REPORT TECNICO

FlareVM

AgentTesla.exe

Redatto da: *Nicolò Calì Cybersecurity Student*

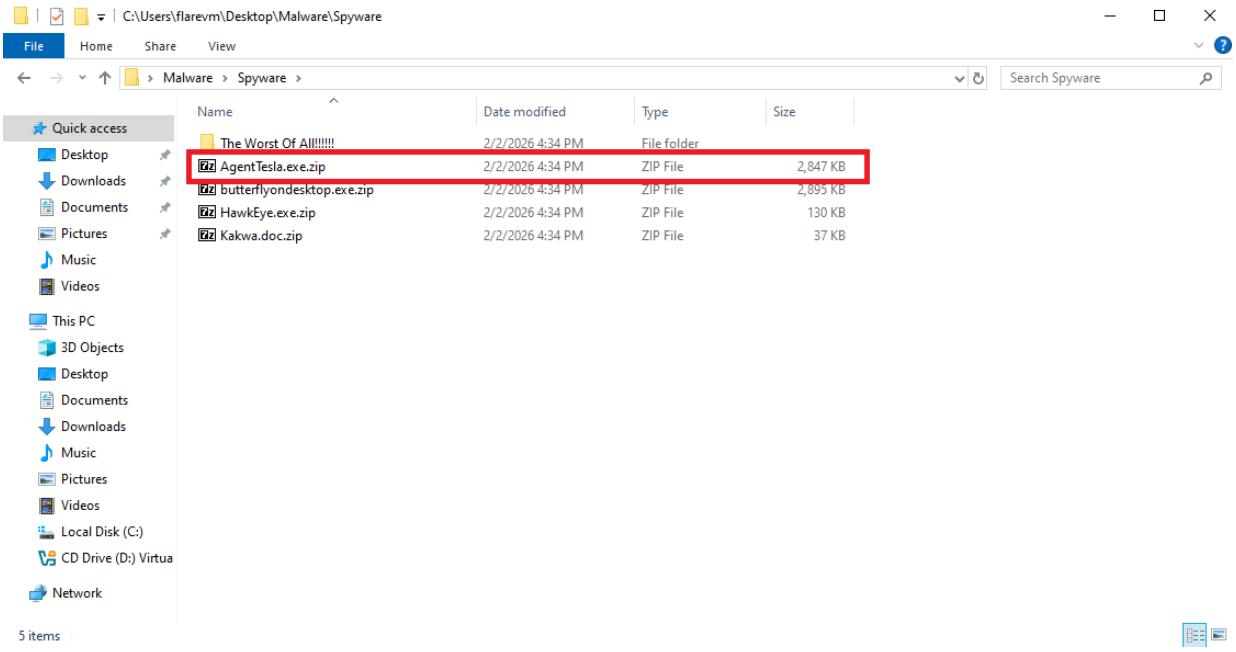
Data: 02/02/2026

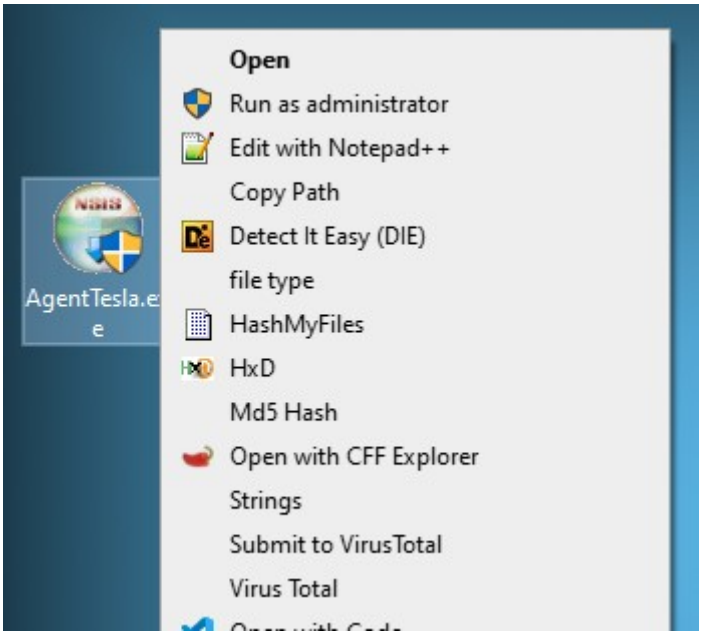
1. Introduzione

L'obiettivo di questo laboratorio è stato condurre un'analisi statica di base su un artefatto malevolo denominato "Agent Tesla". L'attività è stata svolta all'interno di un ambiente isolato e sicuro (**FlareVM**) per prevenire qualsiasi infezione del sistema host.

