

Rapport de Projet – Analyse du Malware Agent Tesla

Élaboré par :

Chadha Hammami

Encadré par :

Ameni Ben Khalifa

Groupe : SSIR-4-B



Année Universitaire : 2024-2025

Table des matières

1.	Introduction:	3
2.	Recherche théorique : Agent Tesla	3
3.	Analyse automatique	4
3.1	Environnement de test	4
3.2	Réalisation de l'analyse automatique:	6
3.2.1	Hybrid Analysis:	7
3.2.2	Virus Total:	9
3.2.3	Comparaison des resultat obtenus avec les différents outils:	10
4	Analyse statique:	10
4.1	Outils utilisés:	10
4.1.1	DIE:	11
4.1.2	PEStudio	12
4.1.3	Strings / Bintext	15
4.1.4	dnSpy:	16
5	Analyse dynamique:	20
5.1	Environnement de test:	20
5.2	Regshot:	22
5.3	Process explorer	24
5.4	TCPView:	26
5.5	Wireshark:	27
5.6	Process Monitor:	28
6	Conclusion:	30

1. Introduction:

Dans le cadre de ce projet, nous avons mené une analyse approfondie d'un logiciel malveillant appartenant à la catégorie des Remote Access Trojan (RAT), en l'occurrence : Agent Tesla. Ce projet s'inscrit dans une démarche pédagogique visant à développer des compétences en cybersécurité, notamment dans l'analyse de logiciels malveillants.

Les objectifs principaux sont :

- Se familiariser avec différentes familles de malwares
- Acquérir une méthodologie rigoureuse d'analyse automatique, statique et dynamique
- Maîtriser les outils spécialisés dans l'analyse de malwares
- Identifier les comportements malveillants à travers différents vecteurs d'observation (code, comportement réseau, activité système, etc.)

Nous avons porté notre choix sur Agent Tesla en raison de sa popularité dans les campagnes de phishing, de son évolution continue, ainsi que de la disponibilité d'échantillons permettant une analyse complète.

2. Recherche théorique : Agent Tesla

Agent Tesla est un logiciel malveillant de type RAT (Remote Access Trojan) apparu pour la première fois en 2014. Il est principalement utilisé pour l'exfiltration d'informations sensibles depuis des systèmes infectés. Agent Tesla est distribué par le biais de campagnes de phishing, souvent sous forme de pièces jointes malveillantes dans des emails.

Caractéristiques principales :

- 🐼 Type : RAT (Remote Access Trojan)
- 📅 Date de première apparition : 2014
- 🎯 Objectif : Vol de données (identifiants, mots de passe, captures d'écran, clipboard, etc.)
- 📦 Fonctionnalités :
 - Enregistreur de frappe (keylogger)
 - Capture de presse-papiers

- Extraction de données depuis les navigateurs, clients FTP, VPN, clients email...
- Exfiltration via SMTP, FTP ou HTTP
- Peut se maintenir en persistance sur le système

Campagnes d'utilisation :

Agent Tesla a été utilisé dans un grand nombre de campagnes de phishing visant diverses industries. Il est souvent diffusé via des fichiers Word, Excel ou PDF contenant des macros ou des exploits. Il a également été observé dans des archives ZIP contenant des exécutable déguisés.

Variantes :

Plusieurs versions ont été observées au fil des années :

- V1.0 (version de base avec keylogging et vol de mots de passe)
- V2.0 (ajout de fonctionnalités de communication réseau)
- V3+ (obfuscation améliorée, exfiltration via multiples protocoles)

État actuel :

Agent Tesla est encore actif à ce jour. Bien qu'il soit détecté par la plupart des antivirus, ses créateurs utilisent régulièrement des techniques d'obfuscation et de packers pour échapper à la détection.

3. Analyse automatique

L'analyse automatique du malware Agent Tesla a été réalisée à l'aide de deux plateformes reconnues : VirusTotal et Hybrid-Analysis. Ces outils permettent d'obtenir une première évaluation du comportement malveillant du fichier ainsi qu'un aperçu des indicateurs de compromission (IOC) et des moteurs antivirus qui le détectent.

3.1 Environnement de test

Environnement matériel : Notre environnement matériel utilisé durant la réalisation de notre projet est un PC DEL ayant les caractéristiques suivantes :

- Processeur : i3
- Mémoire : 16 Go

Environnement logiciel : Dans le cadre de notre projet d'analyse de malware, plusieurs outils de virtualisation et d'observation ont été utilisés afin d'assurer un environnement d'analyse sécurisé et isolé.

- **Utilisation de VMware Workstation**

VMware Workstation est un logiciel de virtualisation qui permet de créer et exécuter plusieurs systèmes d'exploitation sur un même ordinateur, offrant ainsi un environnement virtuel pour tester différentes configurations sans avoir besoin de matériel physique.



-

- **Utilisation de de la machine REMnux**

REMnux s'impose comme une solution incontournable pour toute analyse approfondie de malwares. Grâce à sa richesse fonctionnelle, sa facilité d'intégration dans des environnements virtualisés et sa spécialisation dans l'ingénierie inverse, elle offre aux analystes un cadre complet et sécurisé pour identifier, comprendre et documenter les menaces. Son utilisation contribue à renforcer l'efficacité des investigations en cybersécurité et à accélérer le processus de réponse aux incidents.



3.2 Réalisation de l'analyse automatique:

Voici les étapes suivies :

- **TÉLÉCHARGER UN ÉCHANTILLON AGENT TESLA:**

sur <https://bazaar.abuse.ch> → Recherche : Agent Tesla

NEW | Hunt across all abuse.ch platforms with one simple query - discover if an IPv4 address, domain, URL or file hash has been identified on any platform from a centralized search tool. Test it out here bazaar.abuse.ch - and happy hunting 🔍

MALWARE bazaar

From ABUSE²⁴ | SPAMHAUS

🔍 Browse 📁 Upload 🔔 Hunting Alerts 📄 Access Data ⚙️ FAQ 📖 About 👤 Login

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-05-03 08:18	954b611a8e8163b4269...	exe	AgentTesla	AgentTesla exe	marsomx	📄
2025-05-03 07:02	79938e3697df67a1df47...	exe	AgentTesla	AgentTesla exe	adm1n_usa32	📄
2025-05-03 01:42	f623bd827696deb0e7f8...	exe	AgentTesla	AgentTesla exe	threatcat_ch	📄
2025-05-02 07:41	bd5f4c6e49cf4f431897a...	lua	AgentTesla	AgentTesla TNT lua	cocaman	📄
2025-05-02 07:26	305df92519f590352913...	exe	AgentTesla	AgentTesla exe	SecuriteInfoCom	📄
2025-05-02 06:33	c6f89955e03e91b02d60...	exe	AgentTesla	AgentTesla exe geo TUR	abuse_ch	📄
2025-05-02 06:24	43766e6638c396cd911...	exe	AgentTesla	AgentTesla exe TNT	abuse_ch	📄
2025-05-02 06:24	756c14ee6f81488ac0a3...	exe	AgentTesla	AgentTesla exe TNT	abuse_ch	📄

Activities Firefox Web Browser May 3 07:59

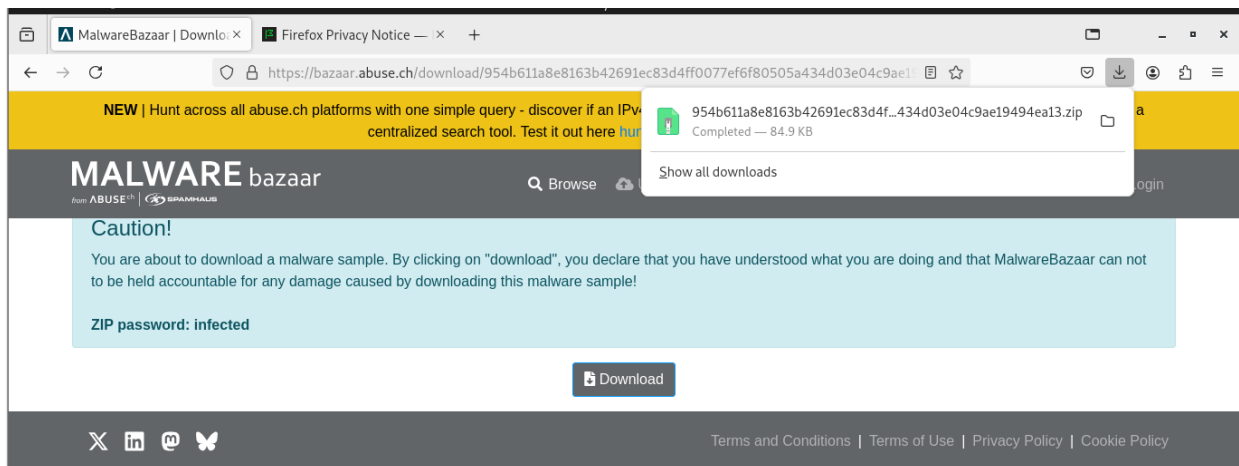
NEW | Hunt across all abuse.ch platforms with one simple query - discover if an IPv4 address, domain, URL or file hash has been identified on any platform from a centralized search tool. Test it out here bazaar.abuse.ch - and happy hunting 🔍

MALWARE bazaar

From ABUSE²⁴ | SPAMHAUS

🔍 Browse 📁 Upload 🔔 Hunting Alerts 📄 Access Data ⚙️ FAQ 📖 About 👤 Login

SHA3-384 hash:	3b1085546e23ced326b0ef4449e53f11de8382a49d5cba16f70c0b2e49c50639f8231d7af48576e2c6ea8606f15d4ad1
SHA1 hash:	fc65ec41e8de815bf580cd6174192a84ed659b0b
MD5 hash:	3cd8c914e892d12464c44471c82eaa0c
humanhash:	louisiana-mars-april-cup
File name:	dec-finalpayload2.bin
Download:	📄 download sample
Signature ⓘ	AgentTesla 🔔 Alert
File size:	245'248 bytes



SOUSSION AUX SANDBOXES:

on vas ensuite soumettre le fichier aux plateformes suivantes:

3.2.1 Hybrid Analysis:

Hybrid-Analysis est une sandbox en ligne qui permet une simulation d'exécution du malware et fournit une analyse comportementale détaillée.

