

S9 – L1

Analisi Statica Malware Agent Tesla (FlareVM)

Introduzione

In questo esercizio ho eseguito un'attività di **analisi statica di un malware di tipo Agent Tesla** utilizzando l'ambiente di laboratorio **FlareVM**.

L'obiettivo è stato **identificare le principali caratteristiche del campione senza eseguirlo, applicando tecniche di fingerprinting, analisi della struttura PE, rilevamento del linguaggio/packer e analisi delle stringhe.**

0) Estraggo Agent Tesla

1. Copio l'archivio di **Agent Tesla** sul **Desktop** di FlareVM.
2. Tasto destro sull'archivio → **7-Zip** → **Extract to...**
3. Quando chiede la password scrivo: **infected** (**non è stata richiesta la password**)
4. Controllo che nella cartella estratta ci sia il file del sample (es. .exe) **senza eseguirlo.**



Output: **archivio sul Desktop** + **cartella estratta** + richiesta password (non richiesta)

1) Calcolo gli hash (Fingerprint)

5. Tasto destro sul file estratto → **HashMyFiles** (oppure lo apro e trascino il file).
6. Copio nel report:
 - **MD5**
 - **SHA256**

| HashMyFiles | | | | |
|-----------------------------|----------------------------------|--|-----------|----------------------|
| File Edit View Options Help | | | | |
| Filename | MD5 | SHA-256 | File Size | Modified Time |
| AgentTesla.exe | cce284cab135d9c0a2a64a7caec09107 | 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9 | 2,932,642 | 5/21/2025 4:46:10 PM |

Output: HashMyFiles con **MD5 e SHA256** visibili.

2) Controllo su VirusTotal (da hash)

- Copio lo **SHA256** e lo cerco su **VirusTotal** (search by hash).
- Tramite la ricerca dello SHA256 su VirusTotal, il campione è risultato segnalato come malevolo da **27 su 70** motori antivirus.
Il file è classificato come **hacktool / trojan** ed è associato alla famiglia **AgentTesla**, con ulteriori etichette quali *docmo* e *negasteal*.

The screenshot displays the VirusTotal analysis interface. At the top, the search bar contains the SHA-256 hash. The main dashboard shows a community score of 27/70 and a status of '27/70 security vendors flagged this file as malicious'. The file is identified as 'AgentTesla.exe' with a size of 2.80 MB. Below this, various threat categories are listed: 'hacktool', 'trojan', 'agenttesla', 'docmo', and 'negasteal'. The 'Security vendors' analysis section is partially visible at the bottom.

Output: **pagina VirusTotal con detection**

3) Analisi PE (struttura del file)

- Apro il file con **PEStudio** (o **CFF Explorer**).
- Nel report segno:
 - Architettura** (x86 / 32 Bit) --- (**File Type: Portable Executable 32**)

CFF Explorer VIII - [AgentTesla.exe]

File Settings ?

AgentTesla.exe

| Property | Value |
|-----------|--|
| File Name | C:\Users\FlareVm\Desktop\AgentTesla.exe |
| File Type | Portable Executable 32 |
| File Info | No match found. |
| File Size | 2.80 MB (2932642 bytes) |
| PE Size | 49.50 KB (50688 bytes) |
| Created | Tuesday 03 February 2026, 20.17.44 |
| Modified | Wednesday 21 May 2025, 15.46.10 |
| Accessed | Tuesday 03 February 2026, 20.34.30 |
| MD5 | CCE284CAB135D9C0A2A64A7CAEC09107 |
| SHA-1 | E4B8F4B6CAB18B9748F83E9FFFD275EF5276199E |

| Property | Value |
|----------|------------------------------|
| Empty | No additional info available |

- **Timestamp --- TimeDateStamp (Value): 5DF6D4E7**

CFF Explorer VIII - [AgentTesla.exe]

File Settings ?

AgentTesla.exe

| Member | Offset | Size | Value | Meaning |
|----------------------|----------|-------|----------|------------|
| Machine | 000000CC | Word | 014C | Intel 386 |
| NumberOfSections | 000000CE | Word | 0005 | |
| TimeDateStamp | 000000D0 | Dword | 5DF6D4E7 | |
| PointerToSymbolTa... | 000000D4 | Dword | 00000000 | |
| NumberOfSymbols | 000000D8 | Dword | 00000000 | |
| SizeOfOptionalHea... | 000000DC | Word | 00E0 | |
| Characteristics | 000000DE | Word | 010F | Click here |

- **Entry Point** (AddressOfEntryPoint = 000033C4)

CFF Explorer VIII - [AgentTesla.exe]

File Settings ?

