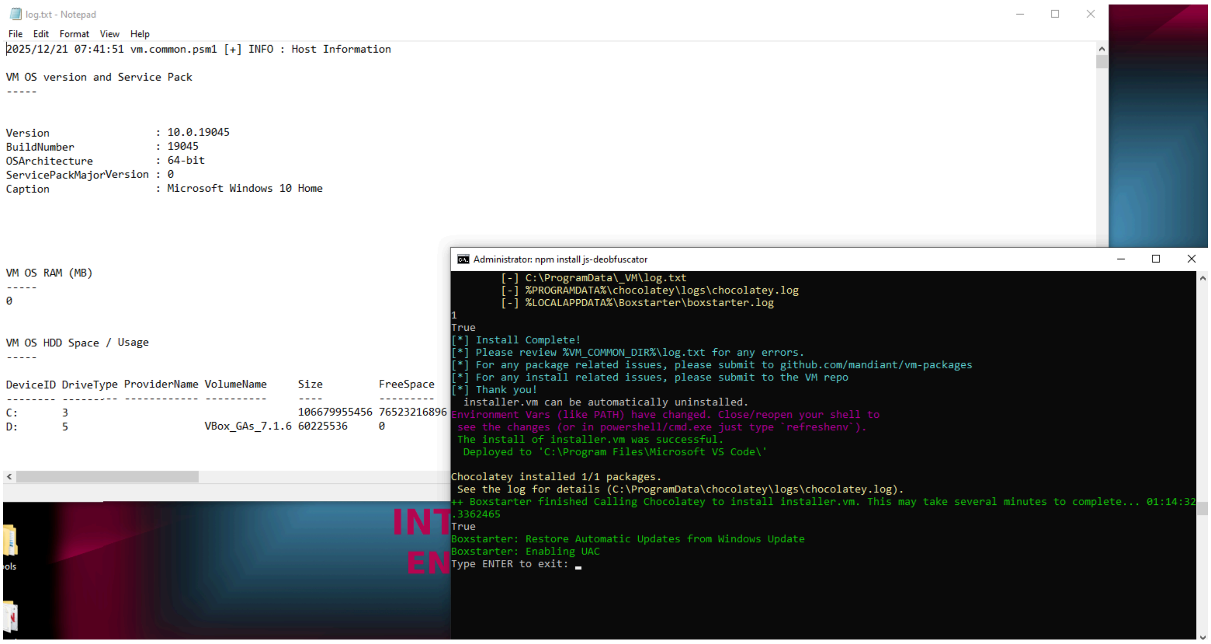
Enough Hard Drive Space — False
A minimum of 60 GB hard drive space is preferred, increase hard drive space

Internet connectivity — True
You must have internet connection (mandatory)

Windows Defender Disabled — False
Disable Windows Defender through Group Policy, reboot, and rerun installer

Installation cannot continue.

This image below is what the terminal will look like once installations are completed and there will be a Notebook file open up explaining the OS VM information

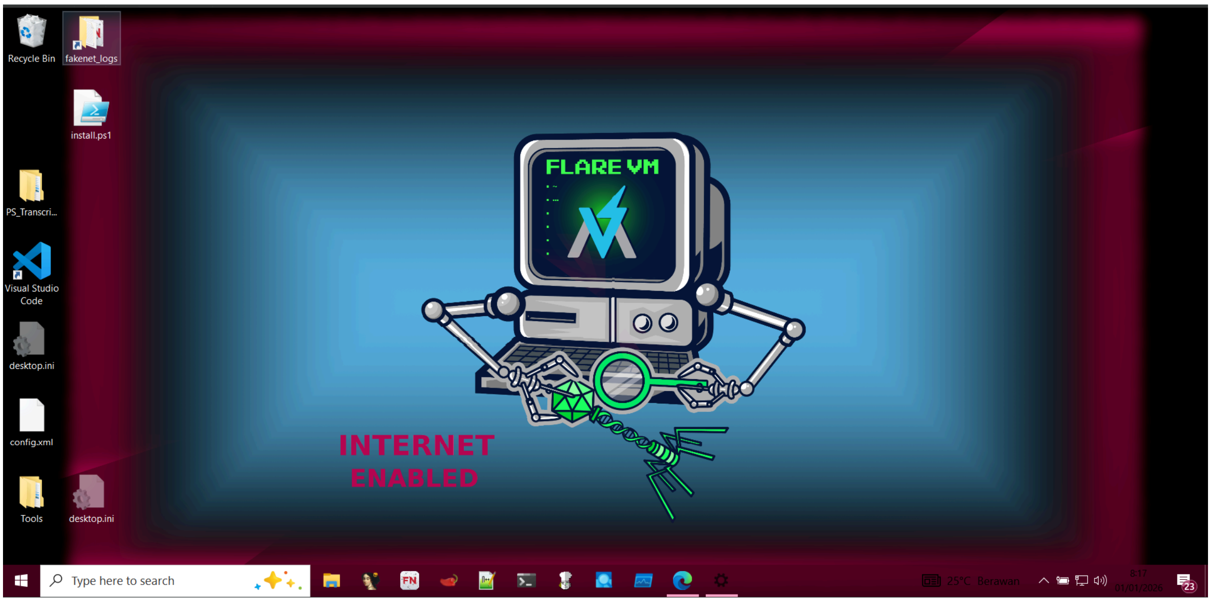

log.txt - Notepad
File Edit Format View Help
Administrator: npm install js-deobfuscator

```
2025/12/21 07:41:51 vm.common.psm1 [+] INFO : Host Information

VM OS version and Service Pack
-----


Version                 : 10.0.19045
BuildNumber             : 19045
OSArchitecture          : 64-bit
ServicePackMajorVersion : 0
Caption                 : Microsoft Windows 10 Home




VM OS RAM (MB)
-----
0


VM OS HDD Space / Usage
-----

DeviceID DriveType ProviderName VolumeName      Size         FreeSpace
-------- --------- ------------ ----------      ----         ---------
C:       3                                      106679955456 76523216896
D:       5                      VBox_GAs_7.1.6  60225536     0
```

```
        [-] C:\ProgramData\_VM\log.txt
        [-] %PROGRAMDATA%\chocolatey\logs\chocolatey.log
        [-] %LOCALAPPDATA%\Boxstarter\boxstarter.log
1
True
[*] Install Complete!
[*] Please review %VM_COMMON_DIR%\log.txt for any errors.
[*] For any package related issues, please submit to github.com/mandiant/vm-packages
[*] For any install related issues, please submit to the VM repo
[*] Thank you!
  installer.vm can be automatically uninstalled.
Environment Vars (like PATH) have changed. Close/reopen your shell to
 see the changes (or in powershell/cmd.exe just type `refreshenv`).
 The install of installer.vm was successful.
  Deployed to 'C:\Program Files\Microsoft VS Code\'

Chocolatey installed 1/1 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
++ Boxstarter finished Calling Chocolatey to install installer.vm. This may take several minutes to complete... 01:14:32
.3362465
True
Boxstarter: Restore Automatic Updates from Windows Update
Boxstarter: Enabling UAC
Type ENTER to exit: _
```

