Analisi Statica: Agent Tesla

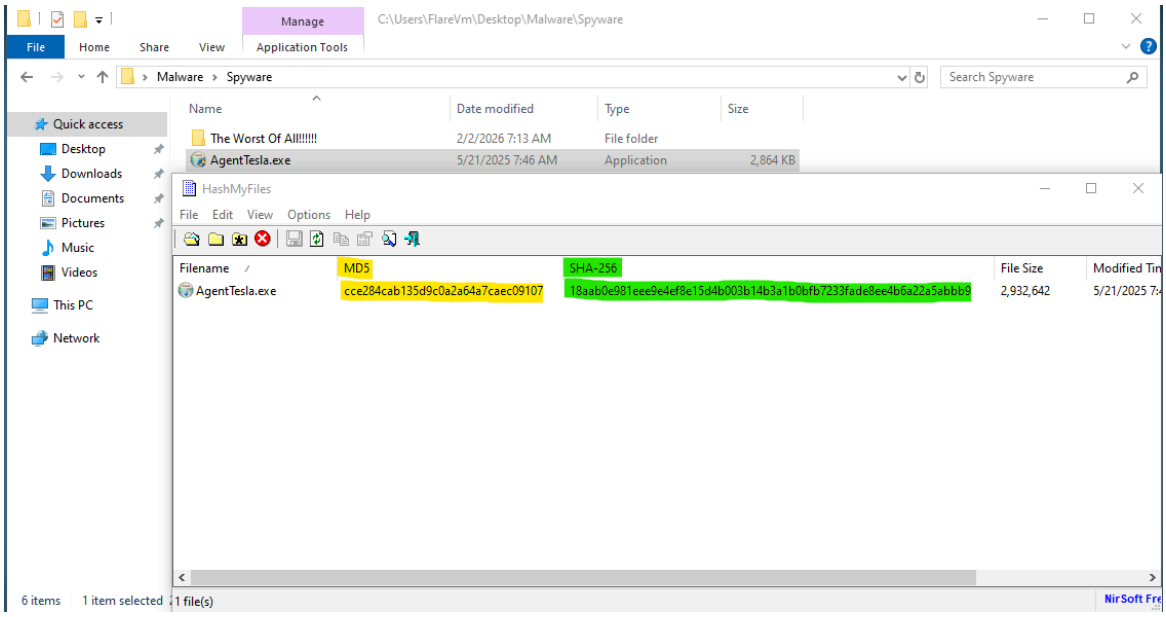
Oggetto: Analisi Statica di base del sample "AgentTesla.exe"

Fingerprinting

In questa fase è stato identificato univocamente il file calcolando le sue impronte digitali (hash) tramite il tool HashMyFiles.

Algoritmo	Hash
Nome File	AgentTesla.exe
Dimensione	2,932,642 bytes
MD5	cce284cab135d9c0a2a64a7caec09107
SHA256	18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

Evidenza:

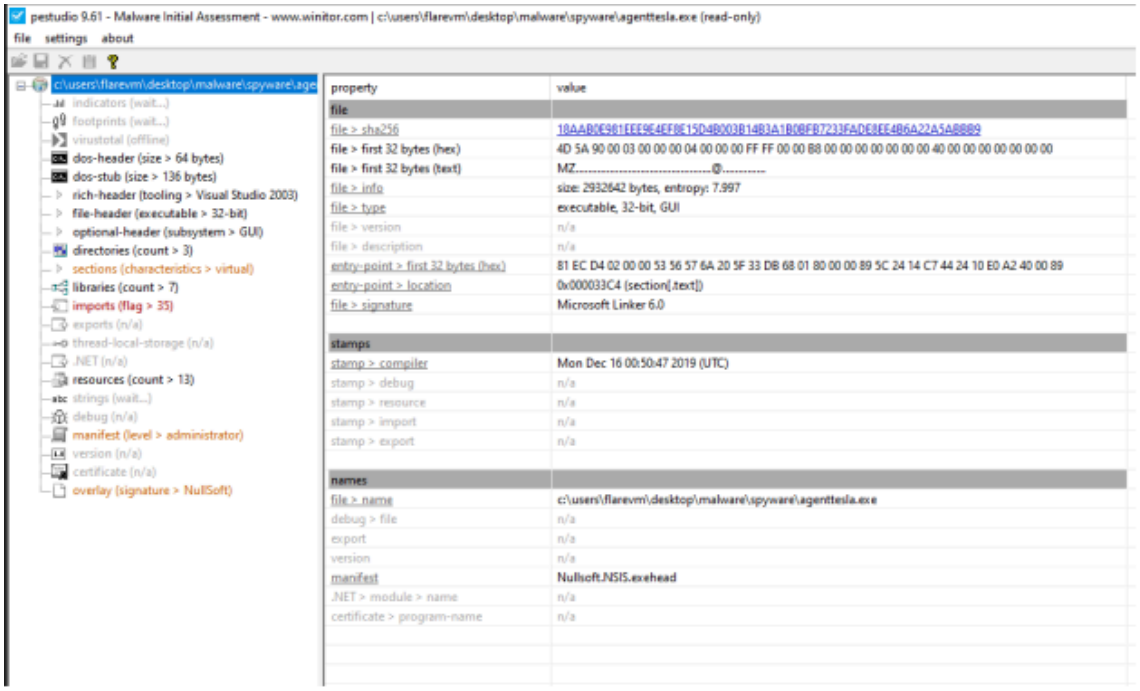


Analisi Struttura PE (Portable Executable)

L'analisi della struttura interna del file, effettuata tramite PEStudio, ha evidenziato che si tratta di un eseguibile con caratteristiche sospette legate all'alta entropia.

Campo	Valore Rilevato	Note / Analisi
Architettura	32-bit (x86)	Eseguibile standard a 32 bit.
Timestamp	Mon Dec 16 00:50:47 2019 (UTC)	La data sembra realistica (non è settata a 0 o nel futuro), indicando un sample creato (o il packer compilato) alla fine del 2019.
Entry Point	0x000033C4	Situato nella sezione .text.
Subsystem	GUI	Il programma possiede un'interfaccia grafica o gira come applicazione windowed (non console).
Entropia	7.997	CRITICO: Un valore così vicino al massimo (8.0) indica che il file è quasi certamente pacchettizzato (packed), cifrato o compresso.
Signature	Microsoft Linker 6.0	Firma del linker generica.

Evidenza:



Rilevamento Packer

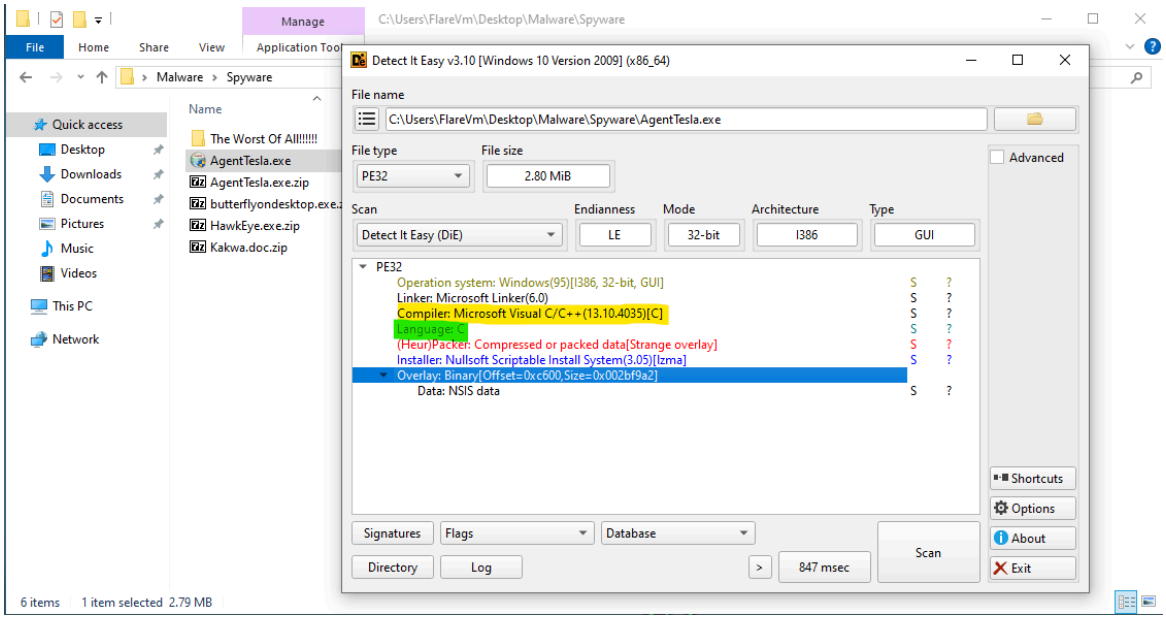
Utilizzando Detect It Easy (DiE), è stato confermato che il malware è nascosto all'interno di un installer.