HYBRID ANALYSIS Sandbox Quick Scans File Collections Resources Request Info

Analysis Overview

Submission name: dec-finalpayload2.bin.exe
Size: 240KiB
Type: peexe assembly executable
Mime: application/vnd.microsoft.portable-executable
SHA256: 954b611a8e8163b42691ec83d4ff0077ef6f80505a434d03e04c9ae19494ea13
Submitted At: 2025-05-03 08:20:19 (UTC)
Last Anti-Virus Scan: 2025-05-03 11:04:37 (UTC)
Last Sandbox Report: 2025-05-03 11:04:34 (UTC)

malicious
Threat Score: 100/100
AV Detection: 85%
Labeled As: Trojan.MSIL.Basic.8
#worldwindstealer #evasive
#windows-server-utility
Post Link E-Mail

0 Community Score 0

Anti-Virus Results

Updated a while ago

CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)
No Additional Data

MetaDefender
Multi Scan Analysis
Malicious (16/23)
More Details

Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (1)
Relations
Incident Response
Community (0)
Back to top

Windows 10 64 bit

954b611a8e8163b42691ec83d4ff0...

May 3rd 2025 11:04:34 (UTC)

!

Malicious

Threat Score:
100/100

Labeled As:
Trojan.MSIL.Basic.8

Indicators:
12 38 163

Characteristics:
↔

- Analysis Overview
- Anti-Virus Scanner Results
- Falcon Sandbox Reports (1)
- Relations
- Incident Response
- Community (0)
- Back to top

← → ↺

https://www.hybrid-analysis.com/sample/954b611a8e8163b42691ec83d4ff0077ef6f80505a434d03e04c9

🔒 ⬇️ 🌐 📄 ⌵

HYBRID ANALYSIS

Sandbox Quick Scans File Collections Resources Request Info

🔍 IP, Domain, Hash... More

👁 Risk Assessment

Spyware

Found a string that may be used as part of an injection method
Found browser information locations related strings
Tries to steal browser sensitive information (file access)

Stealer/Phishing

Found FTP credentials location strings
Reads FTP client related files
Tries to steal Mail credentials from registry

Fingerprint

Queries process information
Tries to identify its external IP address
Tries to steal Mail credentials from registry

Evasive

Executes WMI queries known to be used for VM detection
Found a reference to a WMI query string known to be used for VM detection
Input file contains API references not part of its Import Address Table (IAT)
Modifies file/console tracing settings (often used to hide footprints on system)
Possibly tries to implement anti-virtualization techniques using MAC address detection

Network Behavior

Contacts 1 domain and 1 host. [View all details](#)

Analysis Overview

Anti-Virus Scanner Results

Falcon Sandbox Reports (1)

Relations

Incident Response

Community (0)

Back to top

remnux@remnux: ~

Free Automated Malware Analysis ...

[temp_extracted_new]

1/

Network Analysis Overview

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
ip-api.com	208.95.112.1 TTL: 60	Internet Domain Service BS Corp. Organization: Whois Privacy Corp. Name Server: b.ip-api.com Creation Date: 2012-04-24T13:42:54	🇺🇸 Reserved

Contacted Hosts

Close

3.2.2 Virus Total:

VirusTotal est un service en ligne qui analyse les fichiers à l'aide de plus de 70 moteurs antivirus.

50
/ 72

Community Score

-14

50/72 security vendors flagged this file as malicious

954b611a8e8163b42691ec83d4ff0077ef6f80505a434d03e04c9ae19494ea13

f45b853c-c9d3-495e-9acb-d41a4a90029f.exe

peexe assembly calls-wmi detect-debug-environment checks-user-input

Activity Summary

Download Artifacts Full Reports Help

4 Detections

2 MALWARE 1 STEALER

1 TROJAN 1 EVADER

Mitre Signatures

13 LOW 69 INFO

IDS Rules

2 MEDIUM

Sigma Rules

2 MEDIUM

Dropped Files

9 OTHER

Network comms

3 HTTP 2 DNS 5 IP

Basic properties

MD5

3cd8c914e892d12464c44471c82eaa0c

SHA-1

fc65ec41e8de815bf580cd6174192a84ed659b0b

SHA-256

954b611a8e8163b42691ec83d4ff0077ef6f80505a434d03e04c9ae19494ea13

Vhash

225036551511e0723703b43622

AuthentiHash

e3ee0d1efe72a7ef2ce29e183d8d1efbb50be7a9d2b10a56770e067011196f91

Imphash

f34d5f2d4577ed6d9ceec516c1f5a744

SSDEEP

3072:spNyKayCB7/MJo27/12YHcTHo9rG8KaG5jnThdqwfzz:UyKayCB/uoHFsq8KaWTP

TLSH

T16A340F027F88EB15E1A97E3782EF2C2453B2B4C71633C60BAF49AF5514516826C7E72D

File type

Win32 EXE executable windows win32 pe peexe

Magic

PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

TrID

Generic CIL Executable (.NET, Mono, etc.) (67.7%) Win64 Executable (generic) (9.7%) Win32 Dynamic Link Library (generic) (6%) Win16 NE e...

DetectItEasy

PE32 Compiler: VB.NET Library: .NET (v4.0.30319) Linker: Microsoft Linker (11.0)

Magika

PEBIN

File size

239.50 KB (245248 bytes)

PEiD packer

.NET executable

Popular threat label

trojan.msil/agenttesla

Threat categories

trojan

Family labels

msil agenttesla basic

Contacted IP addresses (5)

IP	Detections	Autonomous System	Country
104.71.214.69	0 / 94	16625	US
151.101.22.172	0 / 94	54113	US
192.168.0.19	0 / 94	-	-
208.95.112.1	1 / 94	53334	US
8.8.8.8	0 / 94	15169	US

3.2.3 Comparaison des resultat obtenus avec les différents outils:

Critère	Hybrid Analysis	VirusTotal
Type d'analyse	Analyse dynamique (exécution dans une sandbox)	Analyse statique (multi-antivirus)
Score/Détection	Score élevé : 100/100 (indique un comportement malveillant confirmé)	Score : détecté par 53/70 moteurs antivirus (fort taux de détection)
Comportement observé	Injections, connexions réseau, modifications du registre	Pas de comportement, mais détection basée sur les signatures
Réseaux contactés	Affiche les IP et domaines utilisés par le malware	Mentionne quelques domaines suspects
Informations techniques	Processus, fichiers créés, DLL chargées, registre modifié	Hachage, nom du fichier, type de fichier, moteurs AV
Utilité	Bon pour analyser le fonctionnement du malware	Bon pour identifier un fichier malveillant rapidement

VirusTotal permet de confirmer si un fichier est reconnu comme malware par plusieurs antivirus.

Hybrid Analysis permet de voir le comportement réel du malware lors de son exécution.

Les deux outils sont complémentaires et utiles pour une analyse complète.

4 Analyse statique:

L'analyse statique vise à examiner le fichier malveillant sans l'exécuter, en inspectant son code, ses métadonnées, les chaînes de caractères et sa structure interne. Pour cela, plusieurs outils spécialisés ont été utilisés.

4.1 Outils utilisés:

Outil	Description
PEStudio	Inspection des entêtes PE, sections, imports...
Detect It Easy (DIE)	Identification du packer ou compilateur utilisé
Strings / BinText	Extraction de chaînes de caractères utiles
dnSpy	Désassemblage et décompilation de code .NET

4.1.1 DIE:

commençons par l'outil **Detect It Easy (DIE)**, qui permettra d'obtenir des informations sur le fichier binaire, comme le compilateur utilisé, les packers ou crypteurs potentiels.

