

---

# Relazione Tecnica: Analisi Statica Malware Agent Tesla

**Studente :** Rocco Paolo Caccamo

**Ambiente di Analisi:** FlareVM (Windows-based Analysis Lab)

**Stato della Rete:** Isolata (Host-only / Disconnessa)

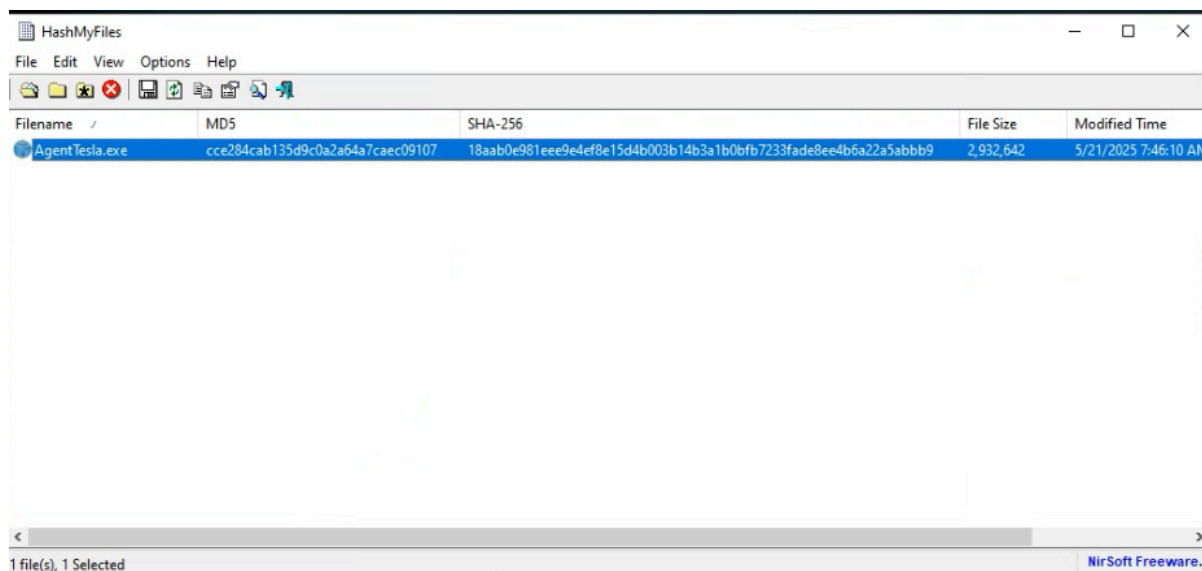
**Data:** 02/02/2026

---

## 1. Fase di Fingerprinting

L'analisi è iniziata con l'identificazione univoca del campione (sample) per garantirne la tracciabilità e permettere future ricerche su database di intelligence. Utilizzando lo strumento **HashMyFiles**, sono stati calcolati gli hash crittografici del file [AgentTesla.exe](#).

- **Algoritmo MD5:** [cce284cab135d9c0a2a64a7caec09107](#).
- **Algoritmo SHA256:**  
[18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9](#).