Lo scopo principale è identificare le caratteristiche fondamentali del file senza mai eseguire il malware.

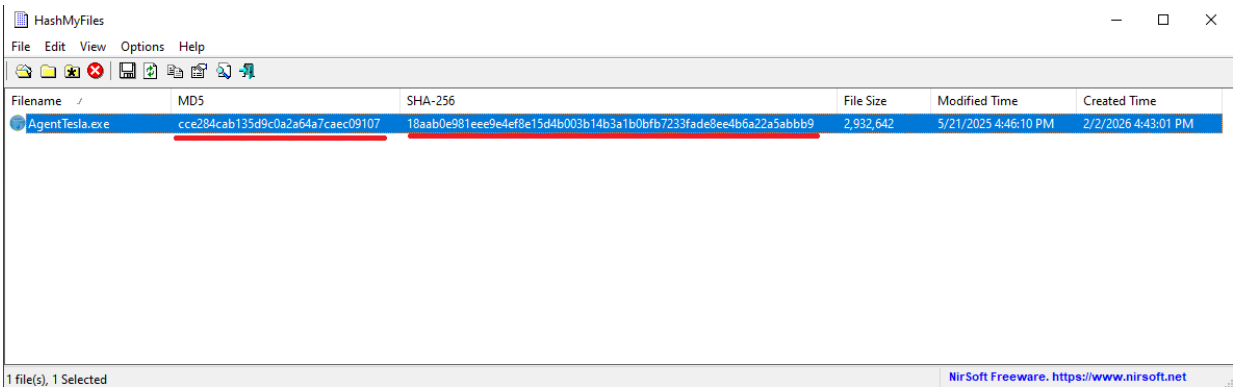
Non appena viene effettuato il download dell'archivio dei malware individuo quello di nostro interesse :"AgentTesla.exe".





2. Fingerprinting

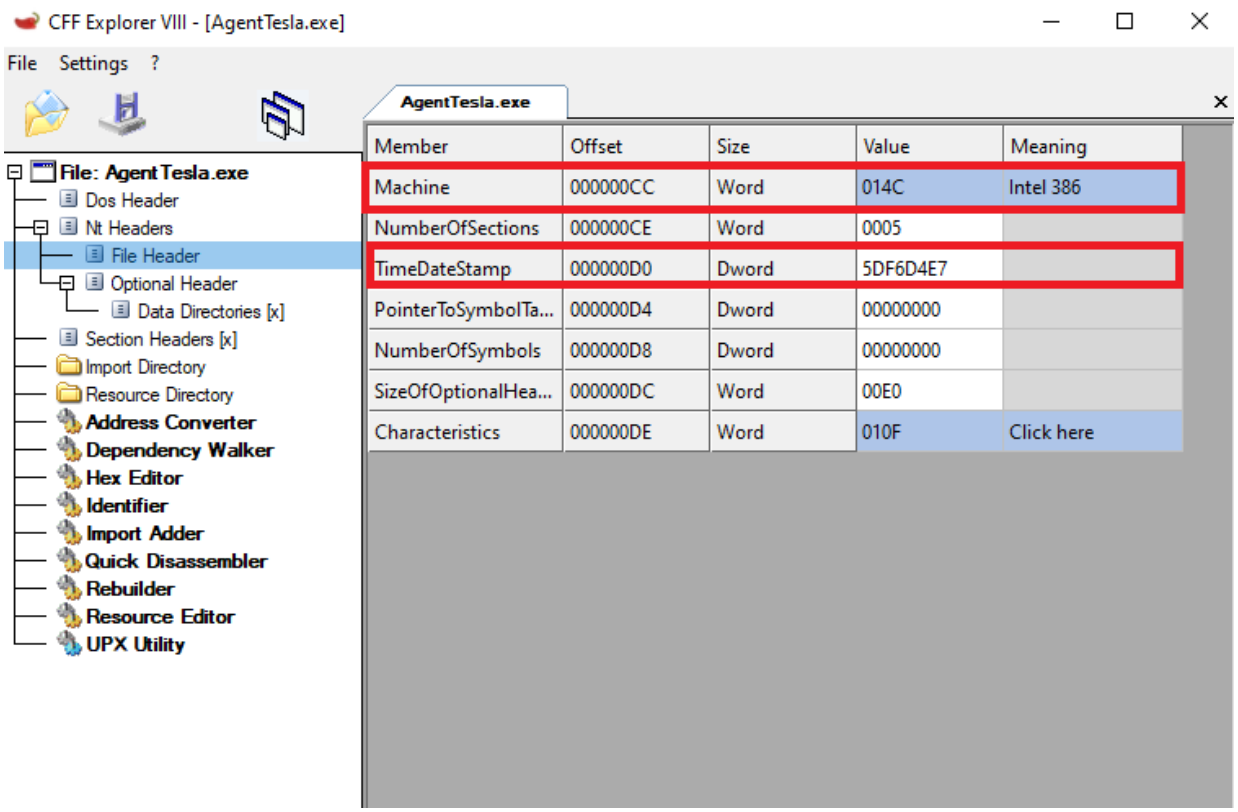
Per identificare univocamente il campione e permetterne la condivisione con la comunità di sicurezza, sono stati calcolati gli hash crittografici utilizzando lo strumento **HashMyFiles**.