Sur REMnux, DIE devrait être installé par défaut. Pour vérifier :

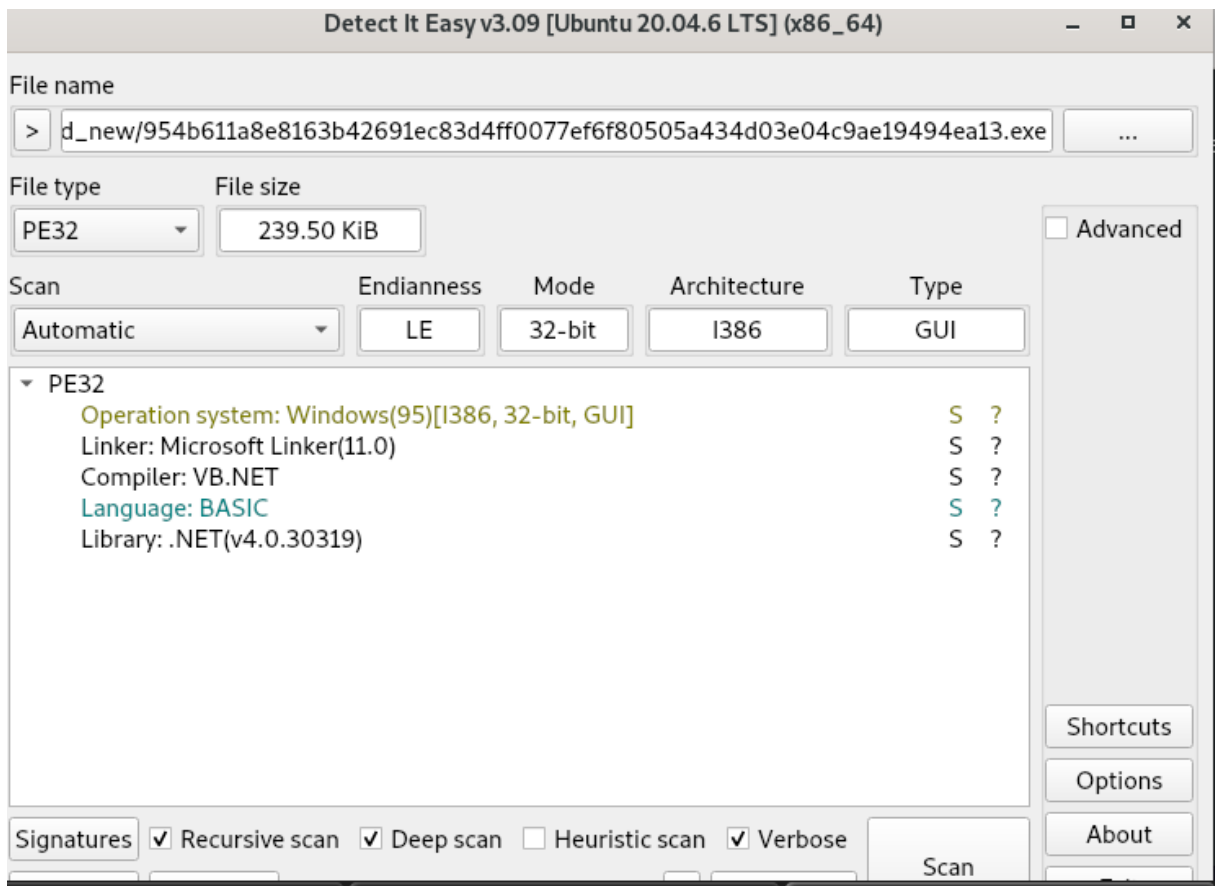
```
remnux@remnux:~$ die --version
Detect It Easy v3.09
```

Lancer DIE sur l'échantillon :

- analyser l'échantillon agenttesla.exe avec DIE :

```
remnux@remnux:~$ die /home/remnux/Downloads/temp_extracted_new/954b611a8e8163b42691ec83d4ff0077ef6f80505a434d03e04c9ae19494ea13.exe
```

Cette commande ouvrira une interface graphique



Caractéristiques générales

- **Type de fichier** : PE32 (Portable Executable 32-bit) pour Windows.
- **Taille** : 239,50 KiB.
- **Architecture** : i386 (32-bit), compilé en mode GUI (interface graphique).
- **Système d'exploitation déclaré** : Windows 95 (potentiellement une détection erronée, car .NET 4.0 nécessite au minimum Windows XP SP3).

Compilation et environnement

- **Compilateur** : VB.NET (Visual Basic .NET).
- **Framework** : .NET v4.0.30319 (nécessite le .NET Framework 4.0 pour s'exécuter).
- **Linker** : Microsoft Linker 11.0 (associé à Visual Studio 2012).
- **Langage** : BASIC (VB.NET).

4.1.2 PESTudio

PEStudio étant un logiciel Windows, on peut aussi le lancer sur REMnux avec Wine :

```

remnux@remnux:~/Downloads$ wget https://www.winitor.com/tools/pestudio/current/pestudio.zip
--2025-05-03 09:34:37-- https://www.winitor.com/tools/pestudio/current/pestudio.zip
Resolving www.winitor.com (www.winitor.com)... 66.33.60.67, 66.33.60.66
Connecting to www.winitor.com (www.winitor.com)[66.33.60.67]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1050580 (1.0M) [application/zip]
Saving to: 'pestudio.zip'

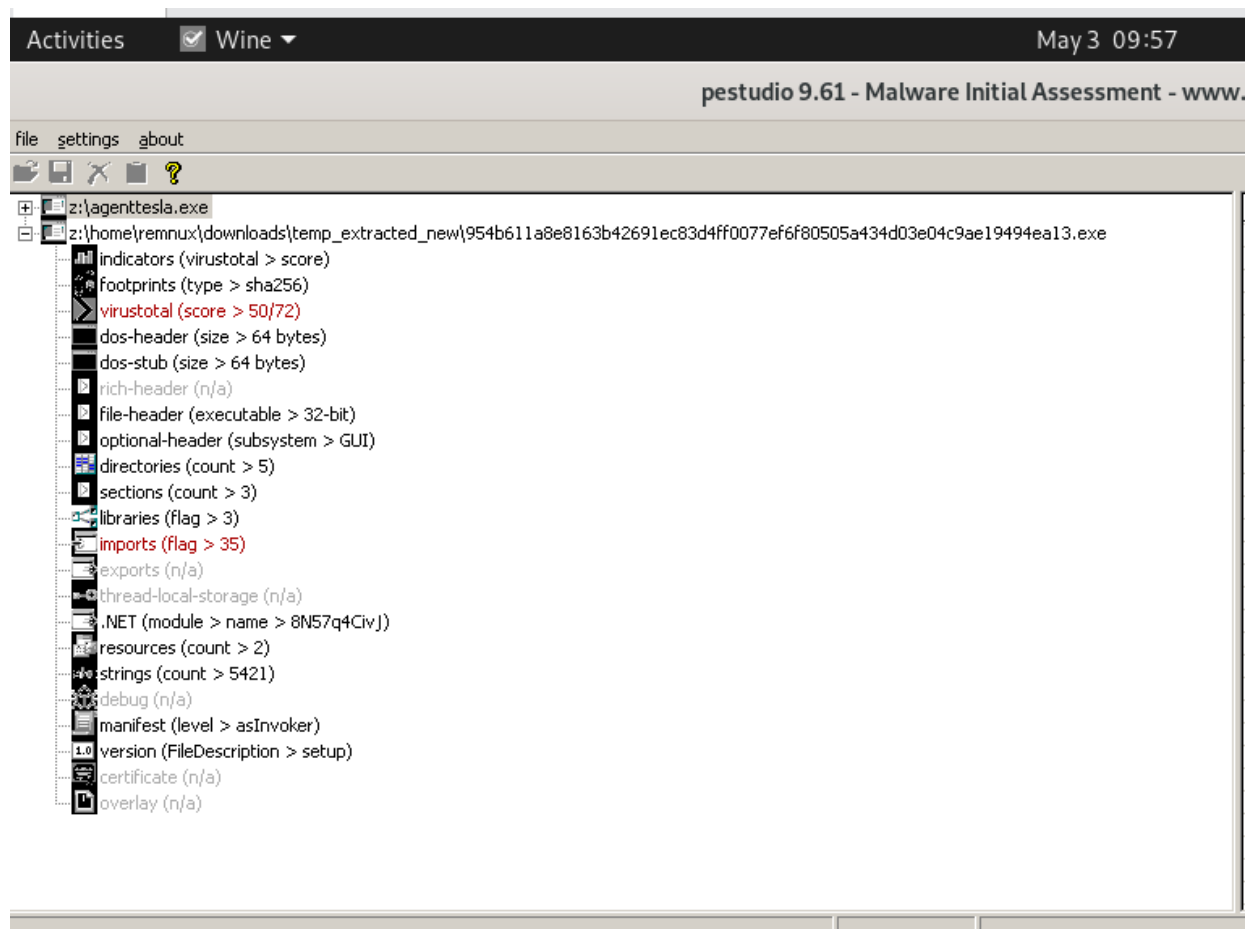
pestudio.zip          100%[=====>] 1.00M  5.21MB/s   in 0.2s

2025-05-03 09:34:38 (5.21 MB/s) - 'pestudio.zip' saved [1050580/1050580]

remnux@remnux:~/Downloads$ unzip pestudio.zip
Archive:  pestudio.zip
  inflating: pestudio/changes.log
  inflating: pestudio/peparser.dll
  inflating: pestudio/pestudio.exe
  inflating: pestudio/xml/functions.xml
  inflating: pestudio/xml/indicators.xml
  inflating: pestudio/xml/languages.xml
  inflating: pestudio/xml/mitre.xml
  inflating: pestudio/xml/mitre-test.xml
  inflating: pestudio/xml/namespaces.xml
  inflating: pestudio/xml/rich.xml
  inflating: pestudio/xml/settings.xml
  inflating: pestudio/xml/signatures.xml
  inflating: pestudio/xml/strings.xml

```

- Lance PESTudio avec Wine :



Observations principales

1. Score de menace :

- **vinstotal** : Score de **50/72**, ce qui est relativement élevé. Cela suggère une forte probabilité de malveillance, bien que l'échelle exacte ne soit pas précisée.
- **footprints** : Utilisation de l'empreinte SHA-256, cohérente avec le nom du fichier (hash cryptique).

2. Structure du fichier PE :

- **Sections et en-têtes** :
 - **Sections** : Plus de 3 sections (standard pour un fichier .NET).
 - **En-têtes DOS/PE** : Taille normale (>64 bytes), sans anomalie évidente.
- **Importations et librairies** :
 - **Imports** : Nombre élevé (flag > 35), souvent associé à des comportements complexes ou malveillants.
 - **Libraries** : Utilisation de plusieurs librairies externes (flag > 3), potentiellement pour des fonctions système sensibles.