AgentTesla.exe

File: AgentTesla.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

| Member | Offset | Size | Value | Meaning |
|-----------------------------|----------|-------|----------|---------|
| SizeOfCode | 000000E4 | Dword | 00006400 | |
| SizeOfInitializedData | 000000E8 | Dword | 00022A00 | |
| SizeOfUninitializedData | 000000EC | Dword | 00000800 | |
| AddressOfEntryPoint | 000000F0 | Dword | 000033C4 | .text |
| BaseOfCode | 000000F4 | Dword | 00001000 | |
| BaseOfData | 000000F8 | Dword | 00008000 | |
| ImageBase | 000000FC | Dword | 00400000 | |
| SectionAlignment | 00000100 | Dword | 00001000 | |
| FileAlignment | 00000104 | Dword | 00000200 | |
| MajorOperatingSystemVers... | 00000108 | Word | 0004 | |
| MinorOperatingSystemVers... | 0000010A | Word | 0000 | |
| MajorImageVersion | 0000010C | Word | 0006 | |
| MinorImageVersion | 0000010E | Word | 0000 | |
| MajorSubsystemVersion | 00000110 | Word | 0004 | |
| MinorSubsystemVersion | 00000112 | Word | 0000 | |

- **Subsystem** (GUI/Console)

Il **Subsystem** del file è **Windows GUI**, come indicato dal campo *Subsystem* dell'Optional Header.

CFF Explorer VIII - [AgentTesla.exe]

File Settings ?

AgentTesla.exe

File: AgentTesla.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

| Member | Offset | Size | Value | Meaning |
|-----------------------------|----------|-------|----------|-------------|
| ImageBase | 000000FC | Dword | 00400000 | |
| SectionAlignment | 00000100 | Dword | 00001000 | |
| FileAlignment | 00000104 | Dword | 00000200 | |
| MajorOperatingSystemVers... | 00000108 | Word | 0004 | |
| MinorOperatingSystemVers... | 0000010A | Word | 0000 | |
| MajorImageVersion | 0000010C | Word | 0006 | |
| MinorImageVersion | 0000010E | Word | 0000 | |
| MajorSubsystemVersion | 00000110 | Word | 0004 | |
| MinorSubsystemVersion | 00000112 | Word | 0000 | |
| Win32VersionValue | 00000114 | Dword | 00000000 | |
| SizeOfImage | 00000118 | Dword | 0004C000 | |
| SizeOfHeaders | 0000011C | Dword | 00000400 | |
| Checksum | 00000120 | Dword | 00000000 | |
| Subsystem | 00000124 | Word | 0002 | Windows GUI |
| DllCharacteristics | 00000126 | Word | 8540 | Click here |

Output: schermata CFF Explorer con i campi visibili.

4) Rilevo packer/linguaggio (.NET o altro)

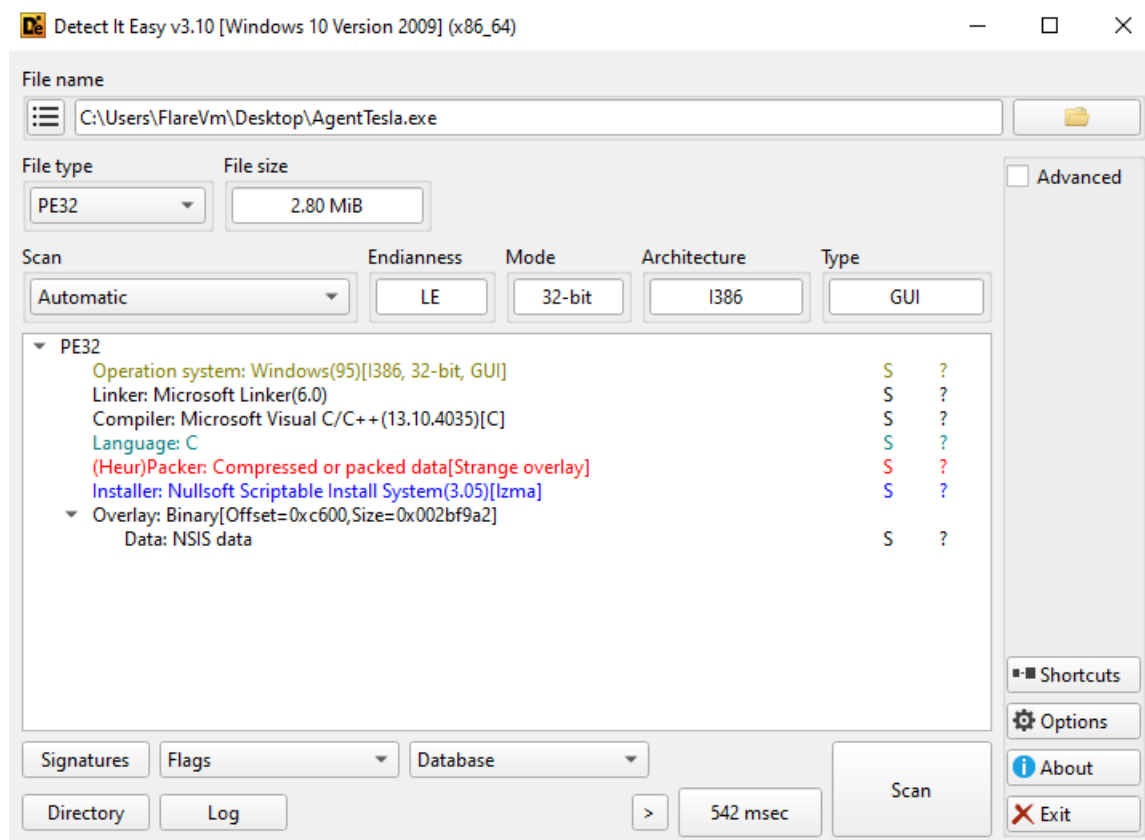
11. Apro il file con **Detect It Easy (DiE)**

