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)

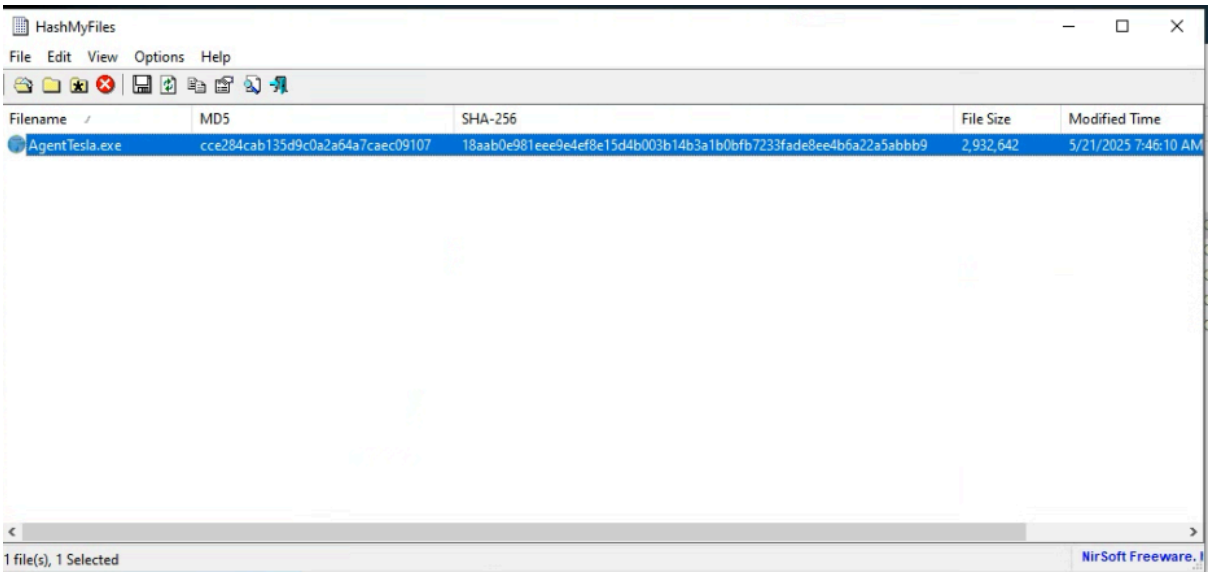
Data: 02/02/2026

---

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.



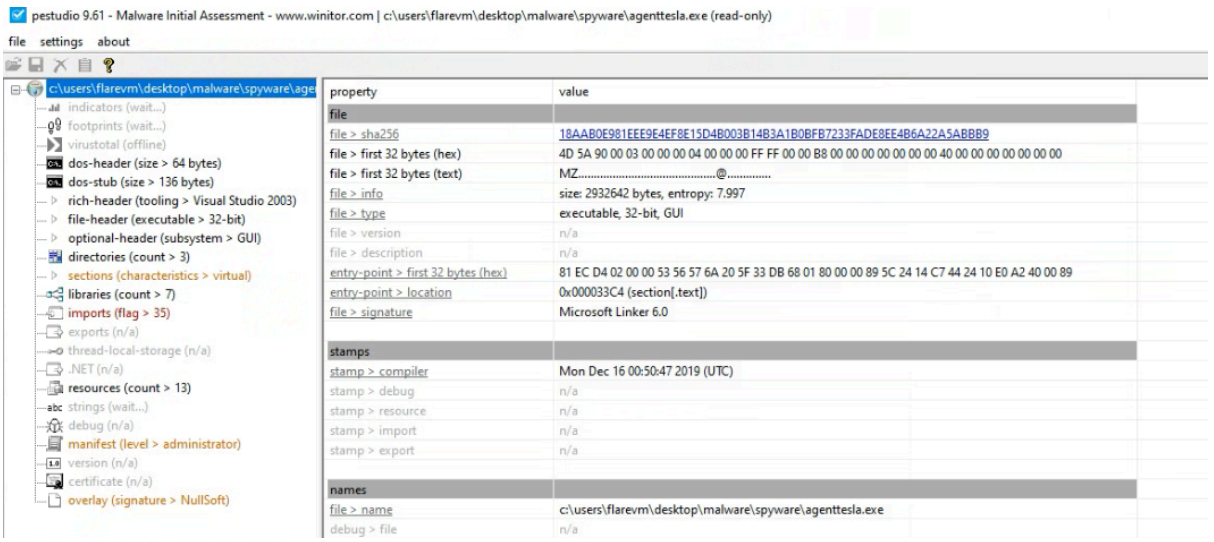
---

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 .text.
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