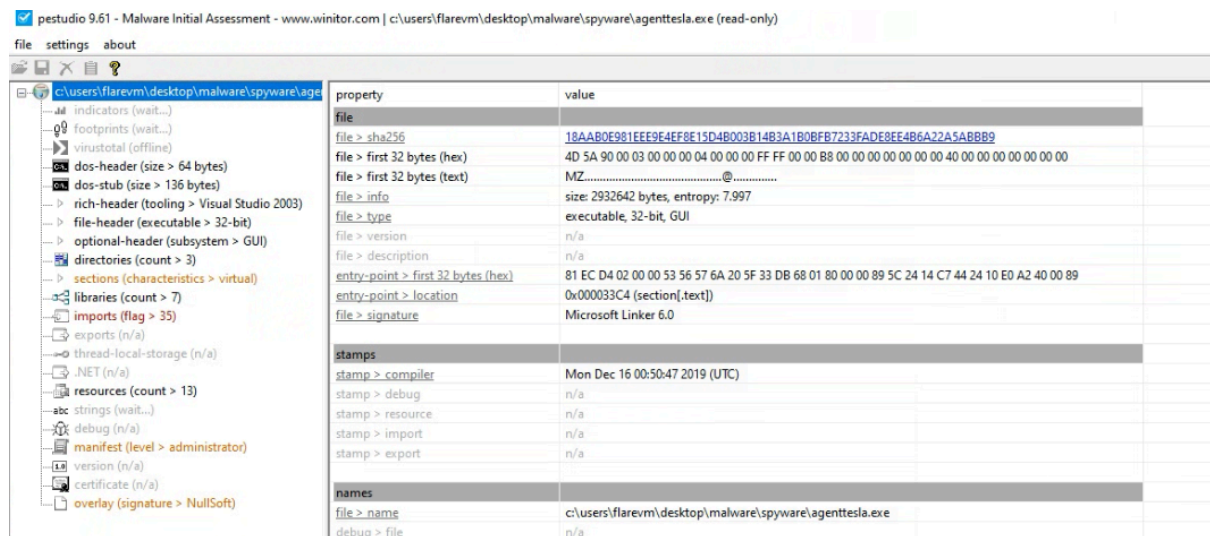
---

## 2. Analisi della Struttura PE (Portable Executable)

Attraverso l'impiego di **PEStudio**, è stata esaminata la struttura interna dell'eseguibile senza procedere alla sua attivazione. I dati raccolti sono sintetizzati nella seguente tabella:

Campo	Valore	Note
Architettura	32-bit (x86)	Eseguibile compatibile con sistemi Windows a 32 e 64 bit.
Timestamp	Mon Dec 16 00:50:47 2019	Datazione compatibile con lo storico del malware Agent Tesla.
Entry Point	0x000033C4	Punto di inizio dell'esecuzione del codice nel segmento <b>.text</b> .
Subsystem	Windows GUI	Il file è compilato come applicazione con interfaccia grafica.

L'analisi ha evidenziato un valore di **entropia estremamente elevato (7.997)**, indicatore critico della presenza di dati compressi o cifrati.



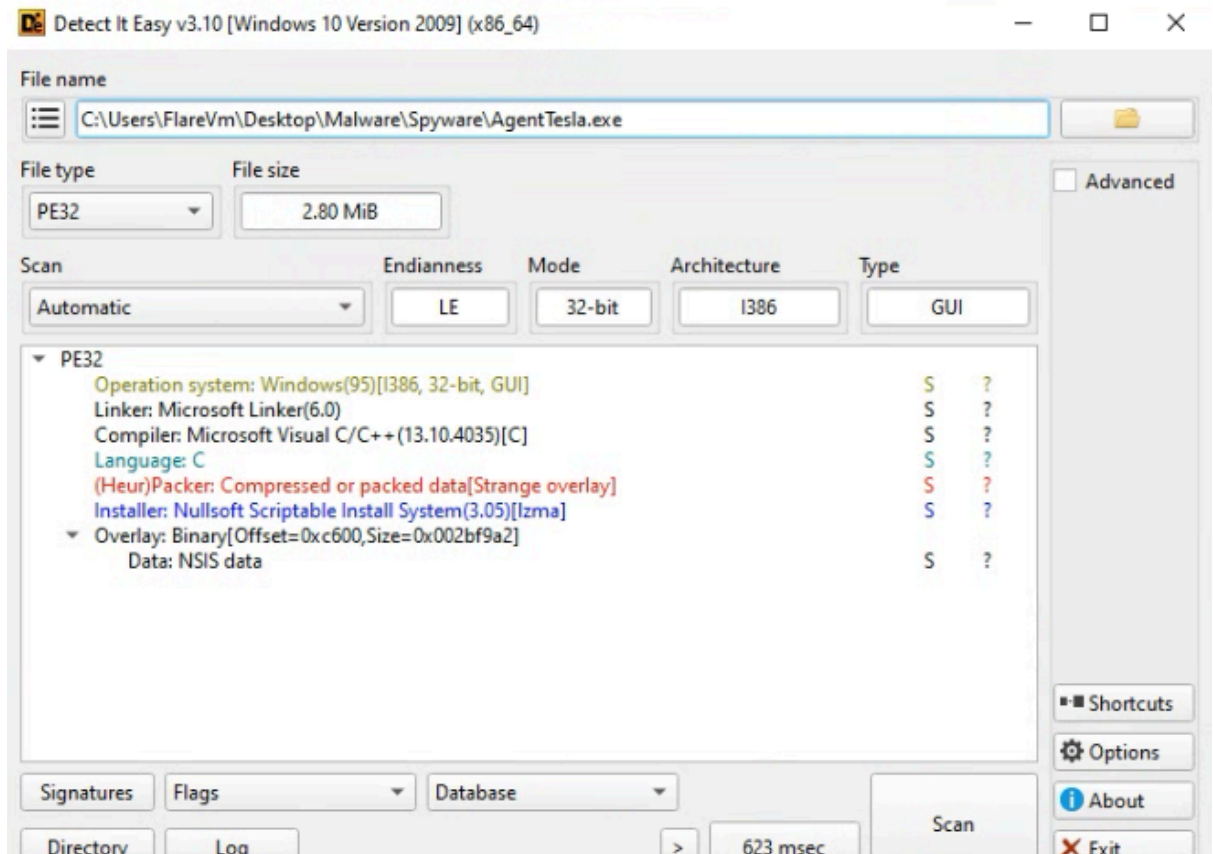
Schermata dei metadati generali in PESTudio