- **Packer/Installer Rilevato:** Nullsoft Scriptable Install System (NSIS) [version 3.05]
- **Compressione:** lzma
- **Linguaggio Rilevato:** C (riferito al wrapper NSIS, non necessariamente al payload finale)
- **Analisi .NET:** In questa fase statica, il tool non rileva .NET nel layer esterno. Questo perché stiamo analizzando il contenitore (l'installer NSIS) e non il vero malware (Agent Tesla) che è nascosto e compresso al suo interno.

Conclusione sul Packer:

Il file AgentTesla.exe non è il malware "nudo", ma un archivio auto-estraente NSIS. Quando verrà eseguito, questo installer decomprimerà il vero codice malevolo in memoria.

Evidenza:



Analisi Stringhe

L'estrazione delle stringhe conferma la natura di "Installer" del file, nascondendo le stringhe relative alle vere funzionalità del malware (come connessioni di rete o furto dati) che sono offuscate dalla compressione.

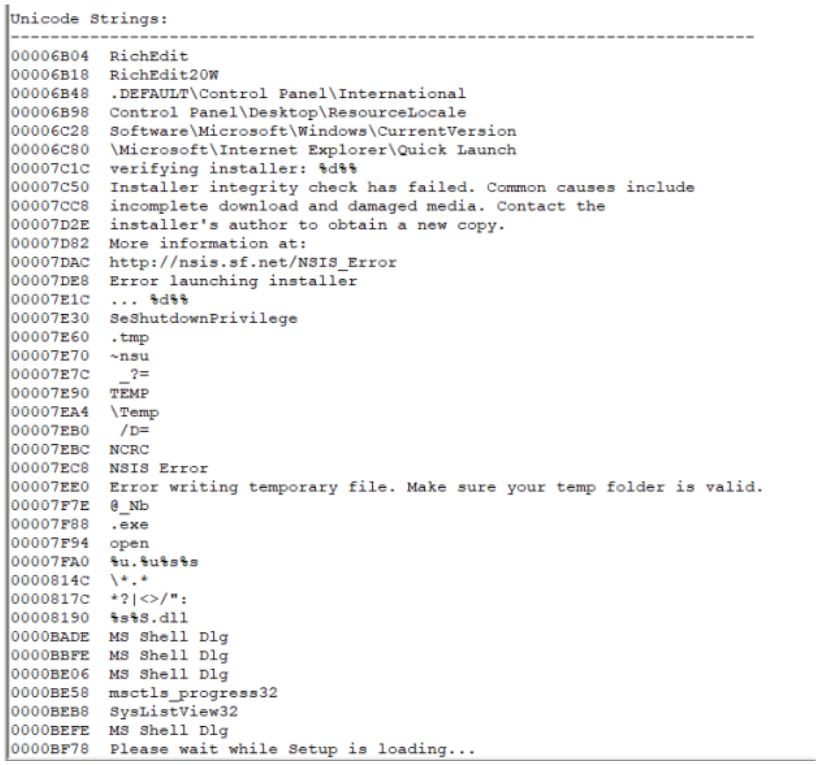
Le stringhe più significative trovate includono:

Categoria	Trovato	Valore / Significato
URL	http://nsis.sf.net/NSIS_Error	URL standard presente negli installer NSIS.
Messaggi Errore	Installer integrity check has failed	Conferma che si tratta di un pacchetto di installazione.
Percorsi	\ Temp	Indica che l'installer probabilmente estrarrà file nella cartella temporanea di Windows.
Librerie	RichEdit, RichEdit20W	Librerie per la gestione del testo nell'interfaccia grafica dell'installer.
Permessi	SeShutdownPrivilege	Privilegio richiesto per spegnere o riavviare il sistema.

Osservazione:

A causa dell'alta entropia (compressione), non sono visibili in chiaro IP di comando e controllo (C2) o indirizzi email in questa fase. Sarà necessaria un'analisi dinamica o il

deobfuscation per vederli. **Evidenza:**



Conclusioni

L'analisi statica indica che il file AgentTesla.exe è un **Dropper/Loader** mascherato da installer NSIS. L'altissima entropia (7.997) conferma che il payload malevolo è cifrato o compresso all'interno. Le tecniche di analisi statica di base si fermano al "guscio" esterno; per analizzare il comportamento reale (Spyware), sarà necessario procedere con l'analisi dinamica o l'unpacking manuale.