Rafael Angelo Christianto

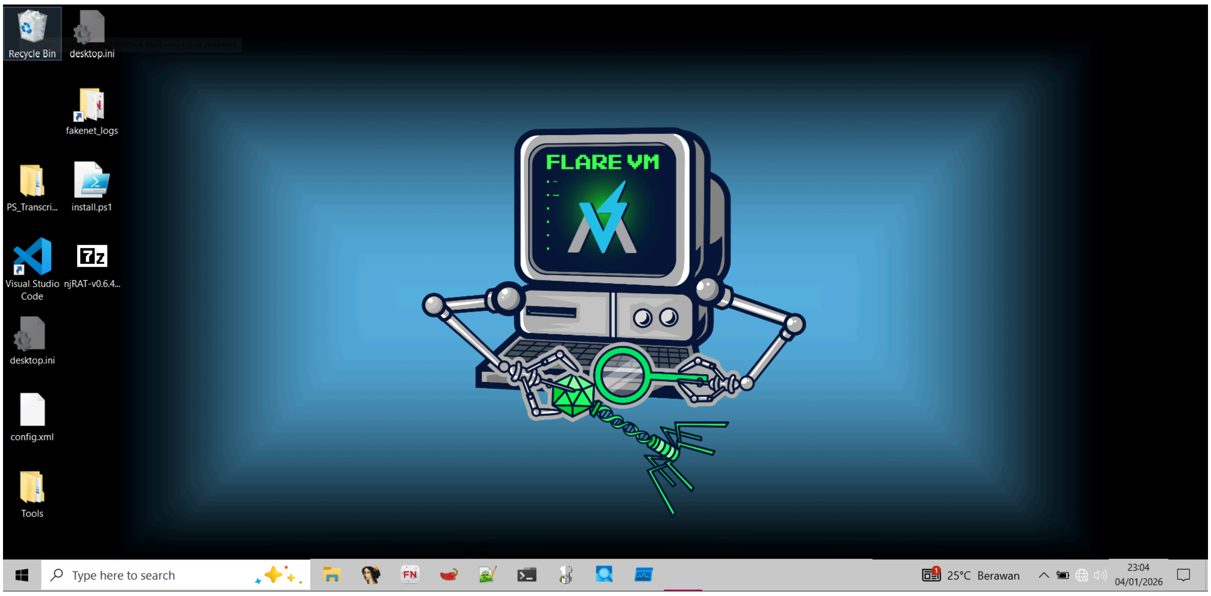
This image below will be what the VM will look like after all installations are complete. The wallpaper will automatically change to FlareVM's.



I will not be using all the tools included into FlareVM, since there are too many, but I will be using only the important ones

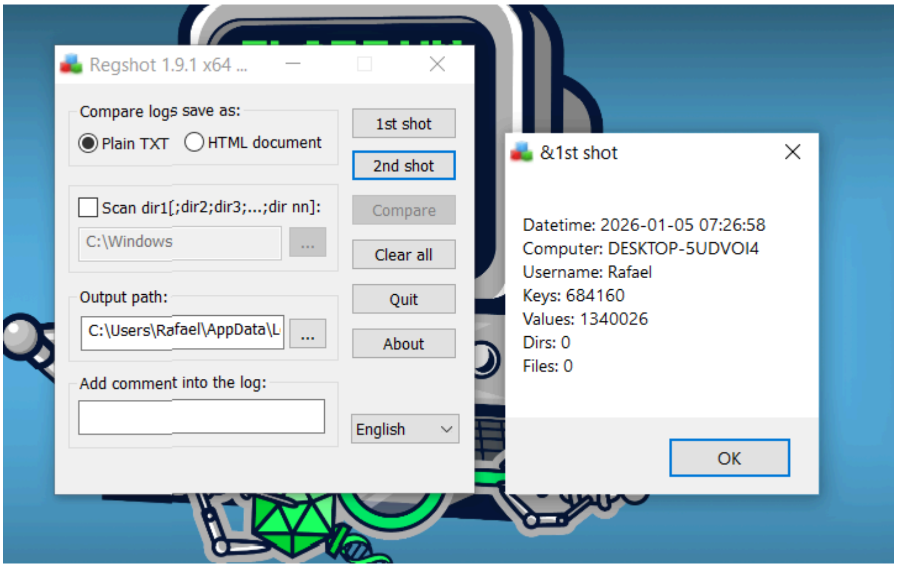
- Procmon → file/registry activity
- Process Explorer → running processes
- Wireshark → network traffic
- Regshot → registry changes
- FakeNet-NG → fake internet + capture C2

Make sure the FlareVM is in this format, since before it tells us that the internet is still enabled. Now, it is safe since it is disconnected from the internet and it does not have internet access. This will prevent the malware from going out into the network.



Rafael Angelo Christianto

We take the first Regshot before we launch the malware to see if the malware changed any key values in the registry editor. This will also output the detailed plain TXT document containing the file which the malware changed.