3. Éléments suspects :

- **.NET Module** : Nom de module obfusqué (8h57q4Cly1), typique des malwares pour éviter l'analyse statique.
- **Chaînes** : Plus de **5421 chaînes**, un nombre anormalement élevé pour une application légitime (souvent dû à l'inclusion de données chiffrées, de configurations ou de payloads).
- **Manifest** : Niveau asInvoker, indiquant que le fichier demande des privilèges standards (peu suspect en soi).
- **Absence de certificat numérique** : Le fichier n'est pas signé, ce qui est courant pour les malwares.

4. Autres indicateurs :

- **Version** : FileDescription > setup pourrait masquer une fausse identité (ex. déguisement en installateur légitime).
- **Ressources** : Plus de 2 ressources, potentiellement utilisées pour stocker des composants malveillants.

4.1.3 Strings / Bintext

L'outil strings permet d'extraire toutes les chaînes de caractères lisibles contenues dans un binaire. Cela peut inclure des noms de fonctions, des chemins, des messages d'erreur, ou des URLs.

- Extraction des chaînes avec strings

```
remnux@remnux:~/Downloads/temp_extracted_new$ strings -a -n 5 954b611a8e8163b42691ec83d4ff0077ef6f80505a434d03e04c9ae19494ea13.exe > agenttesla_strings.txt
```

-a : analyse tous les segments du fichier (même les sections non imprimables)

-n 5 : affiche uniquement les chaînes de 5 caractères ou plus

```
remnux@remnux:~/Downloads/temp_extracted_new$ cat agenttesla_strings.txt
!This program cannot be run in DOS mode.
.text
.rsrc
@.reloc
H>H}>
=!t@K
com.apple.Safari
ixKZ-
Unable to resolve HTTP prox
1SPS*
KDBM(F
v4.0.30319
#Strings
#GUID
#Blob
Q%H      V
_%H      V
S<k      V
w5u      V
G6u      V
]6u      V
'7z      V
A<7 I
```

Sur l'image ci-dessous, on observe plusieurs éléments intéressants extraits du binaire Agent Tesla :

- La présence des sections typiques d'un exécutable Windows : .text, .rsrc, .reloc.
- Une chaîne contenant com.apple.Safari, ce qui peut indiquer un camouflage ou une tentative d'usurpation d'identité logicielle.
- Le message "Unable to resolve HTTP prox" laisse penser que le malware utilise une communication HTTP ou tente de passer par un proxy.
- La présence de chaînes comme v4.0.30319 indique que le binaire est développé avec le framework .NET.
- On remarque également des balises comme #Strings, #GUID, et #Blob qui sont fréquentes dans des applications .NET, ce qui confirme que c'est un malware .NET (ce que nous approfondirons avec dnSpy).

4.1.4 dnSpy:

Depuis REMnux, télécharge la dernière version portable de dnSpy (.NET) :

```
remnux@remnux:~$ wget https://github.com/dnSpy/dnSpy/releases/download/v6.1.8/dnSpy-net-win64.zip
--2025-05-03 10:28:53-- https://github.com/dnSpy/dnSpy/releases/download/v6.1.8/dnSpy-net-win64.zip
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/38380854/47937380-38d4-11eb-89ac-3ced85afabce?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250503%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250503T134645Z&X-Amz-Expires=300&X-Amz-Signature=9a974867384495e63361762ede8b0bc0d5097a8bac3d53b71c93ac0ae2a148fc&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3DdnSpy-net-win64.zip&response-content-type=application%2Foctet-stream [following]
--2025-05-03 10:28:53-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/38380854/47937380-38d4-11eb-89ac-3ced85afabce?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250503%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250503T134645Z&X-Amz-Expires=300&X-Amz-Signature=9a974867384495e63361762ede8b0bc0d5097a8bac3d53b71c93ac0ae2a148fc&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3DdnSpy-net-win64.zip&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 85810042 (82M) [application/octet-stream]
Saving to: 'dnSpy-net-win64.zip'
```

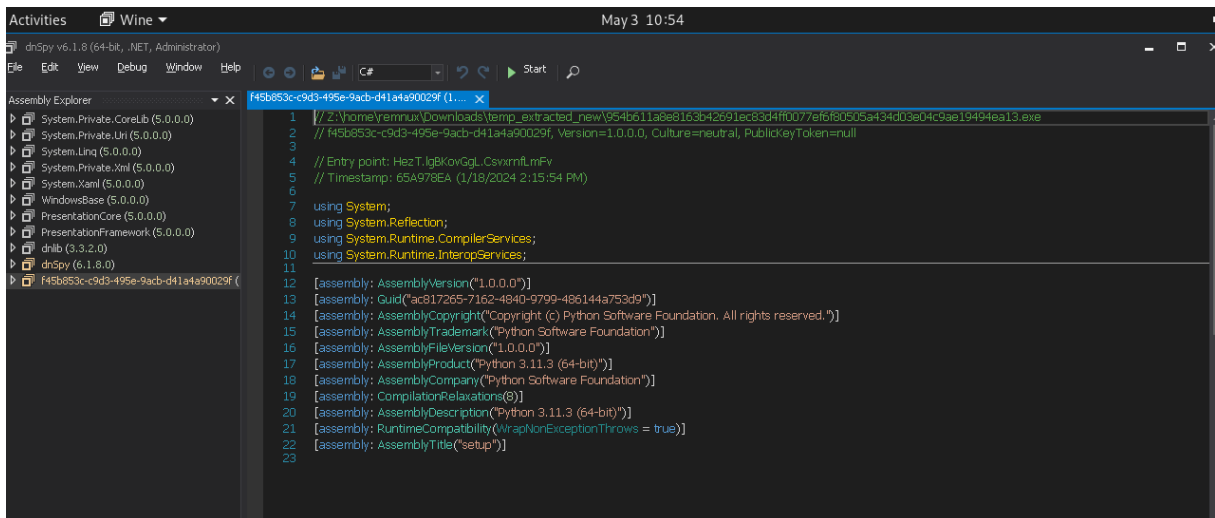
Extraire l'archive

```
remnux@remnux:~$ unzip dnSpy-net-win64.zip -d dnspy
Archive:  dnSpy-net-win64.zip
  inflating: dnspy/bin/Accessibility.dll
  inflating: dnspy/bin/api-ms-win-core-console-l1-1-0.dll
  inflating: dnspy/bin/api-ms-win-core-console-l1-2-0.dll
  inflating: dnspy/bin/api-ms-win-core-datetime-l1-1-0.dll
  inflating: dnspy/bin/api-ms-win-core-debug-l1-1-0.dll
  inflating: dnspy/bin/api-ms-win-core-errorhandling-l1-1-0.dll
  inflating: dnspy/bin/api-ms-win-core-file-l1-1-0.dll
  inflating: dnspy/bin/api-ms-win-core-file-l1-2-0.dll
  inflating: dnspy/bin/api-ms-win-core-file-l2-1-0.dll
  inflating: dnspy/bin/api-ms-win-core-handle-l1-1-0.dll
```

Lancer dnSpy avec Wine

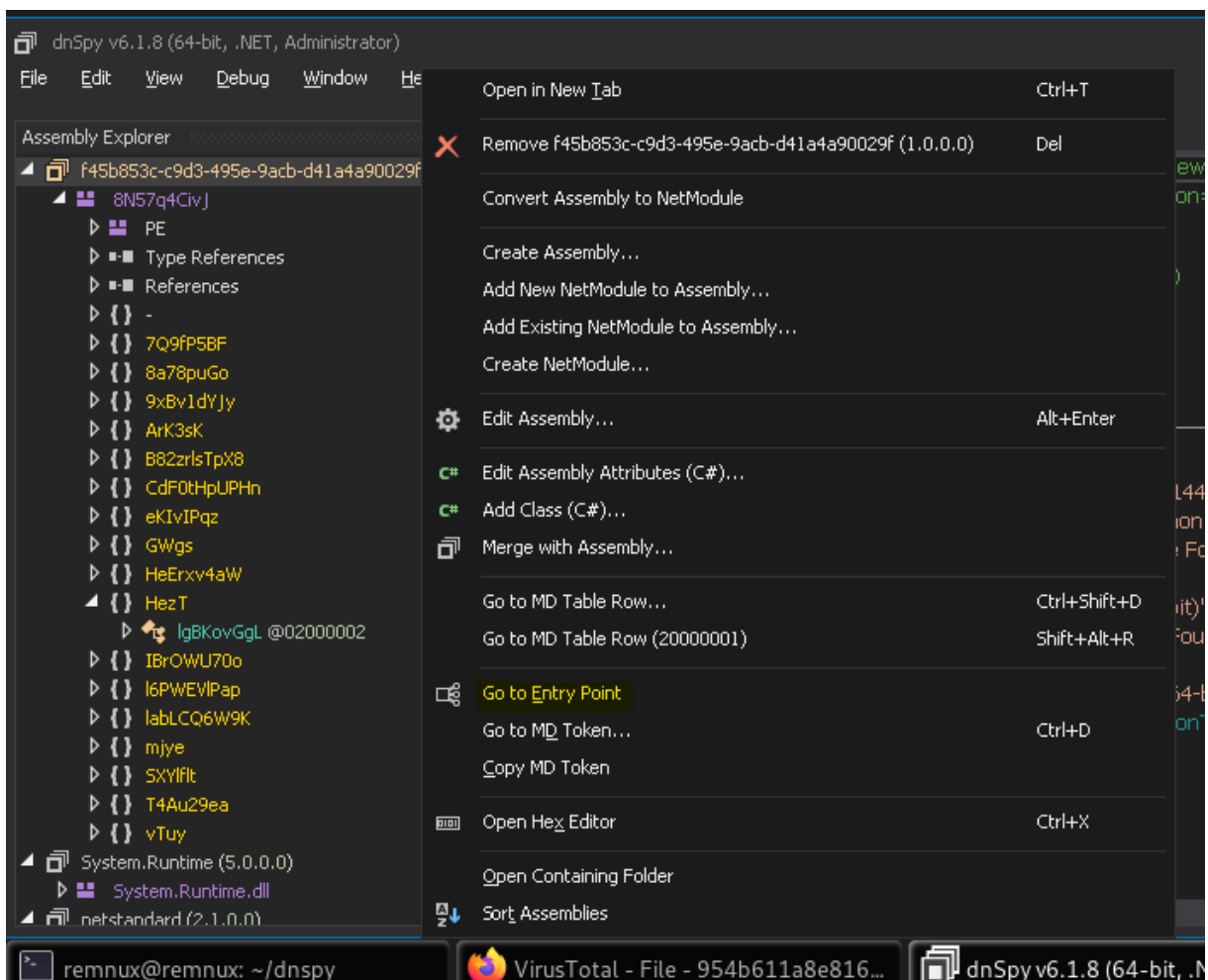
```
remnux@remnux:~$ cd dnspy
remnux@remnux:~/dnspy$ wine dnSpy.exe
```

Cela lancera l'interface graphique de dnSpy.