12. **Dati tecnici rilevati (dal tool)**

- **Tipo file:** PE32
- **Architettura:** 32-bit (i386)
- **Sistema operativo:** Windows (95–11), GUI
- **Compiler:** Microsoft Visual C/C++
- **Linguaggio:** C/C++
- **Installer / Packer:** NSIS (Nullsoft Scriptable Install System)
- **Overlay presente** (dato compresso/packed)

13. L'analisi del campione tramite Detect It Easy ha evidenziato che il file è un PE32 a 32 bit per sistemi Windows.

14. Il malware risulta compilato in C/C++ mediante Microsoft Visual C/C++ ed è confezionato tramite NSIS (Nullsoft Scriptable Install System), con presenza di overlay, indicativo di dati compressi o impacchettati all'interno dell'eseguibile.



🚩 Output: DiE con risultato visibile.

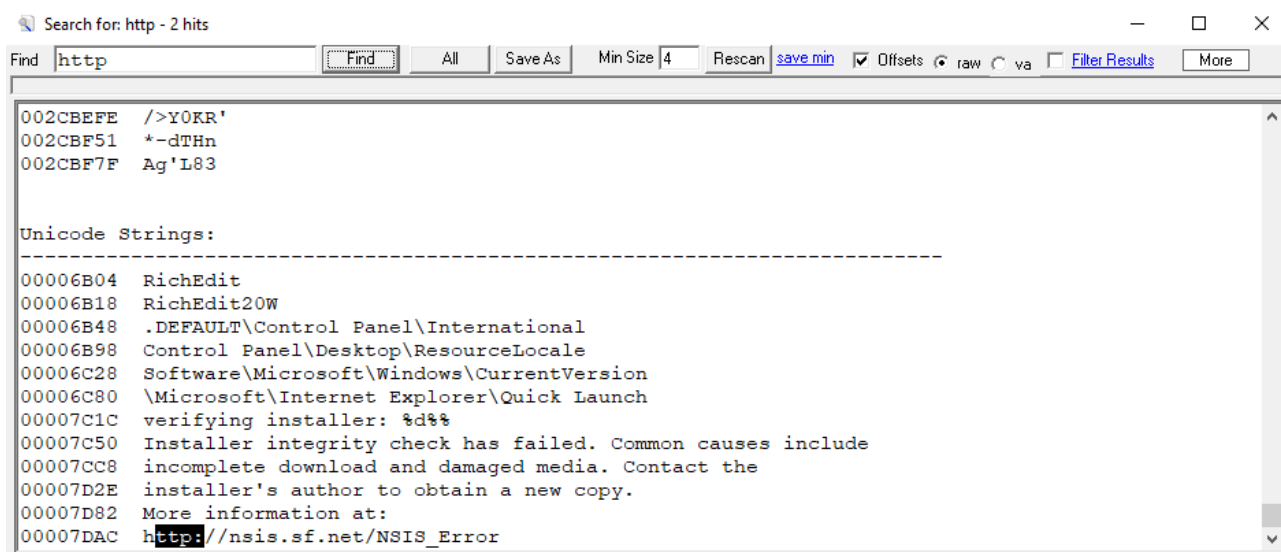
5) Estraggo stringhe e IoC

13. Estraggo le stringhe (tool “Strings”)

14. Dall’analisi delle stringhe statiche del file sono stati individuati Indicatori di Compromissione (IoC).

In particolare è stato rilevato un riferimento a un URL

(http://nsis.sf.net/NSIS_Error), coerente con l’utilizzo del framework NSIS per il confezionamento dell’eseguitabile.



The screenshot shows the output of the Strings tool. At the top, it says "Search for: http - 2 hits". Below that, there are three lines of hex addresses and their corresponding strings: 002CBEFE />Y0KR', 002CBF51 *-dTHn, and 002CBF7F Ag'L83. Then, there is a section titled "Unicode Strings:" followed by a list of system paths and a URL. The URL is http://nsis.sf.net/NSIS_Error.

```
002CBEFE />Y0KR'
002CBF51 *-dTHn
002CBF7F Ag'L83

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
00007CC8 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
```

Output: presenza di un URL, confermando l’utilizzo di NSIS.

Conclusioni

L’analisi statica ha permesso di **raccogliere informazioni rilevanti sul malware Agent Tesla** senza comprometterne l’esecuzione, **individuando hash, struttura dell’eseguitabile, linguaggio di sviluppo e principali indicatori di compromissione.**

Questa fase rappresenta un passaggio fondamentale per comprendere il comportamento di un malware e **costituisce la base per eventuali analisi dinamiche o attività di difesa e threat intelligence.**