Compare logs save as:
● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

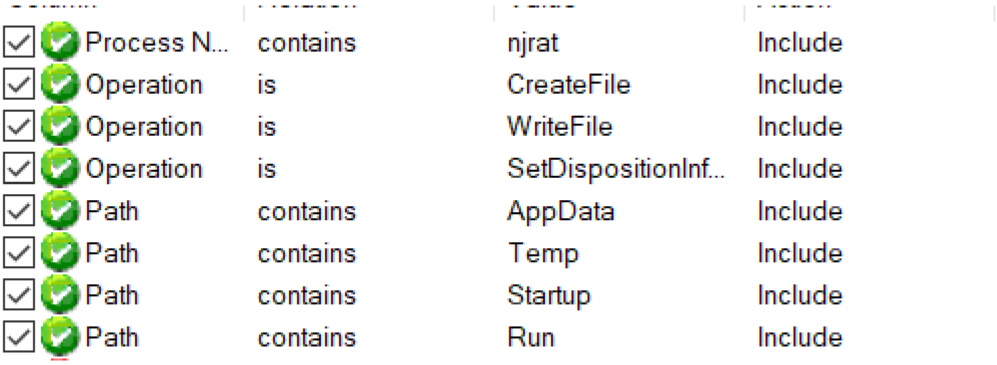
Output path:
C:\Users\Rafael\AppData\L

Add comment into the log:

English

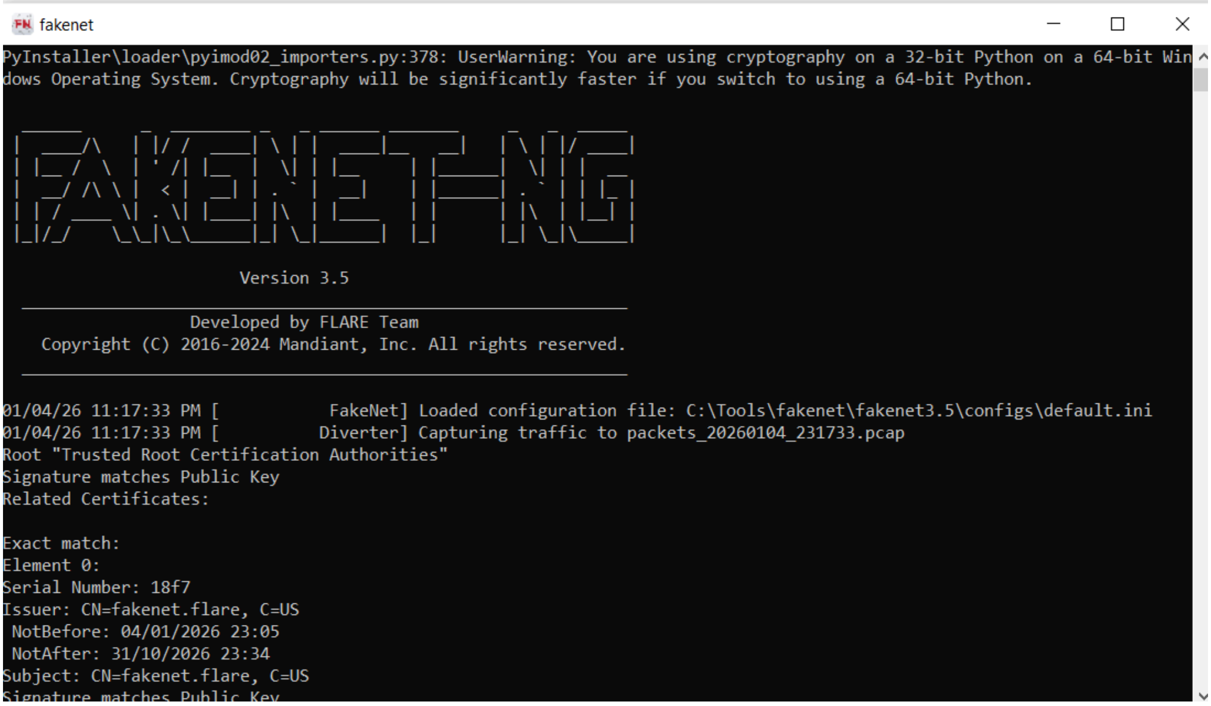
Datetime: 2026-01-05 07:26:58
Computer: DESKTOP-5UDVOI4
Username: Rafael
Keys: 684160
Values: 1340026
Dirs: 0
Files: 0

Here are the filters I use for the procmon (Process Monitor), I added so many filters because procmon is so heavy having all process there, so I just included the necessary ones used for this project.



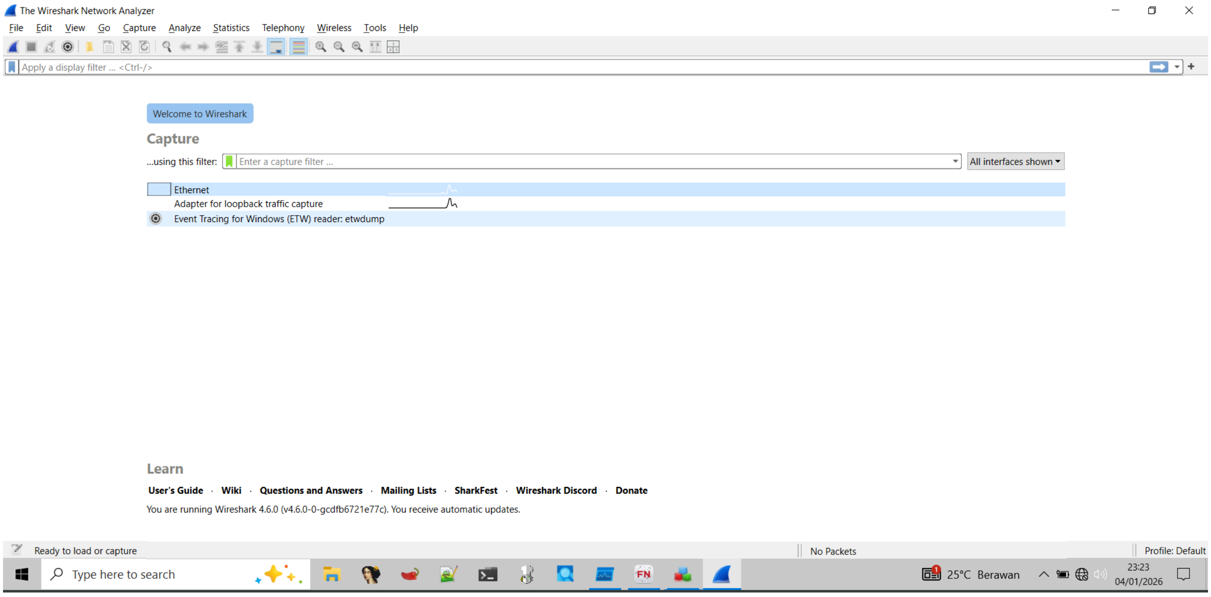
☑ ✓	Process N...	contains	njrat	Include
☑ ✓	Operation	is	CreateFile	Include
☑ ✓	Operation	is	WriteFile	Include
☑ ✓	Operation	is	SetDispositionInf...	Include
☑ ✓	Path	contains	AppData	Include
☑ ✓	Path	contains	Temp	Include
☑ ✓	Path	contains	Startup	Include
☑ ✓	Path	contains	Run	Include

