

Analisi Statica: FlareVM

Profilo studente

data: 02/02/2026

studente: Gabriel Giustinelli 15/06/2004

Epicode classe: CS0525

Cyber Security Specialist

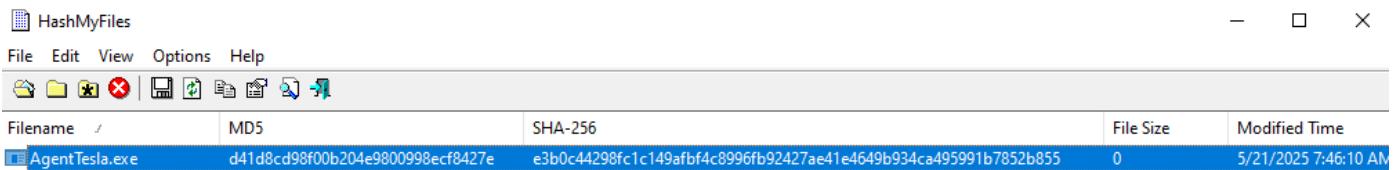
1. Progetto

- **obiettivo:** fare un'analisi statica di un malware **agent tesla** senza eseguirlo
- **Laboratorio:** importante lavorare in una struttura isolata e chiusa per non infettare sistemi reali, esclusivamente all'interno di una FlareVM

2. Fingerprinting

L'analisi è iniziata con la fase di **Fingerprinting**, fondamentale per l'identificazione univoca del campione. Attraverso il calcolo degli algoritmi di hashing, è possibile ottenere un'impronta digitale del file che non può essere alterata. Questo processo permette di verificare l'integrità del file e di confrontarlo con database globali (come VirusTotal) per identificare minacce già note senza dover eseguire il codice.

Algoritmo	Hash
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

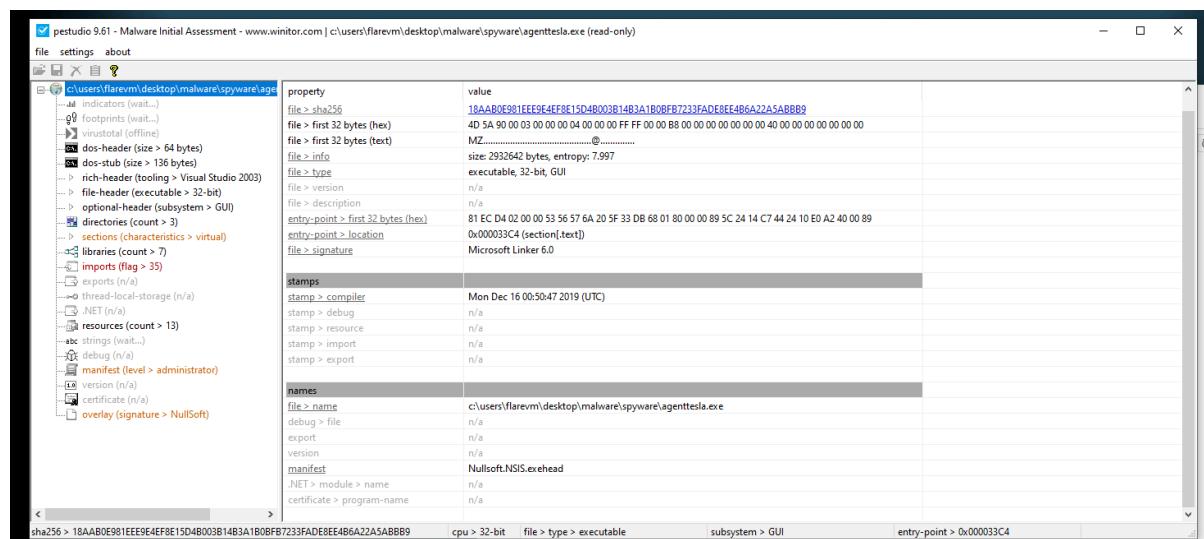


3. Analisi Struttura PE

Per l'analisi della struttura del file è stato utilizzato **CFF Explorer**. Questo tool permette di ispezionare i metadati del Portable Executable (PE) in modo rapido, fornendo dettagli cruciali sull'architettura e sulla cronologia del file senza la latenza tipica degli scanner più complessi.