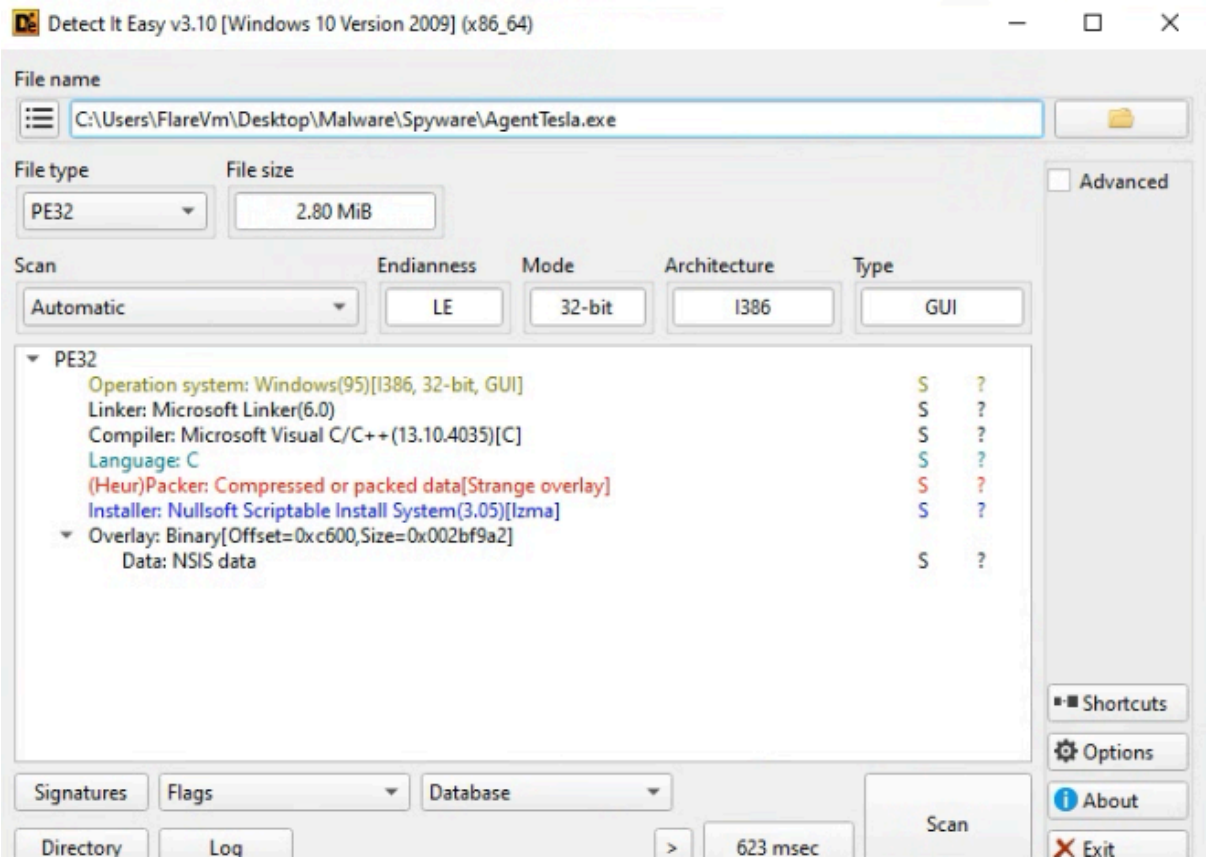
---

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.



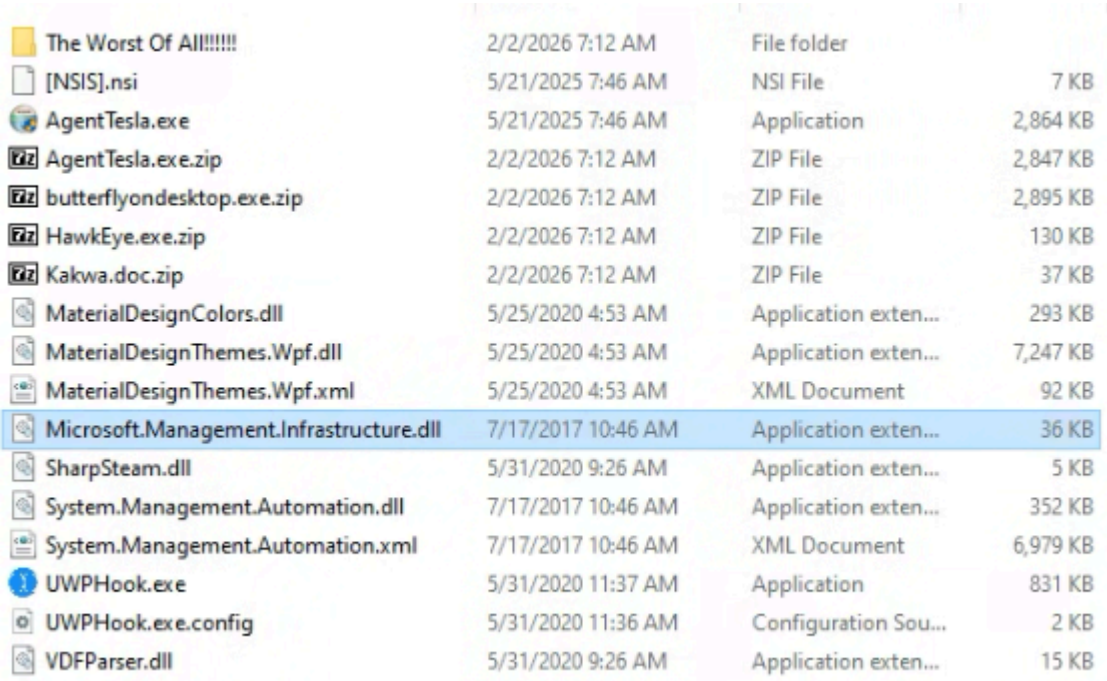
Schermata di Detect It Easy con evidenza del packer Nullsoft