I also added fakenet for simulating a fake network. This is done to see what the malware would do if it were in a network. I ran fakenet as administrator, because it will modify network configurations


fakenet

```
PyInstaller\loader\pyimod02_importers.py:378: UserWarning: You are using cryptography on a 32-bit Python on a 64-bit Win
dows Operating System. Cryptography will be significantly faster if you switch to using a 64-bit Python.

  ______      _  ________ _   _ ______ _______     _   _  _____
 |  ____/\   | |/ /  ____| \ | |  ____|__   __|   | \ | |/ ____|
 | |__ /  \  | ' /| |__  |  \| | |__     | |______|  \| | |  __
 |  __/ /\ \ |  < |  __| | . ` |  __|    | |______| . ` | | |_ |
 | | / ____ \| . \| |____| |\  | |____   | |      | |\  | |__| |
 |_|/_/    \_\_|\_\______|_| \_|______|  |_|      |_| \_|\_____|

                        Version 3.5
  _____________________________________________________________
                   Developed by FLARE Team
    Copyright (C) 2016-2024 Mandiant, Inc. All rights reserved.
  _____________________________________________________________

01/04/26 11:17:33 PM [           FakeNet] Loaded configuration file: C:\Tools\fakenet\fakenet3.5\configs\default.ini
01/04/26 11:17:33 PM [          Diverter] Capturing traffic to packets_20260104_231733.pcap
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

Exact match:
Element 0:
Serial Number: 18f7
Issuer: CN=fakenet.flare, C=US
 NotBefore: 04/01/2026 23:05
 NotAfter: 31/10/2026 23:34
Subject: CN=fakenet.flare, C=US
Signature matches Public Key
```

For the network traffic capturing, I will use Wireshark to see what is happening from a network level point of view. We expect HTTP requests, ARP requests, and others. A screenshot of Wireshark home page will be given below. And I will be capturing a the Ethernet adapter


The Wireshark Network Analyzer

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Ethernet
Adapter for loopback traffic capture
Event Tracing for Windows (ETW) reader: etwdump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

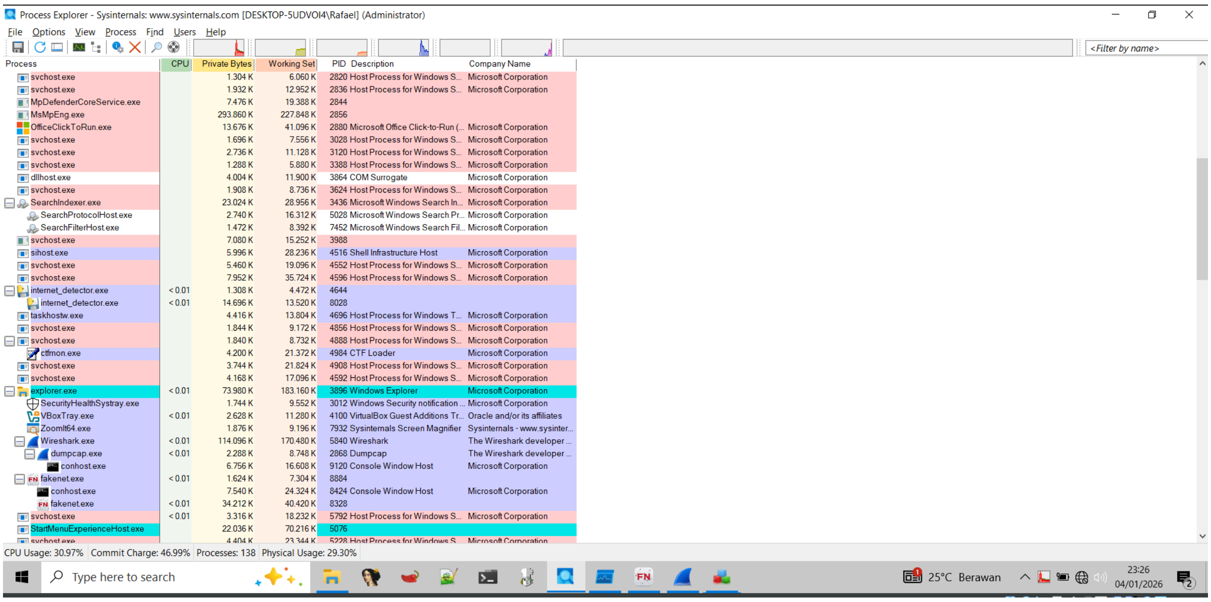
You are running Wireshark 4.6.0 (v4.6.0-0-gcdfb6721e77c). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Type here to search | 25°C Berawan | 23:23 04/01/2026

Here I also opened Procexp (Process Explorer) to see parent processes and child processes and observe whether there is a strange process starting.