### 3. Rilevamento Packer e Offuscamento

Per confermare la natura del "wrapping" rilevato dall'entropia, è stato utilizzato **Detect It Easy (DiE)**.

- **Packer Rilevato: Nullsoft Scriptable Install System (3.05).**

- **Linguaggio:** Il guscio esterno risulta scritto in **C/C++**, agendo da installer per il payload malevolo.
- **Note su .NET:** Sebbene lo strato esterno sia in C, la letteratura tecnica associa Agent Tesla al framework **.NET**; l'installer NSIS viene utilizzato come tecnica di evasione per nascondere il codice sorgente originale.



Schermata di Detect It Easy con evidenza del packer Nullsoft

## 4. Analisi delle Stringhe e De-packaging Manuale

Data l'impossibilità di estrarre stringhe significative direttamente dall'eseguibile compresso (stato "wait" in PESTudio), è stata eseguita l'estrazione manuale dei componenti tramite 7-Zip.

- **Contenuto Estratto:** L'archivio conteneva script di installazione ([[NSIS](#)].nsi) e diverse librerie dinamiche (DLL).
- **Indicatori di Compromissione (IoC):**
  - **Librerie rilevate:** [Microsoft.Management.Infrastructure.dll](#).
  - **Funzioni individuate:** Riferimenti a processi di **serializzazione e deserializzazione** del codice, tecniche comuni per l'esecuzione di payload residenti esclusivamente in memoria (fileless).
  - **Persistenza:** Individuati riferimenti a directory temporanee e file di configurazione ([UWPHook.exe.config](#)) volti a mantenere il controllo sulla macchina vittima.

The Worst Of All!!!!!!	2/2/2026 7:12 AM	File folder	
[NSIS].nsi	5/21/2025 7:46 AM	NSI File	7 KB
AgentTesla.exe	5/21/2025 7:46 AM	Application	2,864 KB
AgentTesla.exe.zip	2/2/2026 7:12 AM	ZIP File	2,847 KB
butterflyondesktop.exe.zip	2/2/2026 7:12 AM	ZIP File	2,895 KB
HawkEye.exe.zip	2/2/2026 7:12 AM	ZIP File	130 KB
Kakwa.doc.zip	2/2/2026 7:12 AM	ZIP File	37 KB
MaterialDesignColors.dll	5/25/2020 4:53 AM	Application exten...	293 KB
MaterialDesignThemes.Wpf.dll	5/25/2020 4:53 AM	Application exten...	7,247 KB
MaterialDesignThemes.Wpf.xml	5/25/2020 4:53 AM	XML Document	92 KB
Microsoft.Management.Infrastructure.dll	7/17/2017 10:46 AM	Application exten...	36 KB
SharpSteam.dll	5/31/2020 9:26 AM	Application exten...	5 KB
System.Management.Automation.dll	7/17/2017 10:46 AM	Application exten...	352 KB
System.Management.Automation.xml	7/17/2017 10:46 AM	XML Document	6,979 KB
UWPHook.exe	5/31/2020 11:37 AM	Application	831 KB
UWPHook.exe.config	5/31/2020 11:36 AM	Configuration Sou...	2 KB
VDFParser.dll	5/31/2020 9:26 AM	Application exten...	15 KB

## Elenco dei file estratti dall'installer

CFF Explorer VIII - [UWPHook.exe]

File Settings ?