---

4. Analisi delle Stringhe e De-packaging Manuale

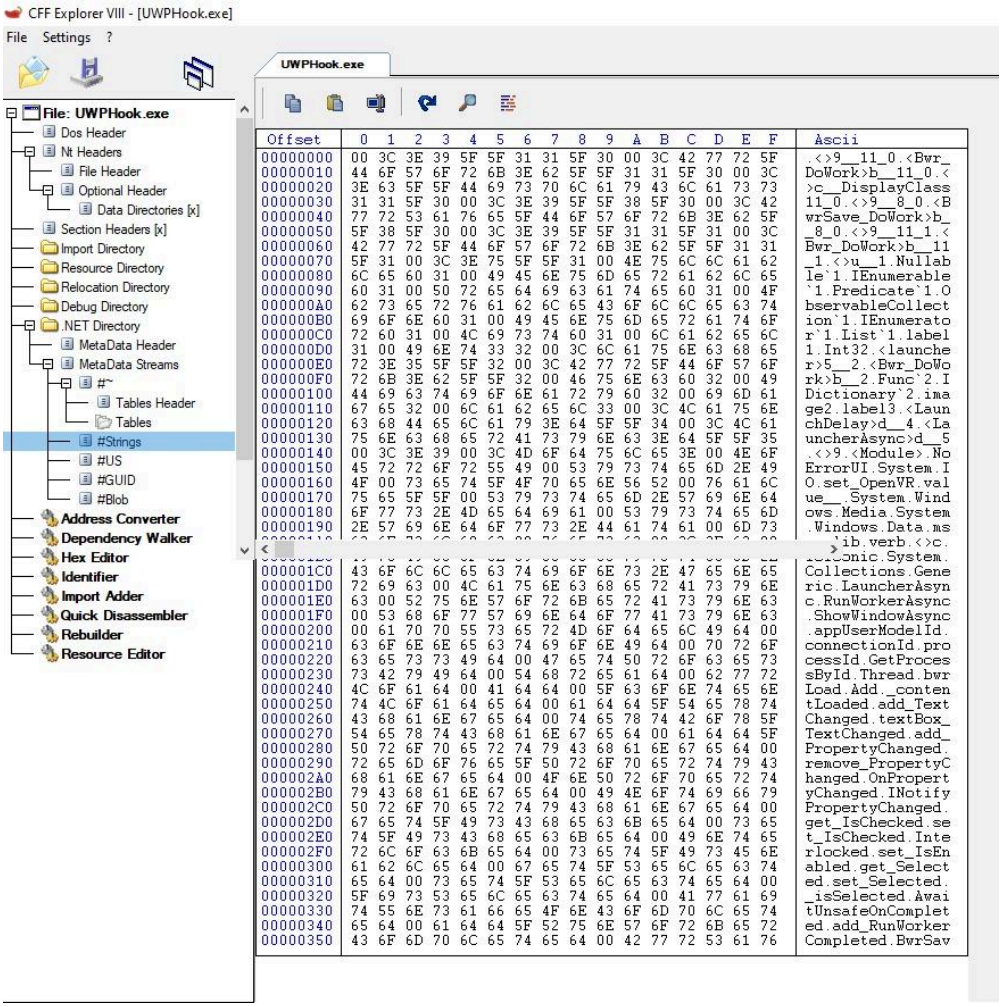
Data l'impossibilità di estrarre stringhe significative direttamente dall'eseguibile compresso (stato "wait" in PEStudio), è stata eseguita l'estrazione manuale dei componenti tramite **7-Zip**.

- **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



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.