Rafael Angelo Christianto



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-5UDVOI4\Rafael] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		1.304 K	6.060 K	2820	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1.932 K	12.952 K	2836	Host Process for Windows S...	Microsoft Corporation
MpDefenderCoreService.exe		7.476 K	19.388 K	2844		
MsMpEng.exe		293.860 K	227.848 K	2856		
OfficeClickToRun.exe		13.676 K	41.096 K	2880	Microsoft Office Click-to-Run (...	Microsoft Corporation
svchost.exe		1.696 K	7.556 K	3028	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2.736 K	11.128 K	3120	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1.288 K	5.880 K	3388	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		4.004 K	11.900 K	3864	COM Surrogate	Microsoft Corporation
svchost.exe		1.908 K	8.736 K	3624	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe		23.024 K	28.956 K	3436	Microsoft Windows Search In...	Microsoft Corporation
SearchProtocolHost.exe		2.740 K	16.312 K	5028	Microsoft Windows Search Pr...	Microsoft Corporation
SearchFilterHost.exe		1.472 K	8.392 K	7452	Microsoft Windows Search Fil...	Microsoft Corporation
svchost.exe		7.080 K	15.252 K	3988		
sihost.exe		5.996 K	28.236 K	4516	Shell Infrastructure Host	Microsoft Corporation
svchost.exe		5.460 K	19.096 K	4552	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7.952 K	35.724 K	4596	Host Process for Windows S...	Microsoft Corporation
internet_detector.exe	< 0.01	1.308 K	4.472 K	4644		
internet_detector.exe	< 0.01	14.696 K	13.520 K	8028		
taskhostw.exe		4.416 K	13.804 K	4696	Host Process for Windows T...	Microsoft Corporation
svchost.exe		1.844 K	9.172 K	4856	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1.840 K	8.732 K	4888	Host Process for Windows S...	Microsoft Corporation
ctfmon.exe		4.200 K	21.372 K	4984	CTF Loader	Microsoft Corporation
svchost.exe		3.744 K	21.824 K	4908	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4.168 K	17.096 K	4592	Host Process for Windows S...	Microsoft Corporation
explorer.exe	< 0.01	73.980 K	183.160 K	3896	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1.744 K	9.552 K	3012	Windows Security notification ...	Microsoft Corporation
VBoxTray.exe	< 0.01	2.628 K	11.280 K	4100	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
ZoomIt64.exe		1.876 K	9.196 K	7932	Sysinternals Screen Magnifier	Sysinternals - www.sysinter...
Wireshark.exe	< 0.01	114.096 K	170.480 K	5840	Wireshark	The Wireshark developer ...
dumpcap.exe	< 0.01	2.288 K	8.748 K	2868	Dumpcap	The Wireshark developer ...
conhost.exe		6.756 K	16.608 K	9120	Console Window Host	Microsoft Corporation
fakenet.exe	< 0.01	1.624 K	7.304 K	8884		
conhost.exe		7.540 K	24.324 K	8424	Console Window Host	Microsoft Corporation
fakenet.exe	< 0.01	34.212 K	40.420 K	8328		
svchost.exe	< 0.01	3.316 K	18.232 K	5792	Host Process for Windows S...	Microsoft Corporation
StartMenuExperienceHost.exe		22.036 K	70.216 K	5076		
svchost.exe		4.404 K	23.344 K	5228	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 30.97% Commit Charge: 46.99% Processes: 138 Physical Usage: 29.30%

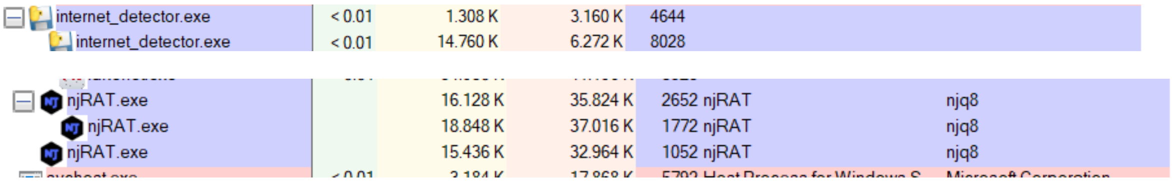
Procmon and Procexp will serve different purposes.

- Captures and logs events (file, registry, network, process/thread) in real-time.
- Provides detailed information about running processes and their state.

Results and Discussion

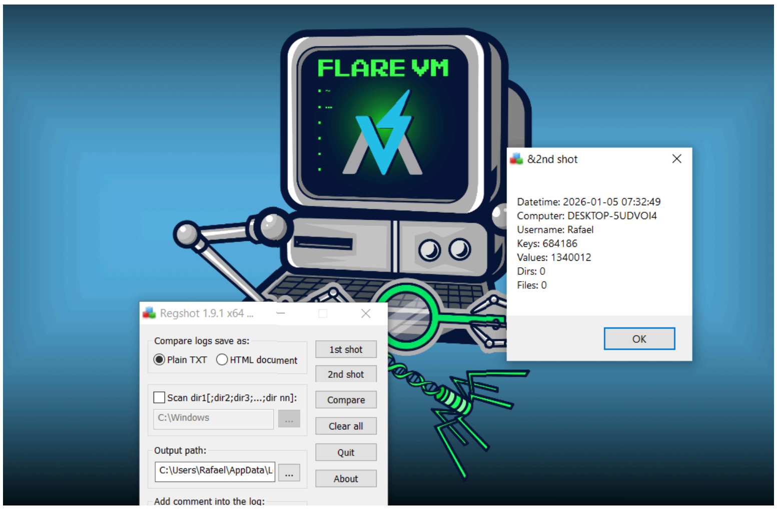
I am going to let the malware run for 1-2 minutes. Then I will analyze the results.

Here in the process explorer, I found 2 processes that could be generated by njRAT. First is the internet_detector.exe which is an uncommon process and would be used by the malware to detect whether the computer is connected to a network. And second, the njRAT.exe which is the application where I executed the malware from, possibly being a remote access trojan (RAT).



```
internet_detector.exe        < 0.01    1.308 K    3.160 K   4644
  internet_detector.exe      < 0.01   14.760 K    6.272 K   8028

njRAT.exe                             16.128 K   35.824 K   2652 njRAT    njq8
  njRAT.exe                           18.848 K   37.016 K   1772 njRAT    njq8
njRAT.exe                             15.436 K   32.964 K   1052 njRAT    njq8
```

After the malware was run, I took the second shot in Regshot to uncover whether the malware changed anything about the files in the registry editor and it can be seen from the 2 screenshot given below.



&2nd shot

Datetime: 2026-01-05 07:32:49
Computer: DESKTOP-5UDVOI4
Username: Rafael
Keys: 684186
Values: 1340012
Dirs: 0
Files: 0

Regshot 1.9.1 x64 ...