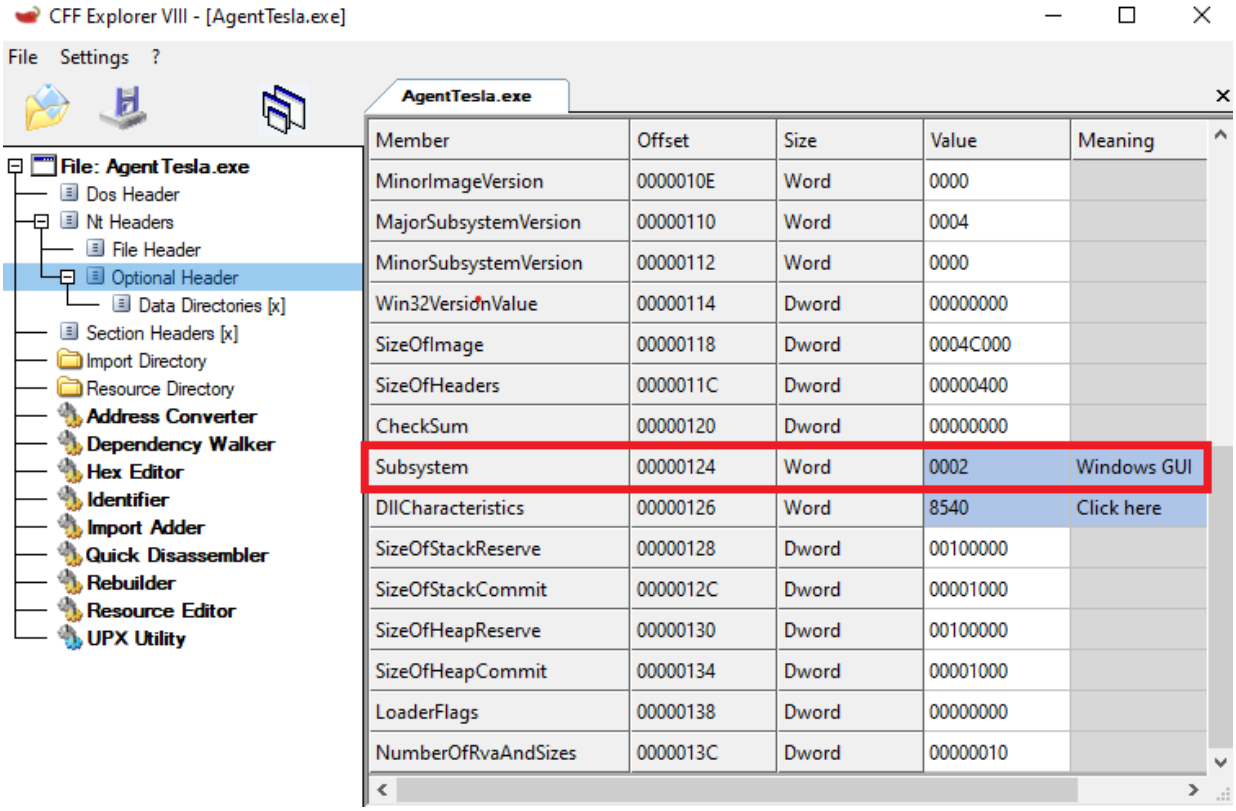


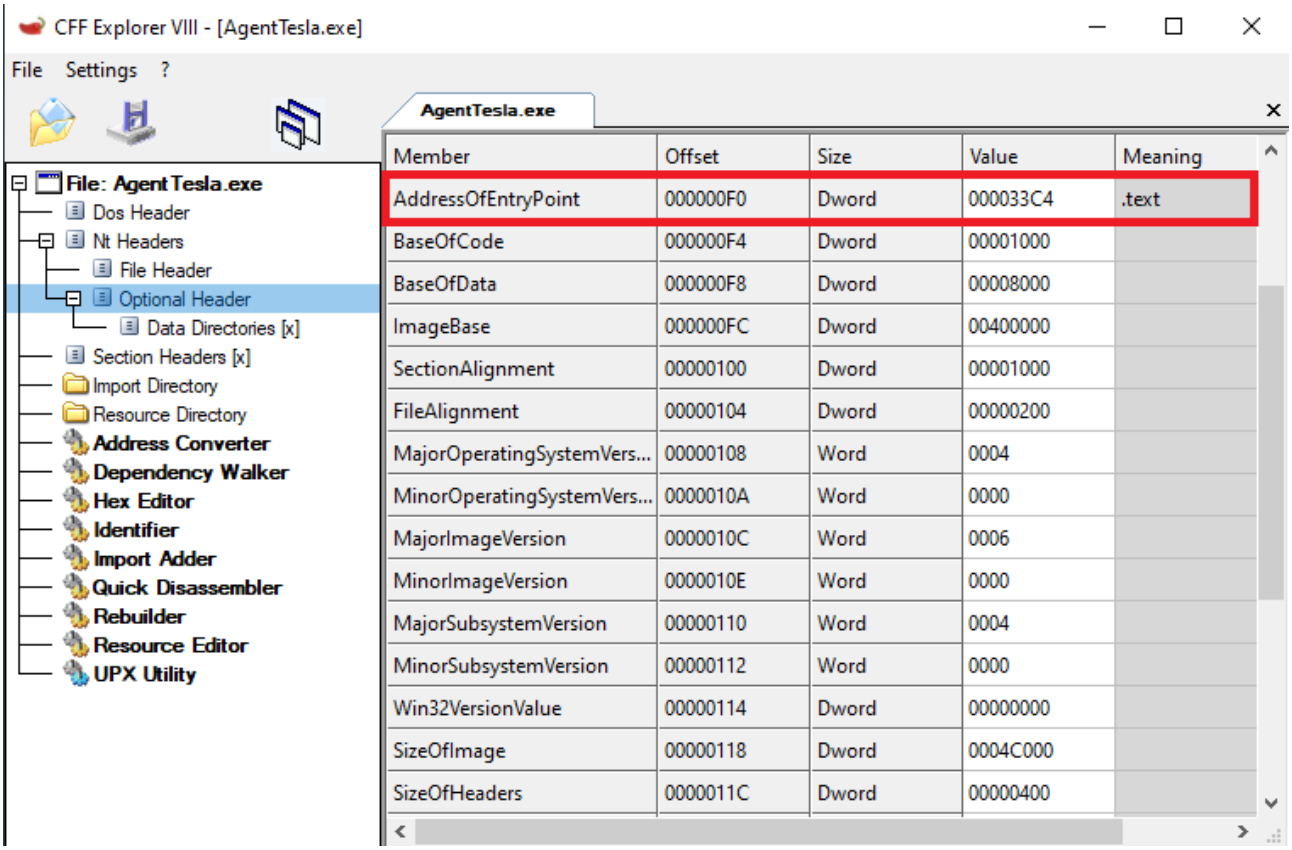
- **MD5** → `cce284cab135d9c0a2a64a7caec09107`
- **SHA256** → `10a5b0e8eece9e4ef0e15d4b0058b14b3a1b0bfe723fadeffea6bba22a5abbb9`

3. Analisi Strutturata PE

Utilizzando lo strumento **CFF Explorer**, è stata analizzata l'intestazione del file (PE Header) per estrarre informazioni sulla sua compilazione e architettura.