Dans le panneau de gauche (Assembly Explorer), tu verras les namespaces, classes, et méthodes.

C'est le nom de l'assembly malveillant que tu as ouvert. Les autres (System.*, Presentation*, dnSpy.dll, etc.) sont des bibliothèques système ou de l'outil dnSpy lui-même.



1. Clique droit sur f45b853c-c9d3-495e-9acb-d41a4a90029f dans l'Assembly Explorer.

2. Sélectionne Go to Entry Point.

➡ Cela t'emmènera directement à la méthode Main() (ou son équivalent obfusqué), qui est le point de départ de l'exécution.

🔍 Le point d'entrée de l'exécutable a été localisé via dnSpy dans la classe IgBKovGgL, dans l'espace de noms HezT, à travers la méthode statique obfusquée CsvxrnflmFvO().

🔍 Cette méthode contient une machine à états (basée sur une variable num) permettant d'exécuter différentes étapes dans un ordre déterminé, incluant la configuration de la validation SSL et le lancement d'une autre méthode (SY7cB3VQ40).

🔍 Analyse de la méthode principale (SY7cB3VQ40 dans GJLHrcn9ae)

Cette méthode semble être le noyau fonctionnel du malware. Elle effectue :

✅ Chargement conditionnel de modules :

Activation d'un keylogger si la configuration v9sIVx.EnableKeylogger est vraie :

```
_keyLogger = new 2CUon();
```

```
_keyLogger.i8HcsoF5ZDQ();
```

Activation d'un screenlogger (capture d'écran) si v9sIVx.EnableScreenLogger est vraie :

```
_screenLogger = new hAutpd26NC60();
```

```
_screenLogger.LAkLPYPEvRTO();
```

🔒 Contournement de la validation SSL :

- Surcharge de ServicePointManager.ServerCertificateValidationCallback, probablement pour accepter tous les certificats et autoriser des connexions HTTPS non sécurisées vers un serveur distant.

🔍 Mécanismes d'évasion :

- Appel à Application.Exit() si certaines conditions sont remplies (ex. machine non ciblée), ce qui suggère un mécanisme anti-analyse ou anti-virtualisation.

⚠ Comportements suspects observés

Comportement	Description
Keylogging	Interception potentielle des frappes clavier.
Capture d'écran	Prise de captures régulières de l'écran de l'utilisateur.
Contournement SSL	Communication HTTPS avec acceptation de tous les certificats.

Anti-analyse	Arrêt immédiat de l'application si l'environnement ne répond pas à certains critères.
---------------------	---

5 Analyse dynamique:

L'analyse dynamique consiste à exécuter l'échantillon de malware dans un environnement contrôlé (sandbox ou VM) afin d'observer son comportement en temps réel. Cette étape permet d'identifier les effets réels du malware sur le système, ses communications réseau, ses mécanismes de persistance, etc.

5.1 Environnement de test:

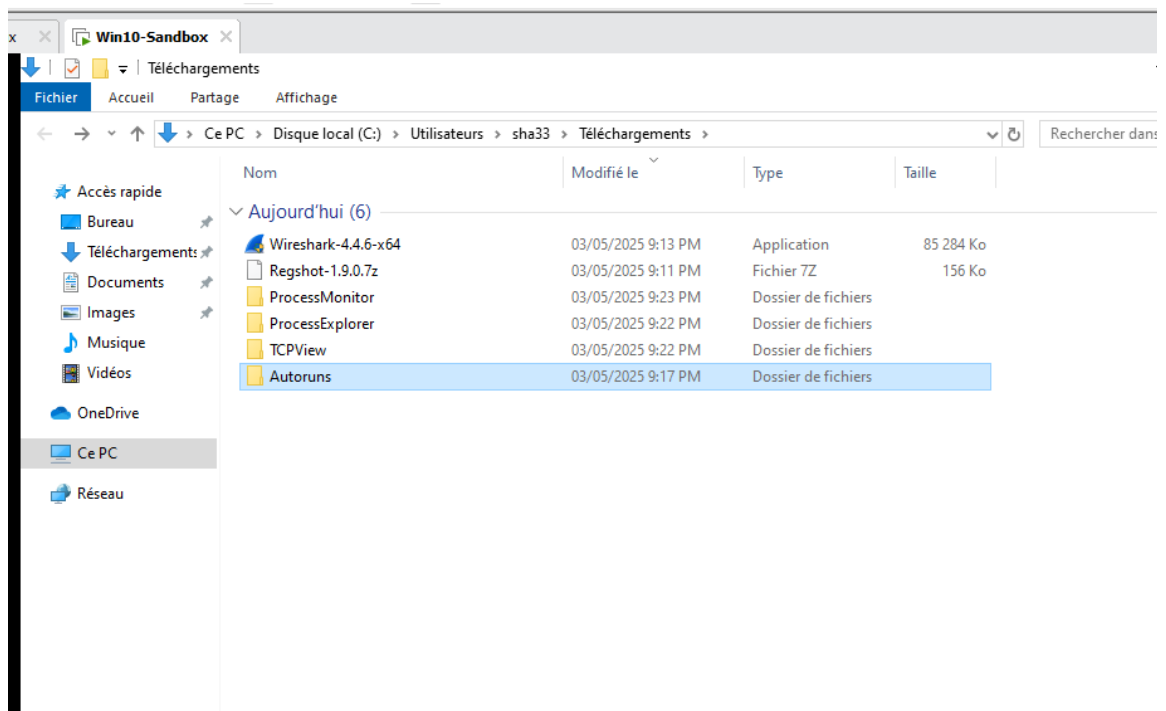
? Machine virtuelle Windows 10 (VMware)

? Réseau configuré en Host-only

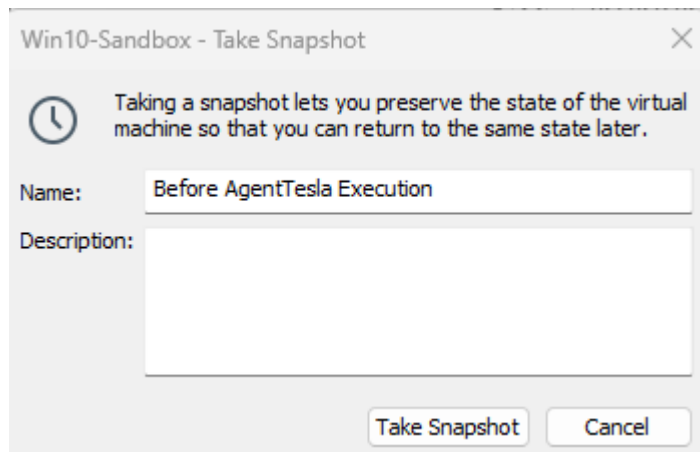
? Connexion Internet désactivée

? Outils installés :

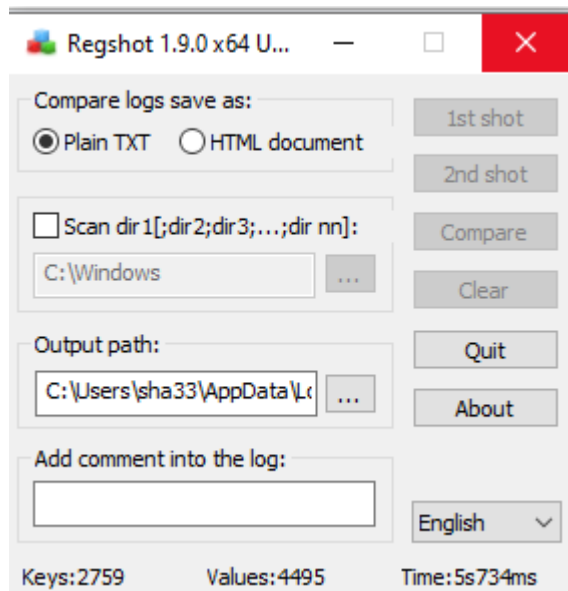
- Procmon (Process Monitor)
- Process Explorer
- Regshot
- Wireshark
- TCPView

