REPORT S9/L1: Analisi Statica Malware (Agent Tesla)

Studente: Vincenzo Zarola

Oggetto: Analisi Statica di base su sample "AgentTesla.exe" in ambiente FlareVM.

---

1. Obiettivo dell'Esercitazione

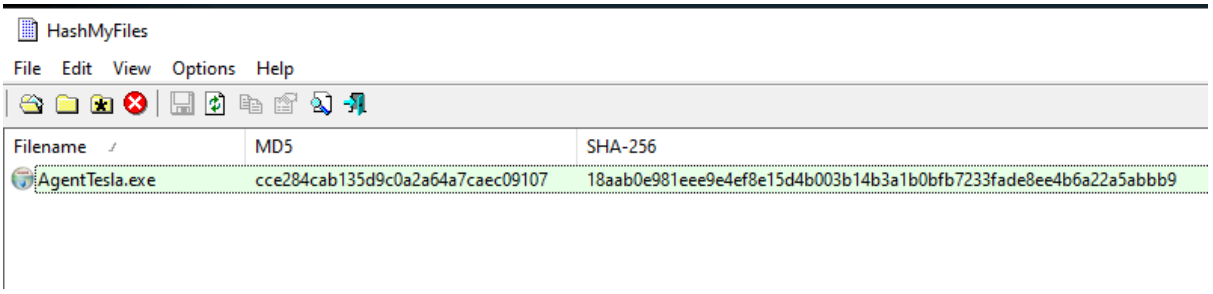
L'attività ha lo scopo di eseguire una prima analisi statica su un campione di malware noto come **Agent Tesla**, utilizzando una macchina virtuale isolata (FlareVM). L'obiettivo è raccogliere indicatori di compromissione (IoC) preliminari, identificare la struttura del file e determinare se il codice è offuscato o impacchettato.

---

2. Fingerprinting (Identificazione del File)

La prima fase ha previsto l'identificazione univoca del campione tramite calcolo degli hash crittografici.

- **Nome File:** AgentTesla.exe
- **MD5:** `cce284cab135d9c0a2a64a7caec09107`
- **SHA256:** 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

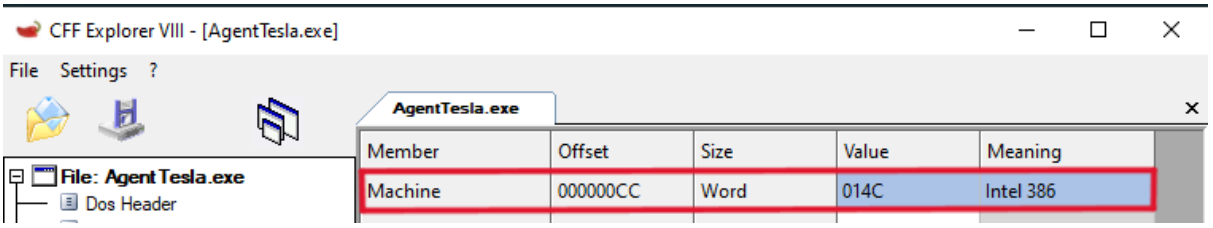


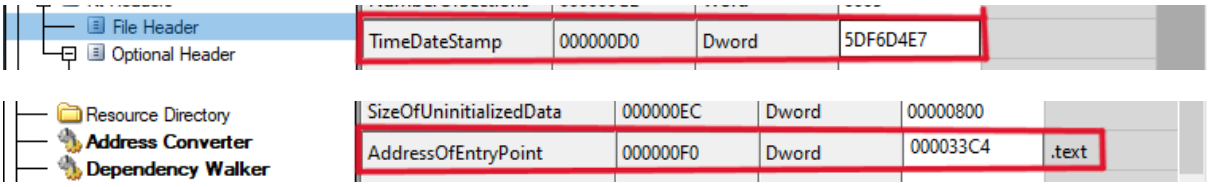
---

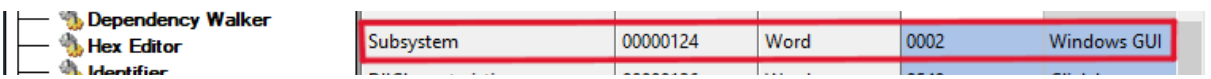
3. Analisi Struttura PE (Portable Executable)

Utilizzando lo strumento **CFF Explorer**, è stata esaminata la struttura interna del file per estrarre i metadati di compilazione.