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
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
SizeOfStackReserve | 00000128 | Dword | 00100000
SizeOfStackCommit | 0000012C | Dword | 00001000
SizeOfHeapReserve | 00000130 | Dword | 00100000
SizeOfHeapCommit | 00000134 | Dword | 00001000
LoaderFlags | 00000138 | Dword | 00000000
NumberOfRvaAndSizes | 0000013C | Dword | 00000010


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
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
Win32VersionValue | 00000114 | Dword | 00000000
SizeOfImage | 00000118 | Dword | 0004C000
SizeOfHeaders | 0000011C | Dword | 00000400

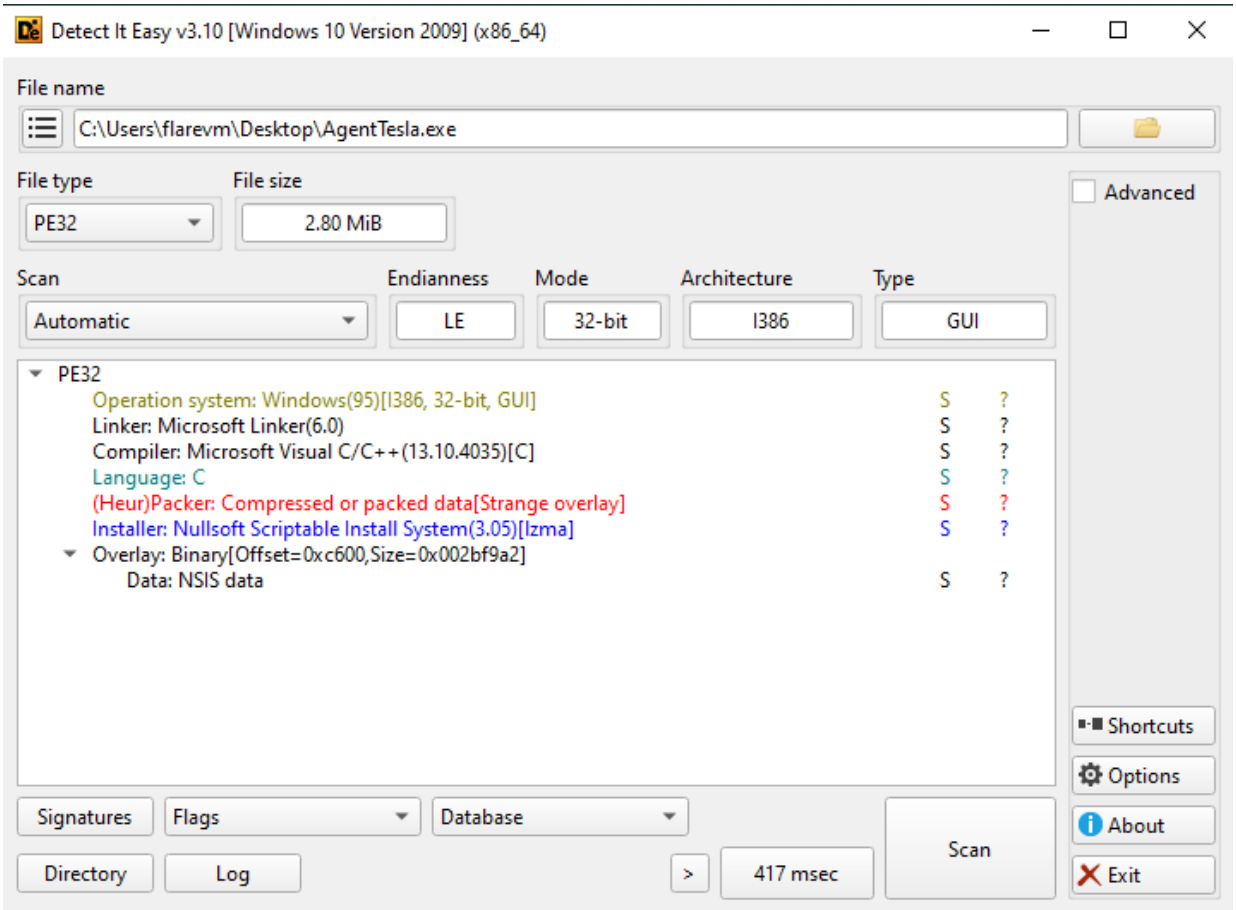
Informazioni ottenute tramite **CFF Explorer**:

Campo	Valore	Note
Architettura	Intel 386	Eseguibile a 32 bit (x86)
Timestamp	5DF6D4E7	Data di compilazione (convertita): 15 Dicembre 2019
Entry Point	000033C4	Indirizzo di memoria iniziale del codice
Subsystem	Windows GUI	Interfaccia grafica (non console)

4. Rilevamento Packer

L'analisi con **Detect It Easy (DiE)** è stata cruciale per capire la natura del file. I risultati indicano che il file non è un semplice eseguibile compilato, ma un pacchetto di installazione che nasconde il vero contenuto.