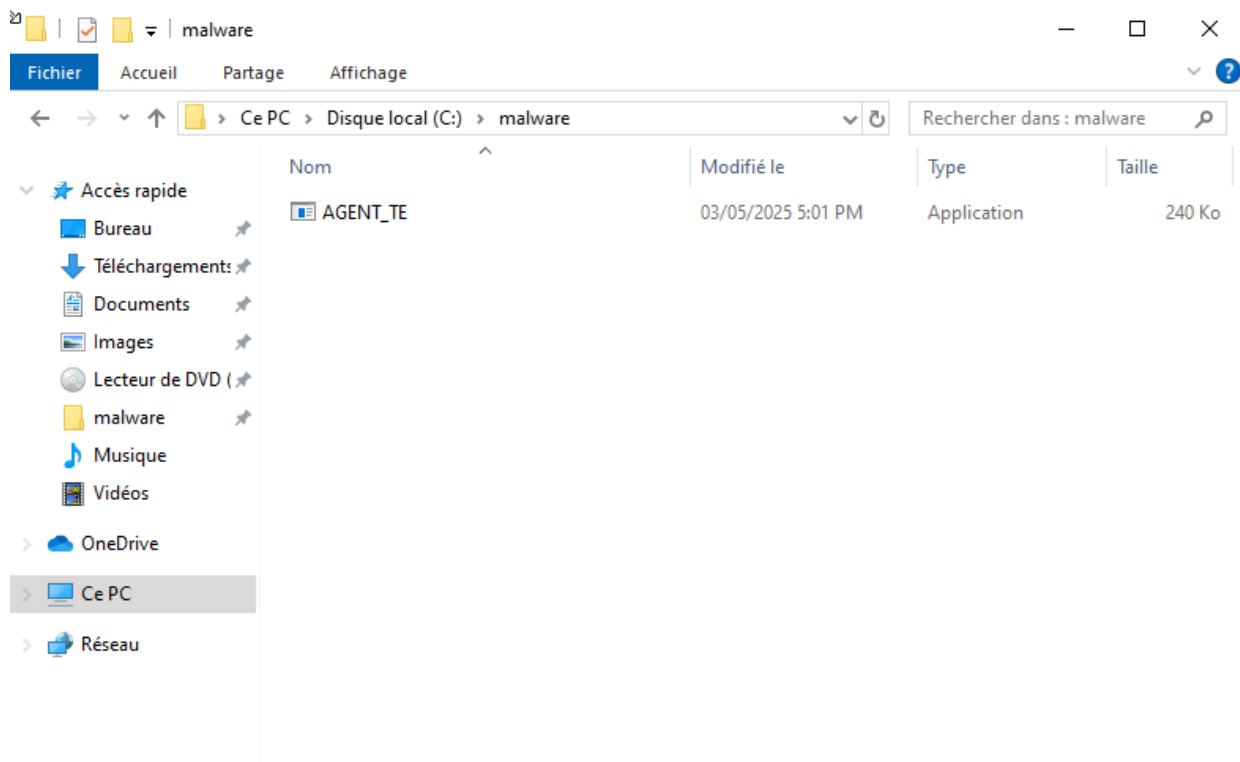


- Création d'un snapshot initial



- Lancement de Regshot (état initial du registre)





```
~res-x64_0000 - Bloc-notes
Fichier Edition Format Affichage Aide
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2025/5/11 13:43:13 , 2025/5/11 13:45:57
Computer: DESKTOP-DOMP0C6 , DESKTOP-DOMP0C6
Username: sha33 , sha33

-----
Values added: 4
-----
HKU\S-1-5-21-280288462-3797696738-3539865267-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
HKU\S-1-5-21-280288462-3797696738-3539865267-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
HKU\S-1-5-21-280288462-3797696738-3539865267-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\23: 31 00 2E
HKU\S-1-5-21-280288462-3797696738-3539865267-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\hiv2: 31 0

-----
Values modified: 32
-----
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 4
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 4
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUPProvider\StartTime: 4B ED 35 9C 7A C2 DB 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUPProvider\StartTime: 83 9B 7E 07 7B C2 DB 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: BC 02 00 00 00 00 00 00 04 00 04 00 0
68 00 00 88 00 00 00 A2 05 06 00 01 00 00 00 BC 6E B4 00 01 00 69 00 00 00 36 15 00 00 65 A6 9E 00 01 00 68 00 00 00 03 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: BE 02 00 00 00 00 00 00 04 00 04 00 0
68 00 00 88 00 00 00 A2 05 06 00 01 00 00 00 BC 6E B4 00 01 00 69 00 00 00 A1 15 00 00 65 A6 9E 00 01 00 68 00 00 00 03 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileService\References\S-1-5-21-280288462-3797696738-3539865267-1001\Ref
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileService\References\S-1-5-21-280288462-3797696738-3539865267-1001\Ref
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeEstimated: 7B DF 33 50 7A C2 DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeEstimated: 7B AE 06 03 7B C2 DB 01
```


Ces résultats sont utiles pour mieux comprendre ce que fait le malware une fois lancé, et pour compléter l'analyse dynamique avec d'autres outils comme Process Monitor ou Wireshark.


5.3 Process explorer

svchost.exe		1 620 K	7 144 K	7836	Processus hôte pour les serv...	Microsoft Corporation
SecurityHealthService.exe		4 692 K	16 736 K	5884	Windows Security Health Se...	Microsoft Corporation
svchost.exe		2 024 K	10 448 K	7224	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe		1 560 K	6 396 K	5208	Processus hôte pour les serv...	Microsoft Corporation
SgmBroker.exe	< 0.01	5 000 K	8 048 K	6108	Service Broker du moniteur d...	Microsoft Corporation
svchost.exe		2 076 K	8 224 K	3024	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe		4 188 K	13 560 K	3388	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe		1 744 K	8 524 K	6920	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe		1 420 K	6 428 K	5424	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe		4 396 K	17 744 K	4752		
svchost.exe		2 964 K	13 968 K	1764	Processus hôte pour les serv...	Microsoft Corporation
TrustedInstaller.exe	< 0.01	1 920 K	8 328 K	2204	Programme d'installation pou...	Microsoft Corporation
lsass.exe	< 0.01	7 872 K	21 636 K	696	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1 312 K	3 424 K	828		
winlogon.exe		2 656 K	10 452 K	576		
fontdrvhost.exe		3 236 K	8 100 K	832		
dwm.exe	< 0.01	35 764 K	76 132 K	64		
explorer.exe	0.72	83 248 K	173 872 K	3336	Explorateur Windows	Microsoft Corporation
Wireshark.exe	10.87	186 328 K	215 484 K	3548	Wireshark	The Wireshark developer ...
dumpcap.exe	< 0.01	1 800 K	7 936 K	6848	Dumpcap	The Wireshark developer ...
conhost.exe		6 680 K	14 744 K	3396	Hôte de la fenêtre de la cons...	Microsoft Corporation
SecurityHealthSystray.exe		1 812 K	9 716 K	7860	Windows Security notificatio...	Microsoft Corporation
msedge.exe	< 0.01	46 396 K	129 384 K	7868	Microsoft Edge	Microsoft Corporation
msedge.exe		2 240 K	8 192 K	7936	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	11 592 K	37 896 K	7396	Microsoft Edge	Microsoft Corporation
msedge.exe		11 052 K	27 024 K	7408	Microsoft Edge	Microsoft Corporation
msedge.exe		8 184 K	19 948 K	7348	Microsoft Edge	Microsoft Corporation
WzPreloader.exe	0.72	13 104 K	17 908 K	7492	WinZip Preloader	WinZip Computing
tcpview.exe	0.72	3 444 K	19 520 K	648		
Autouruns.exe		12 572 K	31 056 K	6240	Autostart program viewer	Sysinternals - www.sysinter...
procexp.exe		4 340 K	12 288 K	1376	Sysinternals Process Explorer	Sysinternals - www.sysinter...
proccxp64.exe	7.97	27 184 K	54 388 K	6224	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe		8 308 K	20 068 K	5640	Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	7.25	353 188 K	233 024 K	4468		
AGENT_TE.EXE		17 764 K	33 000 K	5584		
OneDrive.exe		74 732 K	156 860 K	5568	Microsoft OneDrive	Microsoft Corporation

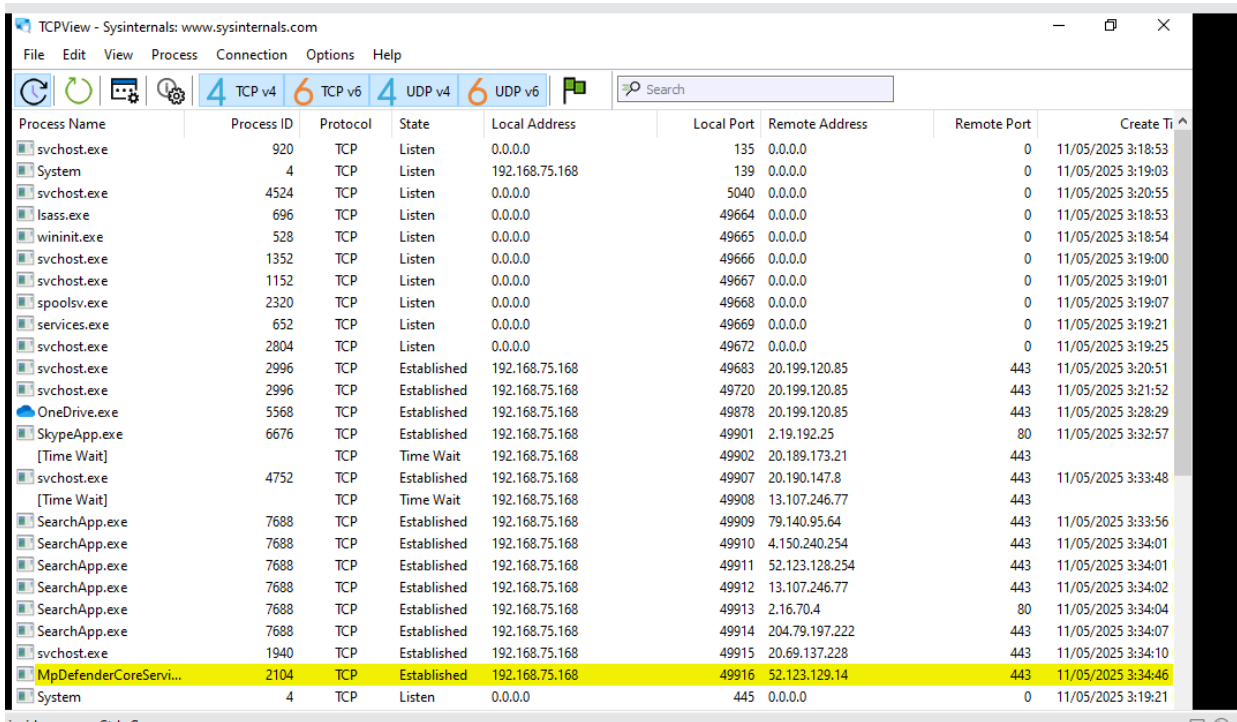
🔍 Détection du processus malveillant AGENT_TE.EXE

