

# Analisi Statica: Agent Tesla

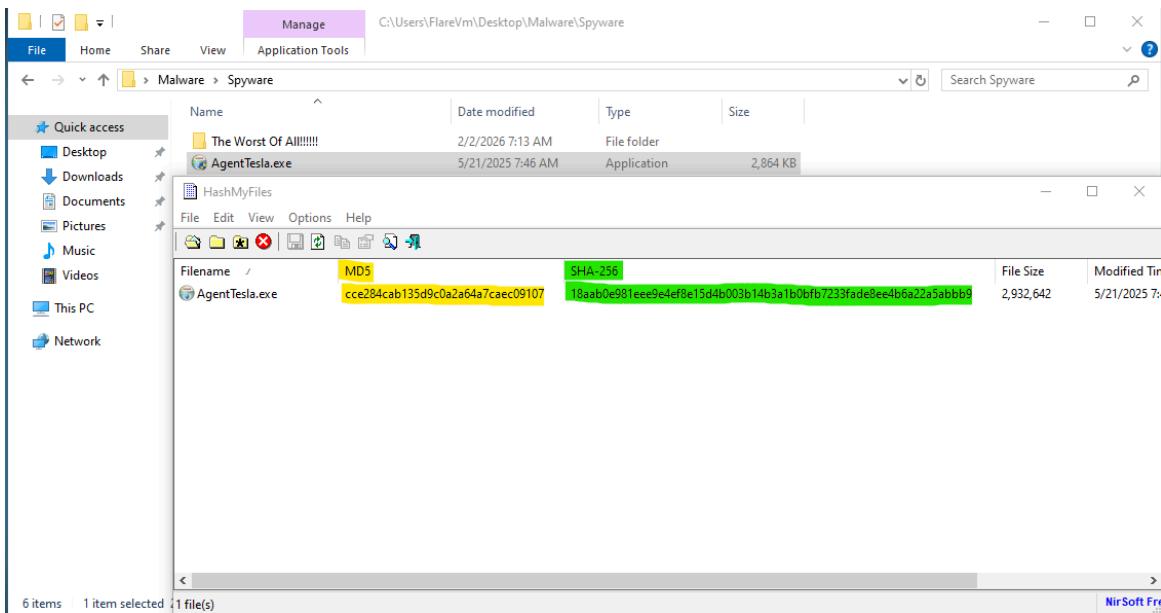
Oggetto: Analisi Statica di base del sample "AgentTesla.exe"

## 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	cce284cab135d9coa2a64a7caec09107
SHA256	18aab0e981eee9e4ef8e15d4b003b14b3a1b0fb7233fade8ee4b6a22a5abbb9

## 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)	Esegibile 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	0x0000033C4	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:

pestudio 9.61 - Malware Initial Assessment - www.wimitor.com | c:\users\flarevm\Desktop\malware\spyware\agenttesta.exe (read-only)

file settings about

File Properties

property	value
file > sha256	10AA80E981EEE9E4FF8E15D4B003B14B3A1B0FB723FADE3EE4B6A22A5A8889
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 40 00 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	
entry-point > first 32 bytes (hex)	B1 EC D4 02 00 00 53 56 57 6A 20 5F 33 DB 68 01 80 00 00 89 5C 24 14 C7 44 24 10 E0 A2 40 00 89
entry-point > location	0x000003C4 (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\agenttesta.exe
debug > file	n/a
export	n/a
version	n/a
manifest	Nullsoft.NSIS.exehead
.NET > module > name	n/a
certificate > program-name	n/a

# Rilevamento Packer

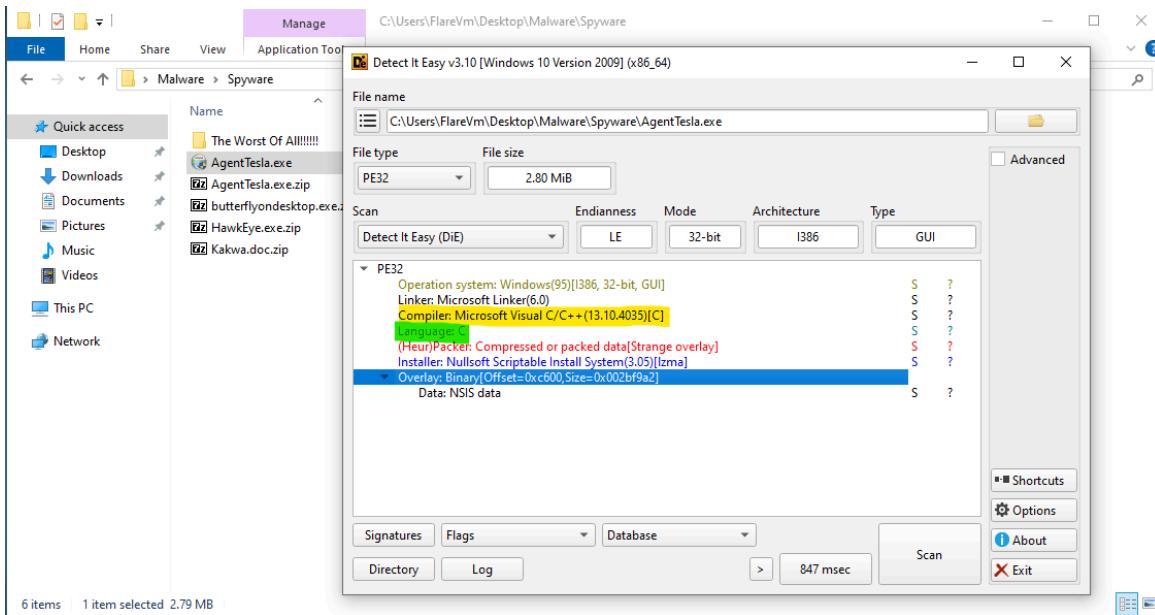
Utilizzando Detect It Easy (DiE), è stato confermato che il malware è nascosto all'interno di un installer.

- **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:**

```
Unicode Strings:
-----
00006B04  RichEdit
00006B18  RichEdit20W
00006B48  .DEFAULT\Control Panel\International
00006B98  Control Panel\Desktop\ResourceLocale
00006C28  Software\Microsoft\Windows\CurrentVersion
00006C80  \Microsoft\Internet Explorer\Quick Launch
00007C1C  verifying installer: %d%%
00007C50  Installer integrity check has failed. Common causes include
incomplete download and damaged media. Contact the
00007D2E  installer's author to obtain a new copy.
00007D82  More information at:
00007DAC  http://nsis.sf.net/NSIS_Error
00007DE8  Error launching installer
00007E1C  ... %d%%
00007E30  SeShutdownPrivilege
00007E60  .tmp
00007E70  ~nsu
00007E7C  _?=
00007E90  TEMP
00007EA4  \Temp
00007EB0  /D=
00007EBC  NCRC
00007EC8  NSIS Error
00007EE0  Error writing temporary file. Make sure your temp folder is valid.
00007F7E  @_Nb
00007F88  .exe
00007F94  open
00007FA0  %u.%u%sts
0000814C  \*.*
0000817C  *?|<>/:";
00008190  %s%.dll
0000BADE  MS Shell Dlg
0000BBFE  MS Shell Dlg
0000BE06  MS Shell Dlg
0000BE58  msctls_progress32
0000BEB8  SysListView32
0000BEFE  MS Shell Dlg
0000BF78  Please wait while Setup is loading...
```

# 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.