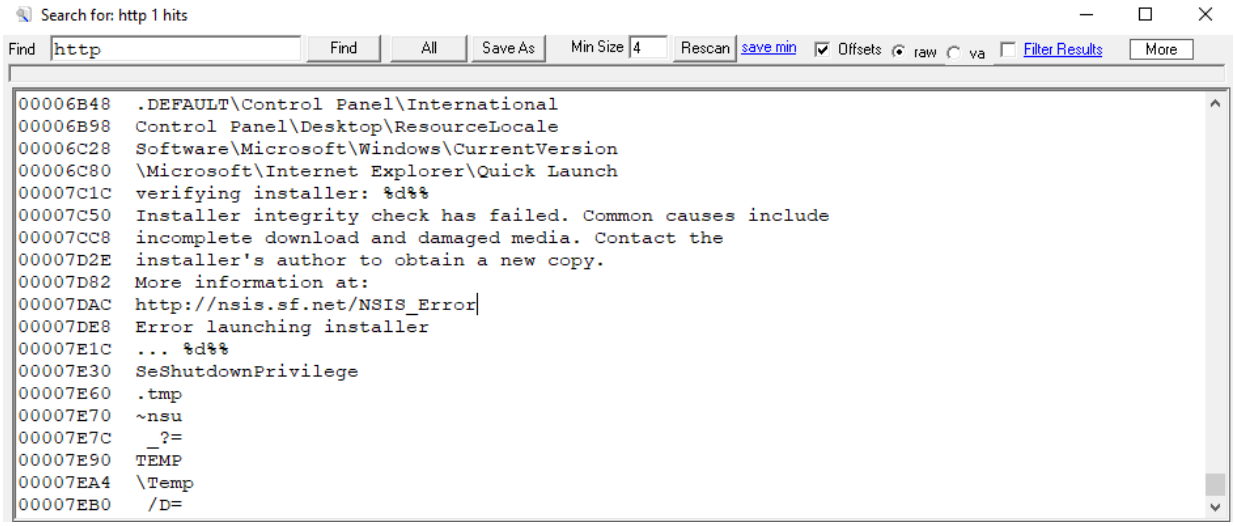
- **Linguaggio:** C
- **Compiler/Packer:** Nullsoft Scriptable Install System (NSIS) v3.05
- **Versione .NET:** N/A (Il file non risulta essere un assemblato .NET visibile a questo livello).



La presenza di **NSIS** indica che il malware è "impacchettato". Il codice malevolo reale è compresso all'interno di questo **installer**.

5. Analisi Stringhe

È stata effettuata una ricerca di stringhe leggibili all'interno del binario. A causa del *packing* rilevato nella fase precedente, le stringhe tipiche di Agent Tesla (come indirizzi SMTP o FTP) non sono visibili in chiaro. Sono state invece trovate stringhe tipiche dell'installer NSIS.



Categoria	Trovato	Note
URL/Domini	http://nsis.sf.net/NSIS_Error	URL legittimo associato all'installer NSIS, non al C2 del malware.
Email/IP	Non rilevati	Nascosti dalla cifratura/compressione del Packer.
File/Percorsi	`.tmp`, `~nsu`	Riferimenti a file temporanei creati durante l'estrazione dell'installer.

6. Conclusione

L'analisi statica ha confermato che il file **`AgentTesla.exe`** è un eseguibile a 32 bit. Tuttavia, l'analisi ha rivelato che il file è **Packed** utilizzando **NSIS** (Nullsoft Scriptable Install System).

Questo "guscio" esterno protegge e nasconde il vero codice malevolo, rendendo inefficace la lettura delle stringhe o degli import in questa fase.

Non è stato possibile estrarre gli Indicatori di Compromissione (IoC) di rete (come server C2 o email) tramite la sola analisi statica di base.