

---

# 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)

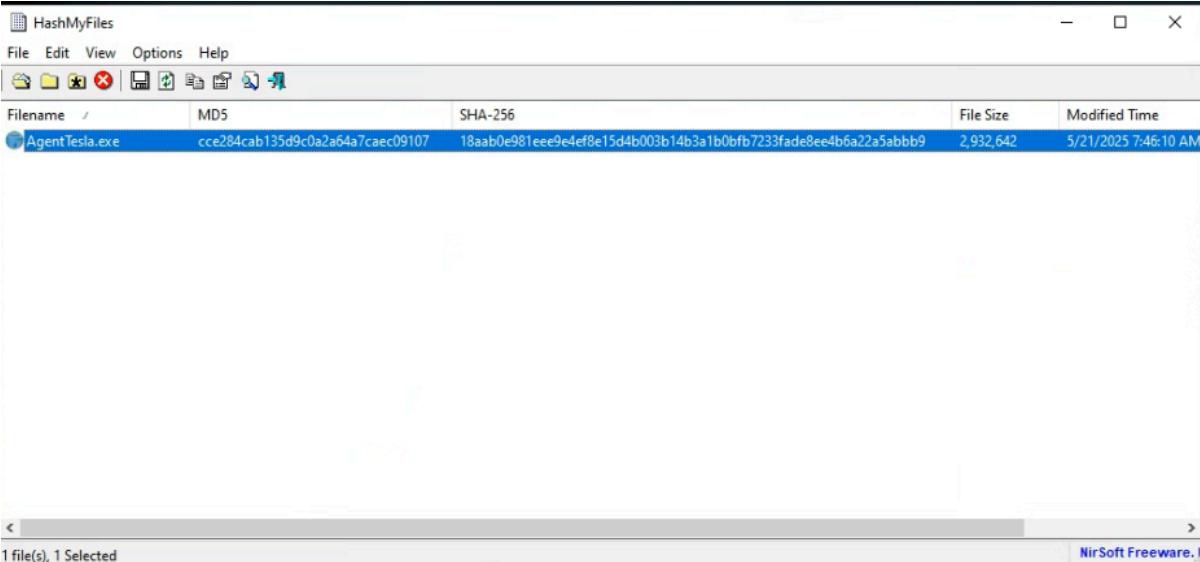
**Data:** 02/02/2026

---

### 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:**  
[18aab0e981eee9e4ef8e15d4b003b14b3a1b0fb7233fade8ee4b6a22a5abbb9](#).



Filename	MD5	SHA-256	File Size	Modified Time
AgentTesla.exe	<a href="#">cce284cab135d9c0a2a64a7caec09107</a>	<a href="#">18aab0e981eee9e4ef8e15d4b003b14b3a1b0fb7233fade8ee4b6a22a5abbb9</a>	2,932,642	5/21/2025 7:46:10 AM

1 file(s), 1 Selected

NirSoft Freeware, Inc.

---

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

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

The screenshot shows the PEStudio interface with the following details:

- File Path:** c:\users\flarevm\Desktop\malware\spyware\agenttesla.exe
- File Properties:**
  - file > sha256:** 18AAB0E981EEE9E4EF8E15D4B003B14B3A1B0BFB7233FADE8EE4B6A22A5ABB9
  - file > first 32 bytes (hex):** 4D 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00
  - file > first 32 bytes (text):** MZ.....@.....
  - file > info:** size: 2932642 bytes, entropy: 7.997
  - file > type:** executable, 32-bit, GUI
  - file > version:** n/a
  - file > description:** n/a
  - entry-point > first 32 bytes (hex):** 81 EC D4 02 00 00 53 56 57 6A 20 F5 33 DB 68 01 80 00 08 95 C2 14 C7 44 24 10 E0 A2 40 00 89
  - entry-point > location:** 0x000033C4 (section,.text)
  - file > signature:** Microsoft Linker 6.0
- Stamps:**
  - stamp > compiler:** Mon Dec 16 00:50:47 2019 (UTC)
  - stamp > debug:** n/a
  - stamp > resource:** n/a
  - stamp > import:** n/a
  - stamp > export:** n/a
- Names:**
  - file > name:** c:\users\flarevm\Desktop\malware\spyware\agenttesla.exe
  - debug > file:** n/a