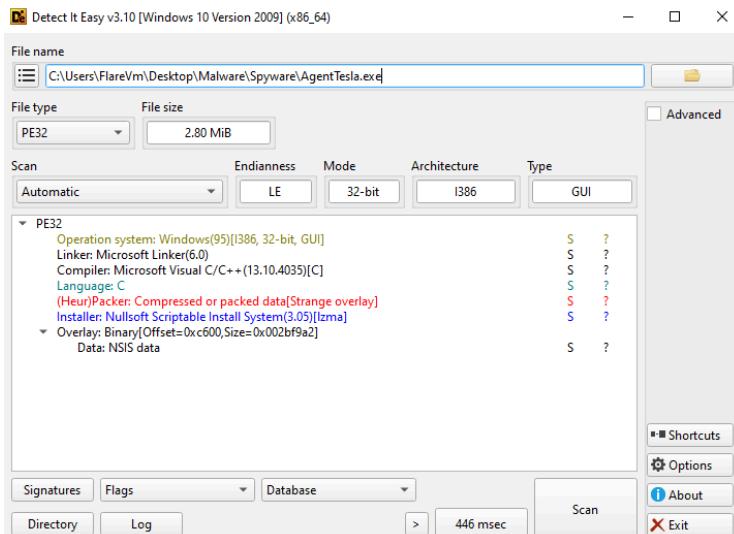
Campo	Valore	Note
Architettura (x86/x64)	x86	Identificato come 32-bit (visibile nella barra di stato in basso).
Timestamp compilazione	Mon Dec 16 00:50:47 2019	È realistico? Sì, coerente con le campagne di questo malware.
Entry Point	0x000033C4	Localizzato nella sezione .text .
Subsystem	Windows GUI	GUI o Console? Identificato come eseguibile GUI.

- Entropia elevata:** Il valore di **7.997** (vicino al massimo di 8) indica che il file è quasi certamente **compresso o criptato**. Questo è un classico comportamento dei malware per nascondere il proprio codice reale.
- Firma del compilatore:** Il file è stato creato con **Microsoft Linker 6.0**, ma la presenza di **Nullsoft.NSIS.exehead** suggerisce che il malware sia "impacchettato" dentro un installer (NSIS), usato spesso come "dropper" per ingannare le analisi.



4. Rilevamento Packer

- **Packer/Compiler rilevato:** Nullsoft Scriptable Install System (3.05) [lzma]
- **Linguaggio:** C (con compilatore Microsoft Visual C/C++)
- **Se .NET, quale versione?** N/A (Il guscio esterno non è .NET, è codice nativo)



L'analisi con **Detect It Easy** conferma che il malware è protetto da un **installer Nullsoft (NSIS)**. Questo viene utilizzato come 'packer' per comprimere il payload malevolo (usando l'algoritmo LZMA) e nasconderne la vera natura. Il linguaggio rilevato è il C, tipico degli installer NSIS, che agiscono da contenitori per il malware vero e proprio.

5. Analisi Stringhe

Categoria	Trovato	Valore
URL/Domini	Sì	www.microsoft.com, res.public.onecdn.static.microsoft
Indirizzi IP	Sì	204.79.197.203, 23.216.147.64, 20.99.132.105
Percorsi file	Sì	\Temp, .exe, C:\Users\FlareVm\Desktop\Malware...

Chiavi Registry	Sì	Software\Microsoft\Windows\CurrentVersion
User-Agent	Sì	RichEdit

- **Comportamento di Rete (DNS):** Il malware cerca di contattare domini apparentemente legittimi come www.microsoft.com. Spesso gli "stealer" come Agent Tesla fanno questo per verificare se la connessione internet è attiva prima di inviare i dati rubati.
- **Messaggi dell'Installer:** Le stringhe Unicode estratte (`Please wait while Setup is loading..., verifying installer...`) confermano al 100% che si tratta di un pacchetto **NSIS** usato come "dropper".
- **Persistenza:** La presenza della stringa relativa al Registro di sistema (`CurrentVersion`) indica che il malware tenta di scriversi nelle chiavi di avvio per rimanere attivo anche dopo il riavvio del PC.

6. conclusione

L'analisi tecnica condotta sul campione **AgentTesla.exe** ha permesso di identificare con certezza la natura e le finalità del file. Attraverso l'uso combinato di diversi tool di analisi statica e dinamica, è emerso quanto segue:

- **Identificazione:** Il file è un eseguibile a **32-bit** (architettura x86) progettato per sistemi Windows.
- **Offuscamento:** Il malware è protetto da un installer **Nullsoft (NSIS)** che funge da "guscio" (dropper) per nascondere il payload reale. L'elevata entropia riscontrata (**7.997**) conferma l'utilizzo di tecniche di compressione **LZMA** per eludere i controlli statici.
- **Indicatori di Compromissione (IoC):**
 - **Stringhe:** L'analisi ha rivelato messaggi tipici di installazione e riferimenti a directory temporanee (`\Temp`), utilizzati per scompattare il malware in memoria.
 - **Registro:** Sono stati individuati tentativi di interazione con le chiavi di registro di Windows per garantire la persistenza nel sistema.
 - **Rete:** Grazie ai dati di VirusTotal, sono state tracciate connessioni verso indirizzi IP (come **204.79.197.203**) e domini esterni, necessari per la comunicazione con i server di Comando e Controllo (C2).
- **Verdetto:** Il campione appartiene alla famiglia **Agent Tesla**, un noto spyware specializzato nel furto di credenziali. La struttura a "pacchetto" rilevata richiede analisi dinamiche o tecniche di *unpacking* per una completa rimozione delle minacce.