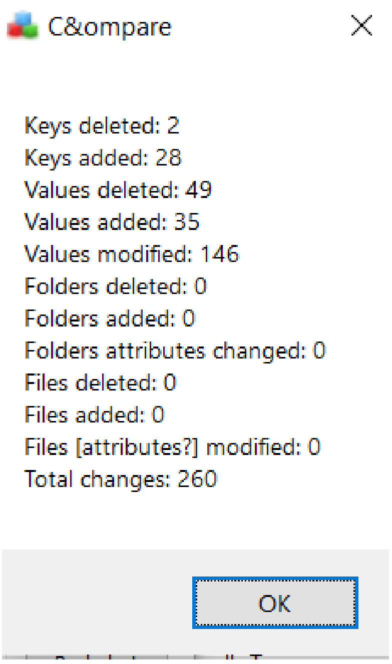
Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]: C:\Windows

Output path: C:\Users\Rafael\AppData\L

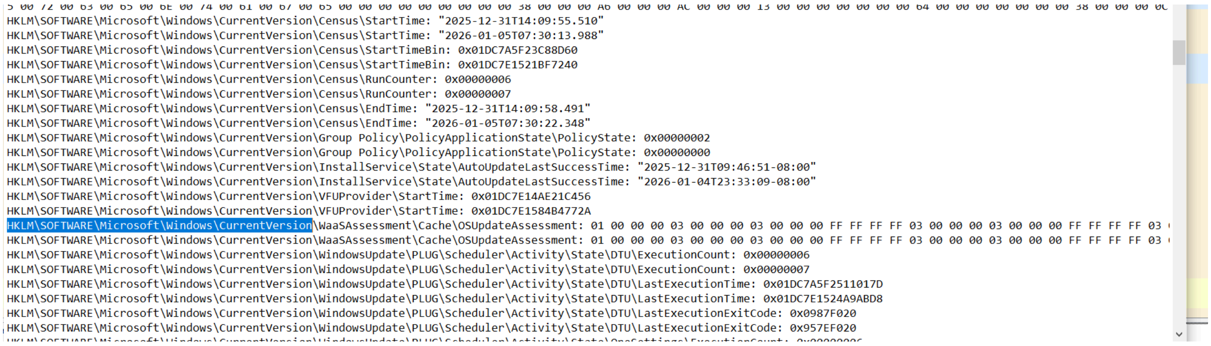
Add comment into the log:

Here I am comparing what was changed from the 1st shot to the 2nd shot.



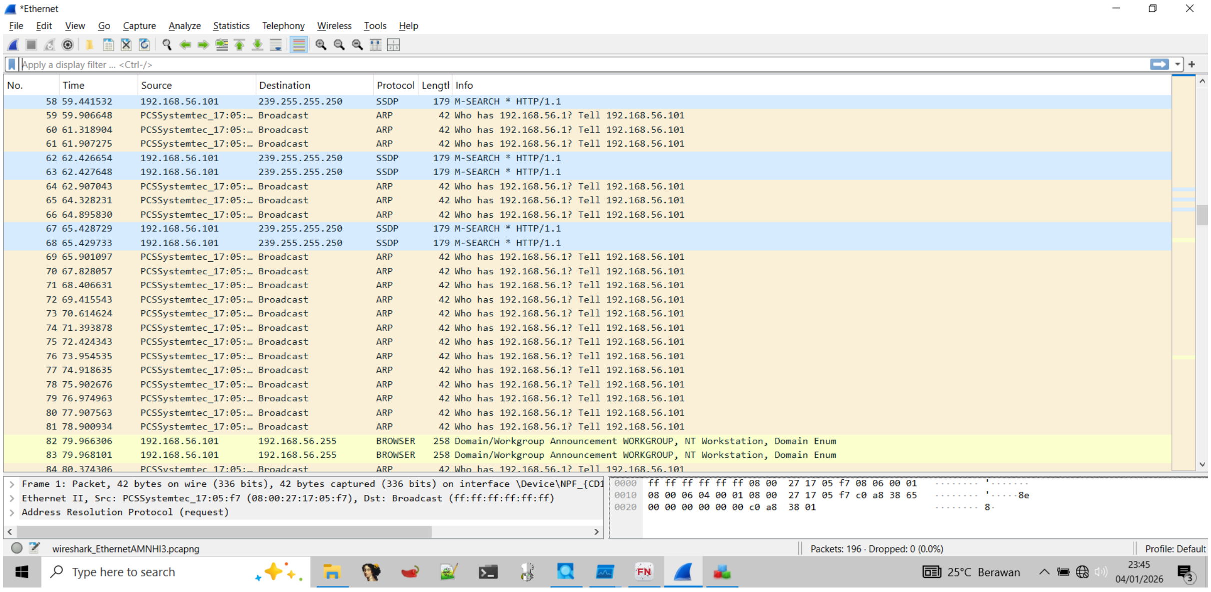
Keys deleted: 2
Keys added: 28
Values deleted: 49
Values added: 35
Values modified: 146
Folders deleted: 0
Folders added: 0
Folders attributes changed: 0
Files deleted: 0
Files added: 0
Files [attributes?] modified: 0
Total changes: 260

From the TXT file outputted by Regshot, we can see the files majorly being updated or written are the group policies and Windows updates registries. These files can be seen from the screenshot below.