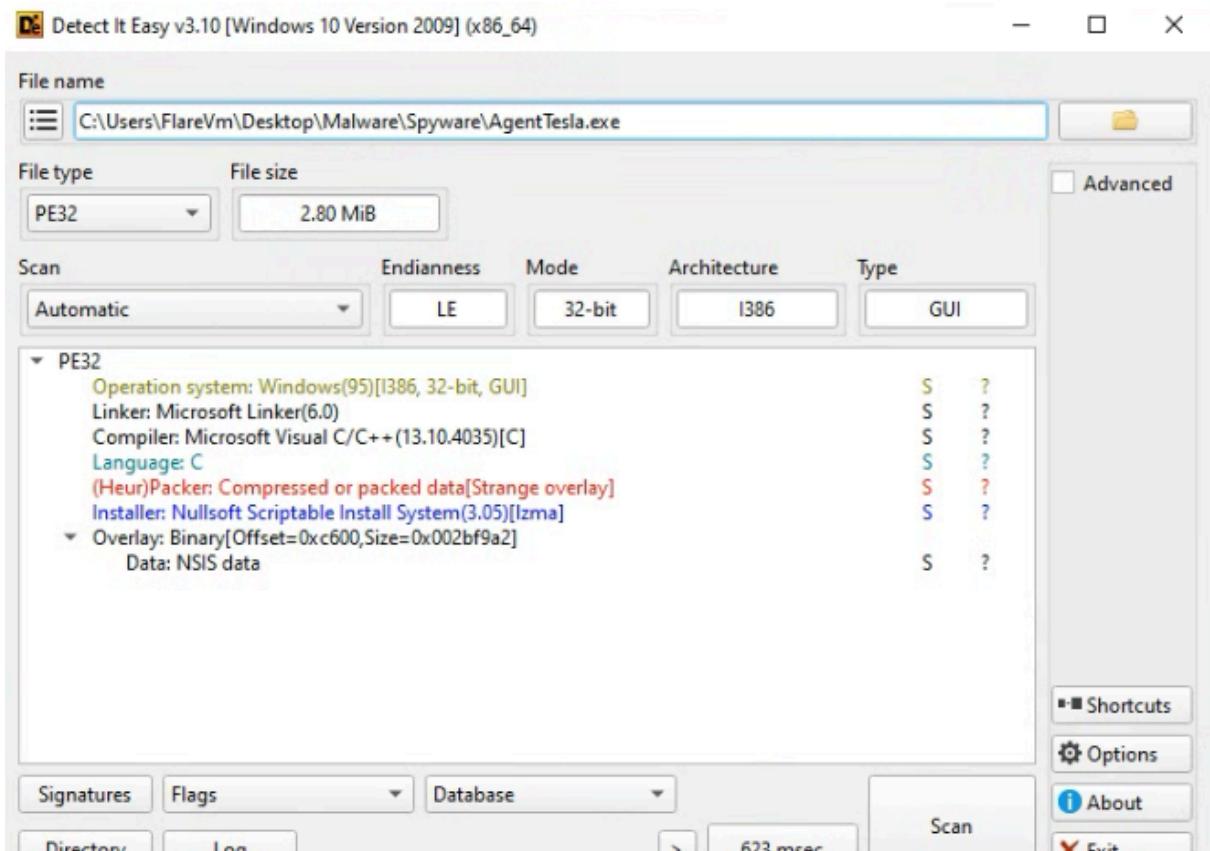
Schermata dei metadati generali in PEStudio

### 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 ?

File: UWPHook.exe

Dos Header

Nt Headers

File Header

Optional Header

Data Directories [x]

Section Headers [x]