Campo	Valore	Note
Architettura	014C	Intel 386.
Timestamp	5DF6D4E7	16 Dicembre 2019
Entry point	000033C4	.text
Subsystem	0002	Windows GUI



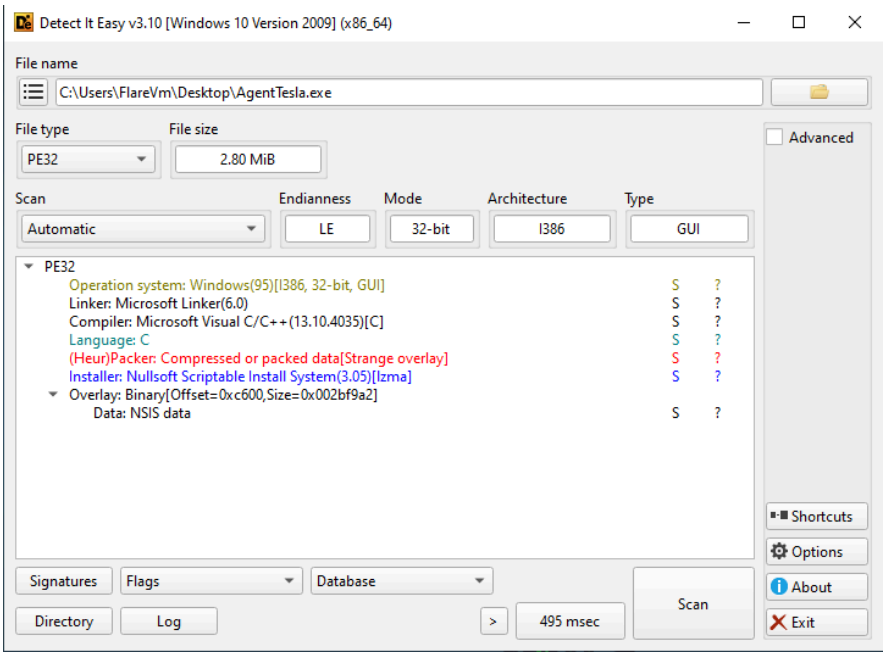




4. Rilevamento Packer (Analisi Protezioni)

Questa è la fase più critica dell'analisi. Utilizzando **Detect It Easy (DiE)**, è emerso che il file non è un semplice eseguibile .NET, ma un contenitore.

- **Packer/Installer Rilevato: Nullsoft Scriptable Install System (NSIS) v3.05**.
- **Compressione:** Dati compressi con algoritmo **lzma**.
- **Linguaggio Wrapper:** C