UWPHook.exe

File: UWPHook.exe

- Dos Header
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Relocation Directory
- Debug Directory
- .NET Directory
- MetaData Header
- MetaData Streams
- #~
- Tables Header
- Tables
- #Strings
- #US
- #GUID
- #Blob
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	3C	3E	39	5F	5F	31	31	5F	30	00	3C	42	77	72	5F	<>9_11_0.<Bvr
00000001	44	6F	57	6F	72	6B	3E	62	5F	5F	31	31	5F	30	00	3C	DoWork>b_11_0.<
00000002	3E	63	5F	5F	44	69	73	70	6C	61	79	43	6C	61	73	73	>c_DisplayClass
00000003	31	31	5F	30	00	3C	3E	39	5F	5F	38	5F	30	00	3C	42	11_0.<>9_8_0.<B
00000004	77	72	53	61	76	65	5F	44	6F	57	6F	72	6B	3E	62	5F	wrSave_DoWork>b_
00000005	5F	38	5F	30	00	3C	3E	39	5F	5F	31	31	5F	31	00	3C	8_0.<>9_11_1.<
00000006	42	77	72	5F	44	6F	57	6F	72	6B	3E	62	5F	5F	31	31	Bvr_DoWork>b_11
00000007	5F	31	00	3C	3E	75	5F	5F	31	00	4E	75	6C	6C	61	62	1.<>u_1.Nullab
00000008	6C	65	60	31	00	49	45	6E	75	6D	65	72	61	62	6C	65	le'1.IEnumerable
00000009	60	31	00	50	72	65	64	69	63	61	74	65	60	31	00	4F	'1.Predicate'1.0
0000000A	62	73	65	72	76	61	62	6C	65	43	6F	6C	6C	65	63	74	bseervableCollect
0000000B	69	6F	6E	60	31	00	49	45	6E	75	6D	65	72	61	74	6F	ion'1.IEnumerato
0000000C	72	60	31	00	4C	69	73	74	60	31	00	6C	61	62	65	6C	r'1 List'1.label
0000000D	31	00	49	6E	74	33	32	00	3C	6C	61	75	6E	63	68	65	1.Int32.<launche
0000000E	72	3E	35	5F	5F	32	00	3C	42	77	72	5F	44	6F	57	6F	r>5_2.<Bvr_DoWo
0000000F	72	6B	3E	62	5F	5F	32	00	46	75	6E	63	60	32	00	49	rk>b_2.<Bvr_DoI
00000010	44	69	63	74	69	6F	6E	61	72	79	60	32	00	69	6D	61	Dictionary'2 ima
00000011	67	65	32	00	6C	61	62	65	6C	33	00	3C	42	61	75	6E	ge2.label3.<Laun
00000012	63	68	44	65	6C	61	79	3E	64	5F	5F	34	00	3C	4C	61	chDelay>d_4.<La
00000013	75	6E	63	68	65	72	41	73	79	6E	63	3E	64	5F	5F	35	uncherAsync>d_5
00000014	00	3C	3E	39	00	3C	4D	6F	64	75	6C	65	3E	00	4E	6F	<>9.<Module>.No
00000015	45	72	72	6F	72	55	49	00	53	79	73	74	65	6D	2E	49	ErrorUI.System.I
00000016	4F	00	73	65	74	5F	4F	70	65	6E	56	52	00	76	61	6C	0.set_OpenVR.val
00000017	75	65	5F	5F	00	53	79	73	74	65	6D	2E	57	69	6E	64	ue_<System.Wind
00000018	6F	77	73	2E	4D	65	64	69	61	00	53	79	73	74	65	6D	ows.Media.System
00000019	2E	57	69	6E	64	6F	77	73	2E	44	61	74	61	00	6D	73	Windows.Data.ms
0000001A	6C	65	60	31	00	49	45	6E	75	6D	65	72	61	74	6F	6F	lib.verb.<>c.
0000001B	6C	65	60	31	00	49	45	6E	75	6D	65	72	61	74	6F	6F	Lonc.System.