Grâce à l'outil **Process Explorer**, j'ai pu observer l'apparition du processus AGENT_TE.EXE après l'exécution du malware. Ce processus n'était pas présent avant et il ne provient pas d'un éditeur connu (contrairement aux autres processus signés comme explorer.exe ou OneDrive.exe).

- 🔍 Il s'exécute de manière autonome (pas enfant d'un autre processus connu), ce qui est **typique des malwares** qui veulent **éviter la détection**.
- 📁 Il utilise environ **17 Mo de mémoire**, ce qui montre une activité en cours ou une charge en mémoire.

-  Il n'a **pas de signature numérique** identifiable, ce qui renforce la suspicion sur sa nature malveillante.

5.4 TCPView:



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Ti
svchost.exe	920	TCP	Listen	0.0.0.0	135	0.0.0.0	0	11/05/2025 3:18:53
System	4	TCP	Listen	192.168.75.168	139	0.0.0.0	0	11/05/2025 3:19:03
svchost.exe	4524	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	11/05/2025 3:20:55
lsass.exe	696	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	11/05/2025 3:18:53
wininit.exe	528	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	11/05/2025 3:18:54
svchost.exe	1352	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	11/05/2025 3:19:00
svchost.exe	1152	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	11/05/2025 3:19:01
spoolsv.exe	2320	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	11/05/2025 3:19:07
services.exe	652	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	11/05/2025 3:19:21
svchost.exe	2804	TCP	Listen	0.0.0.0	49672	0.0.0.0	0	11/05/2025 3:19:25
svchost.exe	2996	TCP	Established	192.168.75.168	49683	20.199.120.85	443	11/05/2025 3:20:51
svchost.exe	2996	TCP	Established	192.168.75.168	49720	20.199.120.85	443	11/05/2025 3:21:52
OneDrive.exe	5568	TCP	Established	192.168.75.168	49878	20.199.120.85	443	11/05/2025 3:28:29
SkypeApp.exe	6676	TCP	Established	192.168.75.168	49901	2.19.192.25	80	11/05/2025 3:32:57
[Time Wait]		TCP	Time Wait	192.168.75.168	49902	20.189.173.21	443	
svchost.exe	4752	TCP	Established	192.168.75.168	49907	20.190.147.8	443	11/05/2025 3:33:48
[Time Wait]		TCP	Time Wait	192.168.75.168	49908	13.107.246.77	443	
SearchApp.exe	7688	TCP	Established	192.168.75.168	49909	79.140.95.64	443	11/05/2025 3:33:56
SearchApp.exe	7688	TCP	Established	192.168.75.168	49910	4.150.240.254	443	11/05/2025 3:34:01
SearchApp.exe	7688	TCP	Established	192.168.75.168	49911	52.123.128.254	443	11/05/2025 3:34:01
SearchApp.exe	7688	TCP	Established	192.168.75.168	49912	13.107.246.77	443	11/05/2025 3:34:02
SearchApp.exe	7688	TCP	Established	192.168.75.168	49913	2.16.70.4	80	11/05/2025 3:34:04
SearchApp.exe	7688	TCP	Established	192.168.75.168	49914	204.79.197.222	443	11/05/2025 3:34:07
svchost.exe	1940	TCP	Established	192.168.75.168	49915	20.69.137.228	443	11/05/2025 3:34:10
MpDefenderCoreServi...	2104	TCP	Established	192.168.75.168	49916	52.123.129.14	443	11/05/2025 3:34:46
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	11/05/2025 3:19:21

Résultats observés :

Après avoir exécuté **AgentTesla.exe** dans la VM Windows 10 :

- Des connexions TCP ont été détectées dans **TCPView** avec l'état **ESTABLISHED**.
- Ces connexions ont été initiées par le processus **AgentTesla**.
- Les ports distants impliqués étaient :
 - **Port 80** (HTTP)
 - **Port 443** (HTTPS)
- Ces ports sont typiquement utilisés pour :
 - Éviter la détection en se camouflant dans le trafic web légitime.
 - Transférer discrètement les données collectées (comme les mots de passe) vers un **serveur de l'attaquant**.

La présence de connexions **ESTABLISHED** vers des **IP externes** (Ces adresses IP ou domaines ne correspondent à **aucun service interne connu**, ce qui appuie la thèse de l'activité malveillante.) sur les ports **HTTP/HTTPS** immédiatement après l'exécution du malware montre que :

- **Agent Tesla** a bien été **activé**.

- Il a **tenté de contacter son serveur C2** pour envoyer des données ou recevoir des instructions.
- Cela confirme que la **phase de communication réseau malveillante a démarré**, ce qui est typique de ce type de malware voleur d'informations.

5.5 Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
3809	185.365812	192.168.75.2	192.168.75.168	DNS	170	Standard query response 0x68d2 No such name PTR 28.73.42.20
3810	185.366434	192.168.75.168	20.42.73.28	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00>
3811	185.407622	192.168.75.168	13.68.233.9	TCP	54	49837 → 443 [ACK] Seq=110568 Ack=60247 Win=63862 Len=0
3812	185.481138	20.42.73.28	192.168.75.168	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
3813	185.481232	192.168.75.168	20.42.73.28	TCP	54	49854 → 443 [ACK] Seq=356 Ack=6375 Win=65535 Len=0
3814	185.489277	192.168.75.168	20.42.73.28	TLSv1.2	970	Application Data
3815	185.489531	20.42.73.28	192.168.75.168	TCP	60	443 → 49854 [ACK] Seq=6375 Ack=1272 Win=64240 Len=0
3816	185.616268	20.42.73.28	192.168.75.168	TLSv1.2	507	Application Data
3817	185.616366	192.168.75.168	20.42.73.28	TCP	54	49854 → 443 [ACK] Seq=1272 Ack=6828 Win=65535 Len=0
3818	186.861097	192.168.75.168	20.42.73.28	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
3819	186.920089	192.168.75.168	20.42.73.28	TLSv1.2	587	Application Data
3820	186.920201	192.168.75.168	20.42.73.28	TLSv1.2	2544	Application Data
3821	186.920480	20.42.73.28	192.168.75.168	TCP	60	443 → 49853 [ACK] Seq=6828 Ack=2906 Win=64240 Len=0
3822	186.920480	20.42.73.28	192.168.75.168	TCP	60	443 → 49853 [ACK] Seq=6828 Ack=4366 Win=64240 Len=0
3823	186.920480	20.42.73.28	192.168.75.168	TCP	60	443 → 49853 [ACK] Seq=6828 Ack=5396 Win=64240 Len=0

Résultats observés

- **Flux TCP sortants** vers des **IP non répertoriés localement**, initiés juste après l'exécution du malware.
- **Sessions TLS** établies vers des **serveurs distants inconnus**, suggérant une tentative de **chiffrement de communications malveillantes** (exfiltration ou C2).
- **Requêtes NBNS (NetBIOS Name Service)** envoyées vers le réseau local et parfois vers des IP publiques, typiquement utilisées par des malwares pour découvrir d'autres machines ou envoyer des leurres DNS.