Import Directory

Resource Directory

Relocation Directory

Debug Directory

.NET Directory

MetaData Header

Meta Data Streams

##

Tables Header

Tables

#Strings

#US

#GUID

#Blob

Address Converter

Dependency Walker

Hex Editor

Identifier

Import Adder

Quick Disassembler

Rebuilder

Resource Editor

Offset D 1 2 3 4 5 6 7 8 9 A B C D E F Ascii

00000000	00	3C	3B	3F	31	31	5F	30	00	3C	42	77	72	5F	<>9_11_0.<Bvr	
00000010	44	67	57	67	72	6B	3E	62	5F	31	31	5F	30	00	3C>DoWork>b_11_0.<	
00000020	3E	63	5F	5F	44	69	73	70	6C	61	79	43	6C	61	73_73>C_DisplayClass	
00000030	31	31	5F	30	00	3C	3E	39	5F	38	5F	30	00	3C	42_11_0.<>9_8_0.<B	
00000040	77	72	53	61	76	65	5F	44	6F	57	6F	72	6B	3E	62_5F>wvSave_DoWork>b_11_0.<>9_8_0.<B	
00000050	5F	38	5F	30	00	3C	3E	39	5F	3F	31	31	5F	31	00	3C>8_0.<>9_11_1.<Bvr_DoWork>b_11_0.<
00000060	42	77	72	58	44	68	57	6F	72	6B	3E	62	5F	9F	31	31>Bvr_DoWork>b_11_0.<
00000070	5E	31	00	3C	3E	75	5F	3F	31	00	4E	75	6C	61	62_1.<>u_1.Nullab	
00000080	6C	65	60	31	00	49	45	6E	75	6D	65	72	61	62	6C	65>Te_1.IEnumerable`1.Predicat<1_0
00000090	60	31	00	50	72	65	64	69	63	61	74	65	60	31	00	4F>bsevableCollect
000000A0	62	73	65	72	76	61	62	65	43	6F	6C	6C	65	63	74>ion_1.IEnumerable`1.List`1.label	
000000B0	69	6F	6E	60	31	00	49	45	6E	75	6D	65	72	61	74	6F>r_1.List`1.launcher
000000C0	72	60	31	00	4C	69	73	74	60	31	00	6C	61	62	65	6C>r_1.Int32_<launche
000000D0	31	00	49	6E	74	33	32	00	3C	6C	61	75	6E	63	68	65>r>5_2.<Bvr_DoWo
000000E0	72	3E	35	5F	72	3C	42	77	72	5F	44	6F	57	6F	57	6F>r>5_2.<Bvr_DoWo
000000F0	72	6B	3E	62	5F	5F	32	00	46	75	6E	60	32	00	49	rk>b_2.Func`2.I
00000100	44	69	63	74	69	6F	61	71	72	79	60	32	00	69	6D	61>Dictionary`2 ima
00000110	67	65	32	00	6C	61	62	65	6C	33	00	3C	6C	61	75	6E>ge2_label3_<Laun
00000120	63	68	44	65	66	61	79	3E	64	5F	34	00	3C	4C	61	chDelay>d_4.<La
00000130	75	6E	63	68	65	72	41	73	79	6E	63	74	64	5F	35	uncherAsync>d_5
00000140	00	3C	3E	39	00	3C	4D	64	75	6C	65	63	00	4E	6F	<>9.<Module>.No
00000150	45	72	72	6F	72	65	49	50	29	23	24	65	6F	2E	49	ErrorUI.System`1
00000160	4F	00	73	65	74	5F	4F	70	65	6E	56	52	00	76	6E	6C>O.set_OpenVR.v1
00000170	75	65	5F	00	53	73	74	65	6D	72	6E	57	69	6E	64	ue_.System.Window
00000180	6F	77	73	2E	4D	65	64	69	61	00	53	79	73	74	65	6D>ows.Media.System
00000190	26	52	69	6E	64	68	77	73	2E	44	61	74	61	00	6D	73>Windows.Data.ms
000001A0	26	52	69	6E	64	68	77	73	2E	44	61	74	61	00	6D	73>ib.verb.<>c.
000001B0	43	6F	6C	65	63	74	69	6F	73	2E	47	65	6E	65	73>onic.System`1	
000001C0	72	69	63	74	69	6F	61	75	6E	63	68	57	42	73	79	6E>Collections.Gene
000001D0	00	53	75	6E	57	6F	72	6B	65	72	41	73	79	6E	63	ric.LauncherAsync
000001E0	63	00	52	75	6E	57	6F	72	6B	65	72	41	73	79	6E	c.RunWorkerAsync
000001F0	00	53	68	67	77	57	69	6E	64	6F	77	41	73	79	6E	.ShowWindowAsync
00000200	00	61	70	70	55	73	65	72	6D	64	65	46	49	64	00	.appUserModelId
00000210	63	6F	6E	65	63	74	69	6F	64	69	64	60	70	72	6F	connectionId
00000220	63	65	73	73	49	64	00	47	65	74	50	72	6F	63	65	73>cessId
00000230	73	42	79	49	64	00	54	68	72	65	61	64	00	62	77	72>Load.Add`content
00000240	4C	6F	61	64	00	41	64	64	00	5F	63	6E	74	65	65	tLoaded.add_Text
00000250	74	4C	6F	61	64	65	64	00	61	64	64	54	65	78	74	Changed.textBox
00000260	43	68	61	6E	67	65	64	00	74	65	78	42	6F	78	75	TextChanged.add_
00000270	54	65	78	74	43	68	61	6E	67	65	64	00	61	64	5F	PropertyChanged
00000280	50	72	67	70	65	72	74	79	43	68	61	6E	67	65	64	00
00000290	72	65	6D	76	65	5F	50	72	6F	70	65	72	74	79	43	remove_PropertyC
000002A0	68	61	6E	67	65	64	00	4F	66	72	6F	70	65	72	74	hanged.OnProperty
000002B0	79	43	68	61	6E	67	65	64	00	49	44	4E	74	69	66	yChanged.Notify
000002C0	50	72	67	70	65	72	74	79	43	68	61	6E	67	65	64	PropertyChanged
000002D0	67	65	74	5F	49	73	43	68	65	63	6B	65	64	00	73	65>get.IsChecked
000002E0	74	5F	49	73	43	68	65	63	6B	65	64	00	49	4E	74	65>t_IsChecked.int
000002F0	72	6C	6F	63	6B	65	64	00	73	65	74	5F	49	73	45	6E>rlocked.set.IsEnabled
00000300	61	62	6C	65	64	00	67	65	74	5F	53	65	6C	65	63	74>abled.get_Select
00000320	58	69	73	53	65	6C	65	63	74	65	64	00	41	77	61	69>ed.set_Selected
00000330	74	55	68	73	61	66	65	4F	6E	43	5F	70	6C	65	74	65>isItemSelected
00000340	65	64	00	61	64	64	5B	75	6E	57	6F	72	6B	65	72	65>ed.add_RunWorker
00000350	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.