0000001C	43	6F	6C	6C	65	63	74	69	6F	6E	73	2E	47	65	6E	65	Collections.Gene
0000001D	72	69	63	00	4C	61	75	6E	63	68	65	72	41	73	79	6E	ric.LauncherAsyn
0000001E	63	00	52	75	6E	57	6F	72	6B	65	72	41	73	79	6E	63	c.RunWorkerAsyn
0000001F	00	53	68	6F	77	57	69	6E	64	6F	77	41	73	79	6E	63	.ShowWindowAsyn
00000020	00	61	70	70	55	73	65	72	4D	6F	64	65	6C	49	64	00	.appUserModelId.
00000021	63	6F	6E	6E	65	63	74	69	6F	6E	49	64	00	70	72	6F	connectionId.pro
00000022	63	65	73	73	49	64	00	47	65	74	50	72	6F	63	65	73	cessId.GetProces
00000023	73	42	79	49	64	00	54	68	72	65	61	64	00	62	77	72	sById.Thread.bvr
00000024	4C	6F	61	64	00	41	64	64	00	5F	63	6F	6E	74	65	6E	Load.Add_content
00000025	74	4C	6F	61	64	65	64	00	61	64	64	5F	54	65	78	74	tLoaded.add_text
00000026	43	68	61	6E	67	65	64	00	74	65	78	74	42	6F	78	5F	Changed.textBox_
00000027	54	65	78	74	43	68	61	6E	67	65	64	00	61	64	64	5F	TextChanged.add_
00000028	50	72	6F	70	65	72	74	79	43	68	61	6E	67	65	64	00	PropertyChanged.
00000029	72	65	6D	6F	76	65	5F	50	72	6F	70	65	72	74	79	43	remove_PropertyC
0000002A	68	61	6E	67	65	64	00	4F	6E	50	72	6F	70	65	72	74	hanged.OnPropert
0000002B	79	43	68	61	6E	67	65	64	00	49	4E	6F	74	69	66	79	yChanged.INotify
0000002C	50	72	6F	70	65	72	74	79	43	68	61	6E	67	65	64	00	PropertyChanged.
0000002D	67	65	74	5F	49	73	43	68	65	63	6B	65	64	00	73	65	get_IsChecked.se
0000002E	74	5F	49	73	43	68	65	63	6B	65	64	00	49	6E	74	65	t_IsChecked.Inte
0000002F	72	6C	6F	63	6B	65	64	00	73	65	74	5F	49	73	45	6E	rlocked.set_IsEn
00000030	61	62	6C	65	64	00	67	65	74	5F	53	65	6C	65	63	74	abled.get_Select
00000031	65	64	00	73	65	74	5F	53	65	6C	65	63	74	65	64	00	ed.set_Selected.
00000032	5F	69	73	53	65	6C	65	63	74	65	64	00	41	77	61	69	_isSelected.Avai
00000033	74	55	6E	73	61	66	65	4F	6E	43	6F	6D	70	6C	65	74	tUnsafeOnComple
00000034	65	64	00	61	64	64	5F	52	75	6E	57	6F	72	6B	65	72	.add_RunWorker
00000035	43	6F	6D	70	6C	65	74	65	64	00	42	77	72	53	61	76	Completed.BvrSav

Stringhe estratte relative alle funzioni di sistema

---

## Conclusioni

L'analisi statica ha confermato che il sample è un esemplare di **Agent Tesla** protetto da un installer **Nullsoft**. L'elevata entropia e l'uso di script NSIS dimostrano una strategia di difesa del malware volta a complicare l'analisi automatizzata. L'estrazione manuale ha permesso di identificare le componenti strutturali necessarie per la fase successiva di analisi dinamica.