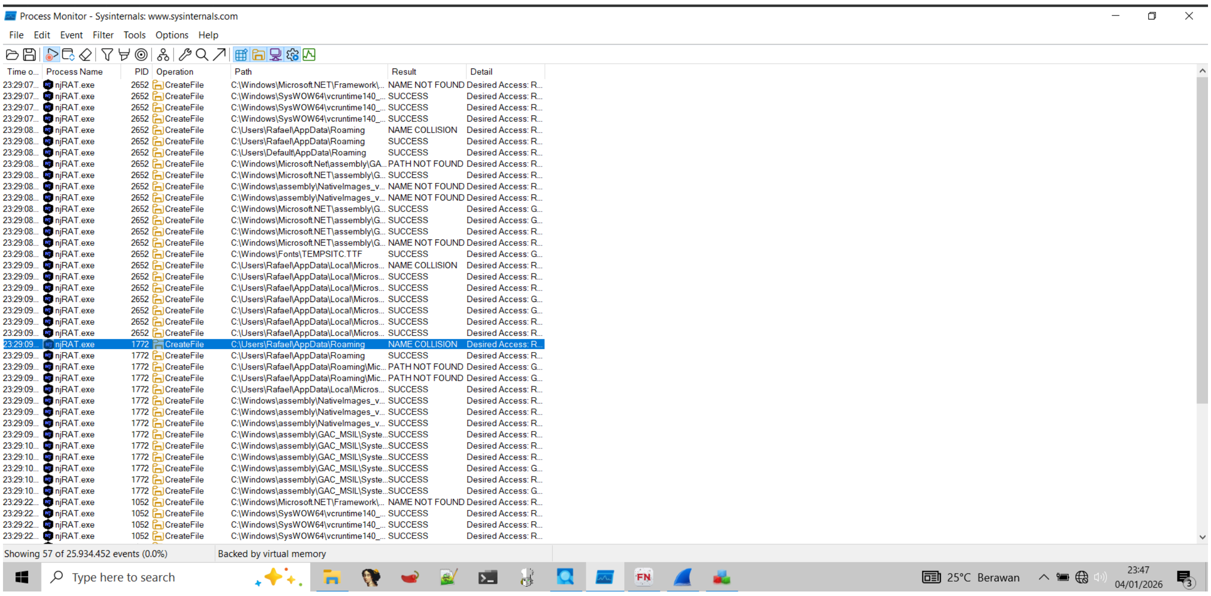
```
5 00 72 00 63 00 65 00 6E 00 74 00 61 00 67 00 65 00 00 00 00 00 00 00 00 00 00 38 00 00 00 A6 00 00 00 AC 00 00 00 13 00 00 00 00 00 00 00 00 64 00 00 00 00 00 00 00 38 00 00 00 0C
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\StartTime: "2025-12-31T14:09:55.510"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\StartTime: "2026-01-05T07:30:13.988"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\StartTimeBin: 0x01DC7A5F23C88D60
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\StartTimeBin: 0x01DC7E1521BF7240
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\RunCounter: 0x00000006
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\RunCounter: 0x00000007
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\EndTime: "2025-12-31T14:09:58.491"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Census\EndTime: "2026-01-05T07:30:22.348"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\PolicyApplicationState\PolicyState: 0x00000002
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\PolicyApplicationState\PolicyState: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\InstallService\State\AutoUpdateLastSuccessTime: "2025-12-31T09:46:51-08:00"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\InstallService\State\AutoUpdateLastSuccessTime: "2026-01-04T23:33:09-08:00"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime: 0x01DC7E14AE21C456
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime: 0x01DC7E1584B4772A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WaaSAssessment\Cache\OSUpdateAssessment: 01 00 00 00 03 00 00 00 03 00 00 00 FF FF FF FF 03 00 00 00 03 00 00 00 FF FF FF FF 03
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WaaSAssessment\Cache\OSUpdateAssessment: 01 00 00 00 03 00 00 00 03 00 00 00 FF FF FF FF 03 00 00 00 03 00 00 00 FF FF FF FF 03
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\PLUG\Scheduler\Activity\State\DTU\ExecutionCount: 0x00000006
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\PLUG\Scheduler\Activity\State\DTU\ExecutionCount: 0x00000007
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\PLUG\Scheduler\Activity\State\DTU\LastExecutionTime: 0x01DC7A5F2511017D
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\PLUG\Scheduler\Activity\State\DTU\LastExecutionTime: 0x01DC7E1524A9ABD8
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\PLUG\Scheduler\Activity\State\DTU\LastExecutionExitCode: 0x0987F020
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\PLUG\Scheduler\Activity\State\DTU\LastExecutionExitCode: 0x957EF020
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\PLUG\Scheduler\Activity\State\OneSettings\ExecutionCount: 0x00000006
```

For the next screenshot image below, it shows a Wireshark capture, consisting of ARP, SSDP, and BROWSER protocols. Network traffic analysis using Wireshark and FakeNet-NG revealed only standard Windows background traffic (ARP, SSDP, NetBIOS). No malicious outbound communication was observed. This suggests that the njRAT sample either failed to execute its network functionality, was configured to connect to a hardcoded C2 server not present in the analysis environment, or terminated early due to environmental checks.”


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

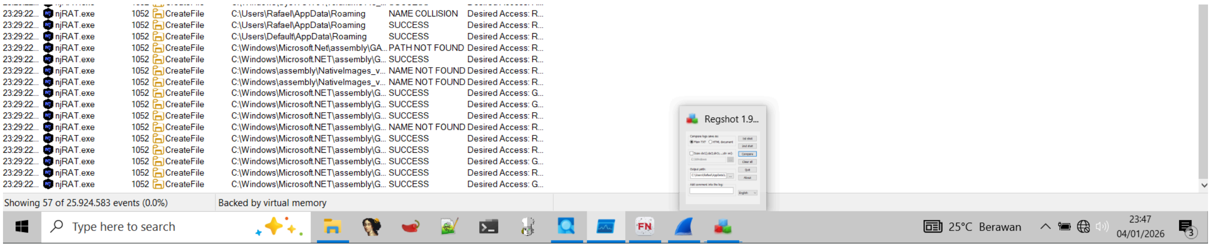
```
No.   Time       Source                Destination      Protocol Lengtl Info
   58 59.441532  192.168.56.101        239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
   59 59.906648  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   60 61.318904  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   61 61.907275  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   62 62.426654  192.168.56.101        239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
   63 62.427648  192.168.56.101        239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
   64 62.907043  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   65 64.328231  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   66 64.895830  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   67 65.428729  192.168.56.101        239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
   68 65.429733  192.168.56.101        239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
   69 65.901097  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   70 67.828057  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   71 68.406631  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   72 69.415543  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   73 70.614624  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   74 71.393878  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   75 72.424343  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   76 73.954535  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   77 74.918635  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   78 75.902676  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   79 76.974963  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   80 77.907563  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   81 78.900934  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101
   82 79.966306  192.168.56.101        192.168.56.255   BROWSER  258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
   83 79.968101  192.168.56.101        192.168.56.255   BROWSER  258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
   84 80.374306  PCSSystemtec_17:05:…  Broadcast        ARP       42 Who has 192.168.56.1? Tell 192.168.56.101

> Frame 1: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{CD1
> Ethernet II, Src: PCSSystemtec_17:05:f7 (08:00:27:17:05:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00  27 17 05 f7 08 06 00 01   ········ '·······
0010  08 00 06 04 00 01 08 00  27 17 05 f7 c0 a8 38 65   ········ '·····8e
0020  00 00 00 00 00 00 c0 a8  38 01                     ········ 8·

wireshark_EthernetAMNHI3.pcapng          Packets: 196 · Dropped: 0 (0.0%)          Profile: Default
```