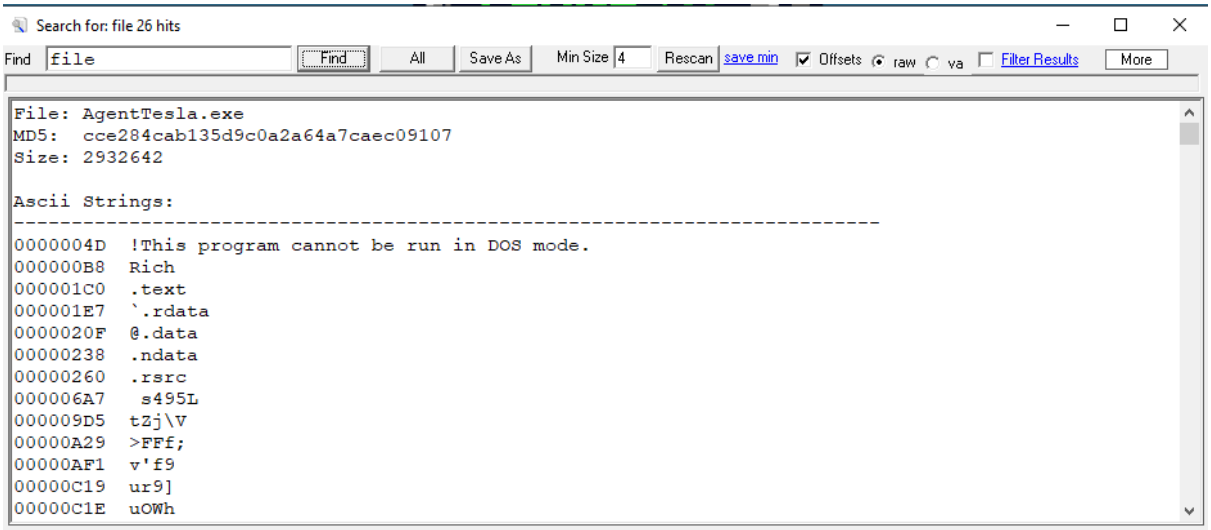
5. Analisi delle Stringhe

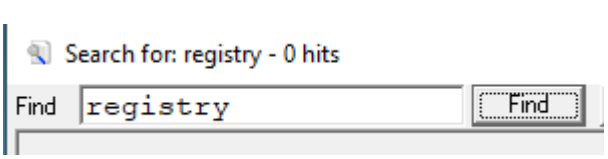
A causa della natura "impacchettata" del file (NSIS Installer), l'estrazione delle stringhe ASCII e Unicode ha prodotto risultati limitati, confermando l'offuscamento del payload.

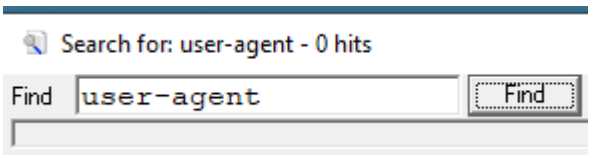
Categoria	Esito Ricerca	Dettagli Tecnici
URL / Domini	Negativo	Nessun dominio visibile in chiaro. Trovata solo la variabile interna `!URL`.
Indirizzi IP	Negativo	Nessun indirizzo IP rilevato in chiaro.
Email	Negativo	Nessuna email rilevata in chiaro.
Chiavi Registry	Negativo	Nessuna chiave di persistenza leggibile.
User-Agent	Negativo	Stringa User-Agent non presente in chiaro.
Percorsi file	Positivo	Trovate chiamate API come `CreateDirectoryW`, `WriteFile`, `GetTempFileNameW`. Questo indica che l'installer, una volta avviato, creerà file temporanei ed estrarrà il malware sul disco.


Search for: Url - 2 hits
Find Url Find All Save As Min Size 4 Rescan save min Offsets raw va Filter Results More
002C695D j.Qa><
002C696C }wD%,p
002C697D j9k@S2.
002C6A18 4l/M}
002C6A46 pze`
002C6AEB vg*h
002C6B3B $ T{
002C6B94 fx!0
002C6BAA n3[7
002C6BC9 nw}F$
002C6BE3 VTTQy1
002C6BEF @"5"
002C6C1B /A!.
002C6C8C p~V;`e
002C6CA8 +g5m
002C6CB7 :O4r
002C6D72 |e9e
002C6E11 !>B
002C6E49 lURL


Search for: address - 2 hits
Find address Find All Save As Min Size 4 Rescan save min Offsets raw va Filter Results More
00007368 GlobalUnlock
00007378 GlobalLock
00007386 CreateThread
00007396 GetLastError
000073A6 CreateDirectoryW
000073BA CreateProcessW
000073CC RemoveDirectoryW
000073E0 lstrcmpiA
000073EC CreateFileW
000073FA GetTempFileNameW
0000740E WriteFile
0000741A lstrcpyA
00007426 MoveFileExW
00007434 lstrcatW
00007440 GetSystemDirectoryW
00007456 GetProcAddress
00007468 GetModuleHandleA
0000747C GetExitCodeProcess
00007492 WaitForSingleObject


Search for: file 26 hits
Find file Find All Save As Min Size 4 Rescan save min Offsets raw va Filter Results More
File: AgentTesla.exe
MD5: cce284cab135d9c0a2a64a7caec09107
Size: 2932642
Ascii Strings:
0000004D !This program cannot be run in DOS mode.
000000B8 Rich
000001C0 .text
000001E7 `.rdata
0000020F @.data
00000238 .ndata
00000260 .rsrc
000006A7 s495L
000009D5 tZj\V
00000A29 >FFf;
00000AF1 v'f9
00000C19 ur9]
00000C1E uOWh


Search for: registry - 0 hits
Find
registry
Find


Search for: user-agent - 0 hits
Find
user-agent
Find