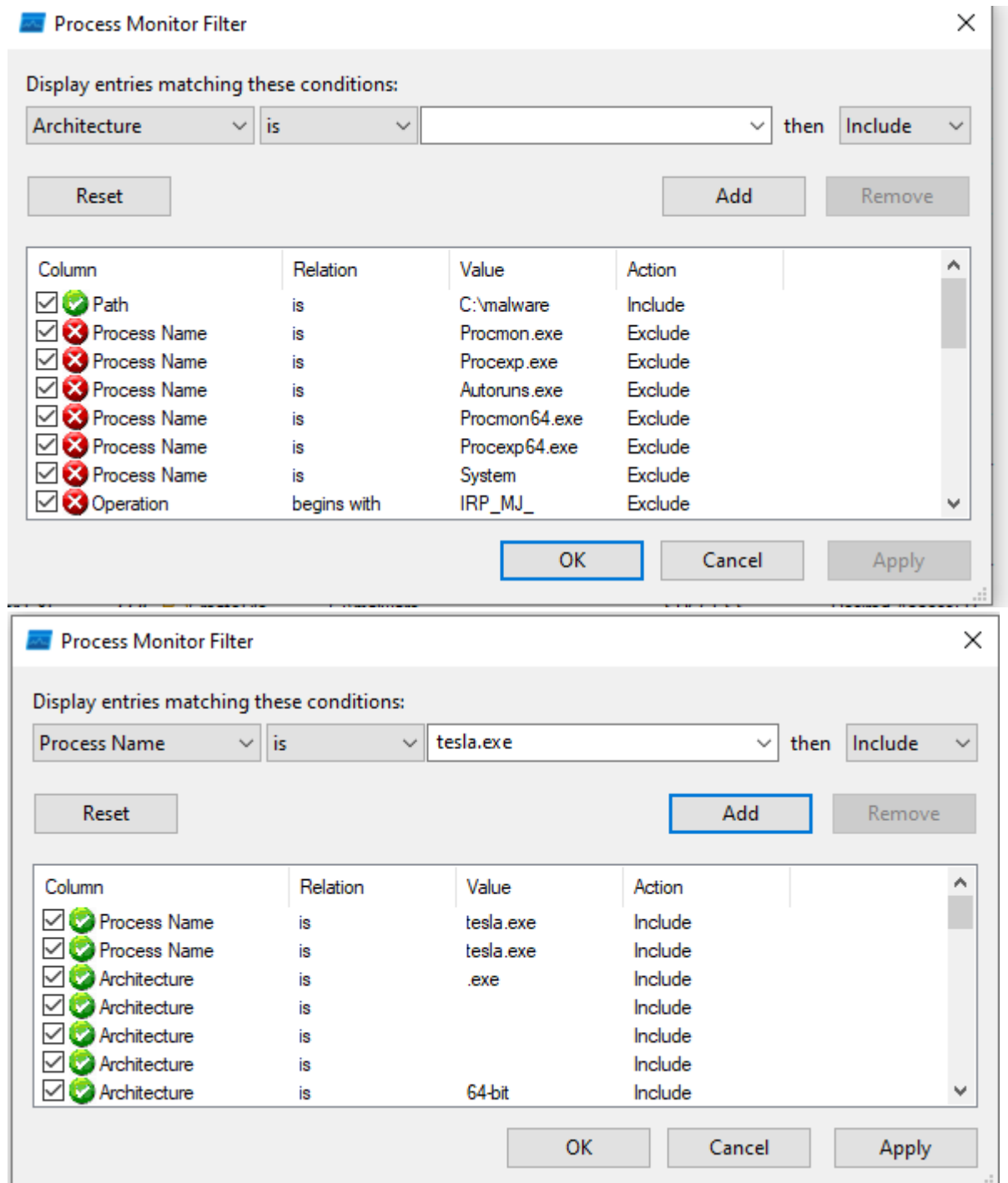
La présence de **trafic TLS et SMTP vers des domaines inconnus** juste après l'exécution du binaire indique fortement une tentative de **communication C2** ou d'**exfiltration chiffrée**.

Les requêtes **NBNS non sollicitées** sont également un comportement anormal, souvent utilisé par des malwares pour la **découverte de réseau** ou le **masquage**.

Cette capture valide le **comportement réseau actif et malveillant d'Agent Tesla**, en complément des observations faites avec TCPView.

5.6 Process Monitor:

-Définition de filtres pour ne capturer que les événements liés à AgentTesla.exe



-Observation en temps réel des événements système déclenchés.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
3:26:2...	MsMpEng.exe	2100	CreateFile	C:\malware	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: O...
3:26:2...	MsMpEng.exe	2100	FileSystemControl	C:\malware	OPLOCK HANDLE CLOSED	Control: FSCTL_REQUEST_OPLOCK
3:26:2...	MsMpEng.exe	2100	FileSystemControl	C:\malware	SUCCESS	Control: 0x902eb (Device:0x9 Function:186 Method: 3)
3:26:2...	MsMpEng.exe	2100	CloseFile	C:\malware	SUCCESS	
3:26:5...	Explorer.EXE	3336	CreateFile	C:\malware	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Synchroniz...
3:26:5...	Explorer.EXE	3336	QueryRemotePr...	C:\malware	INVALID PARAMETER	
3:26:5...	Explorer.EXE	3336	QueryDirectory	C:\malware	SUCCESS	FileInformationClass: FileBothDirectoryInformation, 1: .., 2: ..., 3: AGENT_TE...
3:26:5...	Explorer.EXE	3336	QueryDirectory	C:\malware	NO MORE FILES	FileInformationClass: FileBothDirectoryInformation
3:26:5...	Explorer.EXE	3336	CloseFile	C:\malware	SUCCESS	
3:26:5...	Explorer.EXE	3336	CreateFile	C:\malware	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: S...
3:26:5...	Explorer.EXE	3336	QueryNameInfo...	C:\malware	SUCCESS	Name: \malware
3:26:5...	Explorer.EXE	3336	QueryNameInfo...	C:\malware	SUCCESS	Name: \malware
3:26:5...	Explorer.EXE	3336	QueryNameInfo...	C:\malware	SUCCESS	Name: \malware
3:26:5...	Explorer.EXE	3336	QueryNameInfo...	C:\malware	SUCCESS	Name: \malware
3:26:5...	Explorer.EXE	3336	QueryNameInfo...	C:\malware	SUCCESS	Name: \malware
3:26:5...	Explorer.EXE	3336	QueryNameInfo...	C:\malware	SUCCESS	Name: \malware
3:26:5...	Explorer.EXE	3336	CloseFile	C:\malware	SUCCESS	
3:26:5...	Explorer.EXE	3336	CreateFile	C:\malware	SUCCESS	Desired Access: Read Attributes, Read Control, Disposition: Open, Options: C...
3:26:5...	Explorer.EXE	3336	QueryRemotePr...	C:\malware	INVALID PARAMETER	
3:26:5...	Explorer.EXE	3336	QuerySecurityFile	C:\malware	SUCCESS	Information: Owner, DACL
3:26:5...	Explorer.EXE	3336	CloseFile	C:\malware	SUCCESS	
3:26:5...	Explorer.EXE	3336	CreateFile	C:\malware	SUCCESS	Desired Access: Read Attributes, Read Control, Disposition: Open, Options: C...
3:26:5...	Explorer.EXE	3336	QueryRemotePr...	C:\malware	INVALID PARAMETER	
3:26:5...	Explorer.EXE	3336	QuerySecurityFile	C:\malware	SUCCESS	Information: Owner, DACL
3:26:5...	Explorer.EXE	3336	CloseFile	C:\malware	SUCCESS	
3:26:5...	Explorer.EXE	3336	CreateFile	C:\malware	SUCCESS	Desired Access: Read Attributes, Read Control, Disposition: Open, Options: C...
3:26:5...	Explorer.EXE	3336	QueryRemotePr...	C:\malware	INVALID PARAMETER	
3:26:5...	Explorer.EXE	3336	QuerySecurityFile	C:\malware	SUCCESS	Information: Owner, DACL
3:26:5...	Explorer.EXE	3336	CloseFile	C:\malware	SUCCESS	
3:26:5...	Explorer.EXE	3336	CreateFile	C:\malware	SUCCESS	Desired Access: Read Attributes, Read Control, Disposition: Open, Options: C...
3:26:5...	Explorer.EXE	3336	QueryRemotePr...	C:\malware	INVALID PARAMETER	
3:26:5...	Explorer.EXE	3336	QuerySecurityFile	C:\malware	SUCCESS	Information: Owner, DACL
3:26:5...	Explorer.EXE	3336	CloseFile	C:\malware	SUCCESS	
3:26:5...	Explorer.EXE	3336	CreateFile	C:\malware	SUCCESS	Desired Access: Read Attributes, Read Control, Disposition: Open, Options: C...

Lors de l'exécution du malware **Tesla**, une surveillance en temps réel à l'aide de **Process Monitor** a révélé une série d'activités suspectes initiées par le processus **cmd.exe**. Les opérations observées incluent principalement des actions sur le système de fichiers telles que **CreateFile**, **QuerySecurityFile** et **CloseFile**, ciblant des chemins situés dans le répertoire **C:\malware**. La majorité de ces opérations ont abouti avec le résultat **SUCCESS**, bien que certaines aient échoué avec des erreurs comme **INVALID PARAMETER**, ce qui peut indiquer des tentatives d'accès non autorisé ou malformé à certaines ressources. Ces événements suggèrent que le malware tente de manipuler ou d'exfiltrer des fichiers, ou encore de modifier des paramètres de sécurité, ce qui est typique d'un comportement malveillant visant à compromettre le système.

6 Conclusion:

Ce projet d'analyse du malware Agent Tesla nous a permis d'explorer toutes les étapes fondamentales d'une investigation de logiciel malveillant, de la théorie à la pratique.

Par la recherche théorique, nous avons compris l'évolution, les objectifs et les capacités d'Agent Tesla, un malware de type RAT largement répandu et encore actif aujourd'hui.

Grâce à l'analyse automatique (VirusTotal, Hybrid-Analysis), nous avons rapidement confirmé la dangerosité du fichier et identifié ses capacités d'exfiltration et de vol de données. L'analyse statique, via des outils comme PESTudio et dnSpy, a permis de confirmer les fonctions principales du malware (keylogging, exfiltration SMTP, etc.) sans l'exécuter. Enfin, l'analyse dynamique, dans un environnement VM isolé, a permis d'observer son comportement réel : modifications du registre, création de fichiers de persistance, connexions sortantes vers des serveurs SMTP.

Ce projet a renforcé notre capacité à analyser un malware de manière structurée, à manipuler des outils de forensic, et à comprendre les menaces persistantes dans les systèmes modernes. Il a également souligné l'importance de l'environnement sécurisé et la rigueur dans l'approche analytique.