Below we can see from the njRAT process it is having multiple PIDs and numerous writing files. Then njRAT is a .NET malware so we see expected behaviour.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
23:29:07...	njRAT.exe	2652	CreateFile	C:\Windows\Microsoft.NET\Framework\...	NAME NOT FOUND	Desired Access: R...
23:29:07...	njRAT.exe	2652	CreateFile	C:\Windows\SysWOW64\vcruntime140_...	SUCCESS	Desired Access: R...
23:29:07...	njRAT.exe	2652	CreateFile	C:\Windows\SysWOW64\vcruntime140_...	SUCCESS	Desired Access: R...
23:29:07...	njRAT.exe	2652	CreateFile	C:\Windows\SysWOW64\vcruntime140_...	SUCCESS	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Roaming	NAME COLLISION	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Roaming	SUCCESS	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Users\Default\AppData\Roaming	SUCCESS	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\Microsoft.Net\assembly\GA...	PATH NOT FOUND	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\assembly\NativeImages_v...	NAME NOT FOUND	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\assembly\NativeImages_v...	NAME NOT FOUND	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: G...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: G...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	NAME NOT FOUND	Desired Access: R...
23:29:08...	njRAT.exe	2652	CreateFile	C:\Windows\Fonts\TEMPSITC.TTF	SUCCESS	Desired Access: G...
23:29:09...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	NAME COLLISION	Desired Access: R...
23:29:09...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	SUCCESS	Desired Access: G...
23:29:09...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	SUCCESS	Desired Access: G...
23:29:09...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	2652	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Users\Rafael\AppData\Roaming	NAME COLLISION	Desired Access: R...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Users\Rafael\AppData\Roaming	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Users\Rafael\AppData\Roaming\Mic...	PATH NOT FOUND	Desired Access: G...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Users\Rafael\AppData\Roaming\Mic...	PATH NOT FOUND	Desired Access: G...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Users\Rafael\AppData\Local\Micros...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\NativeImages_v...	SUCCESS	Desired Access: R...
23:29:09...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\GAC_MSIL\Syste...	SUCCESS	Desired Access: R...
23:29:10...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\GAC_MSIL\Syste...	SUCCESS	Desired Access: R...
23:29:10...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\GAC_MSIL\Syste...	SUCCESS	Desired Access: R...
23:29:10...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\GAC_MSIL\Syste...	SUCCESS	Desired Access: G...
23:29:10...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\GAC_MSIL\Syste...	SUCCESS	Desired Access: R...
23:29:10...	njRAT.exe	1772	CreateFile	C:\Windows\assembly\GAC_MSIL\Syste...	SUCCESS	Desired Access: G...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\Framework\...	NAME NOT FOUND	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\SysWOW64\vcruntime140_...	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\SysWOW64\vcruntime140_...	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\SysWOW64\vcruntime140_...	SUCCESS	Desired Access: R...

Showing 57 of 25.934.452 events (0.0%) Backed by virtual memory



Time o...	Process Name	PID	Operation	Path	Result	Detail
23:29:22...	njRAT.exe	1052	CreateFile	C:\Users\Rafael\AppData\Roaming	NAME COLLISION	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Users\Rafael\AppData\Roaming	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Users\Default\AppData\Roaming	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.Net\assembly\GA...	PATH NOT FOUND	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\assembly\NativeImages_v...	NAME NOT FOUND	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\assembly\NativeImages_v...	NAME NOT FOUND	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: G...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: G...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	NAME NOT FOUND	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: G...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: R...
23:29:22...	njRAT.exe	1052	CreateFile	C:\Windows\Microsoft.NET\assembly\G...	SUCCESS	Desired Access: G...

Showing 57 of 25.924.583 events (0.0%) Backed by virtual memory

I tried to delete the Process in Process Explorer but after killing its processes it does not seem to persist after being deleted. After I tried to reboot the VM, just in case it sets it in the Startup folder, but it does not reappear in Process Explorer as well.

After all the malware analysis was complete, I reverted back to the snapshot where FlareVM is installed, but before the malware was executed for safety reasons.

Rafael Angelo Christianto

Conclusion

Sample Name: njRAT v0.6.4
Malware Type: Remote Access Trojan (RAT)
Analysis Type: Dynamic Analysis in Isolated FLARE VM Environment

Based on the dynamic analysis conducted in an isolated Windows 10 FLARE VM environment, the njRAT v0.6.4 sample demonstrated limited malicious behavior during execution.

Execution Behavior

- The malware executed successfully and spawned the primary process njRAT.exe.
- An additional suspicious process, internet_detector.exe, was observed, likely used to check for network connectivity before initiating further actions.
- The malware ran silently without displaying any user-visible interface.

Persistence Mechanisms

- Registry analysis using Regshot indicated changes primarily within Windows Update and Group Policy–related registry keys.
- No clear evidence of traditional persistence mechanisms (such as Run or RunOnce startup keys, scheduled tasks, or startup folder entries) was observed.
- After terminating the malware process and rebooting the virtual machine, the malware did not reappear, suggesting persistence was either not implemented, misconfigured, or failed due to environmental conditions.

File System Activity

- Process Monitor revealed multiple file write operations associated with the njRAT process, which is consistent with expected behavior for a .NET-based malware.
- No long-lived malicious binaries were conclusively identified as being dropped for persistence.

Network Activity

- Network traffic analysis using Wireshark and FakeNet-NG showed only standard background Windows traffic (ARP, SSDP, NetBIOS).
- No malicious outbound connections or command-and-control (C2) communication were detected.
- This suggests that the njRAT sample may:
    - Rely on a hardcoded C2 server that was unavailable,
    - Perform environmental checks and suppress network activity when conditions are unmet,
    - Or require specific configuration parameters not present in this sample.

Overall Assessment

While njRAT v0.6.4 is a known Remote Access Trojan with capabilities such as persistence, surveillance, and remote command execution, these behaviors were not fully exhibited in this controlled analysis environment. The lack of observable persistence and network communication indicates that the malware either failed to fully activate or was restricted by environmental safeguards.

This analysis highlights the importance of environment-aware malware behavior and reinforces the need to combine dynamic analysis with static analysis to fully uncover a malware sample’s capabilities.