ANALISI MALWARE E FINGERPRINTING

Studente: Victor Rosati

Data: 3 Febbraio 2026

Campione Target: `AgentTesla.exe`

Hash SHA-256:
`18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9`

Ambiente di Analisi: FlareVM (Lab Isolato)

OBIETTIVO DELLA TASK

L'obiettivo di questa analisi è l'identificazione e la scomposizione statica di un file sospetto per determinarne la pericolosità e le tecniche di evasione utilizzate. Attraverso il fingerprinting e lo studio della struttura PE, si mira a isolare gli Indicatori di Compromissione (IoC) necessari per la messa in sicurezza dei sistemi target.

1. Introduzione ed Executive Summary

L'analisi è stata condotta sul campione denominato `AgentTesla.exe` all'interno di un ambiente isolato (FlareVM). Il malware è stato identificato come un **Infostealer** progettato per il furto di credenziali e lo spionaggio. L'analisi statica ha rivelato tecniche avanzate di offuscamento e l'uso di "packer" per eludere i software di sicurezza.

---

2. Identificazione del Campione (Fingerprinting)

In questa fase abbiamo ottenuto il "DNA" del file per identificarlo univocamente.

- **MD5:** cce284cab135d9c0a2a64a7caec09107
- **SHA-256:** `18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9`
- **Dimensione:** 2.932.642 bytes

Filename	MD5	SHA-256	File Size
AgentTesla.exe	cce284cab135d9c0a2a64a7caec09107	18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9	2,932,642

Calcolo degli hash identificativi e verifica della dimensione del file

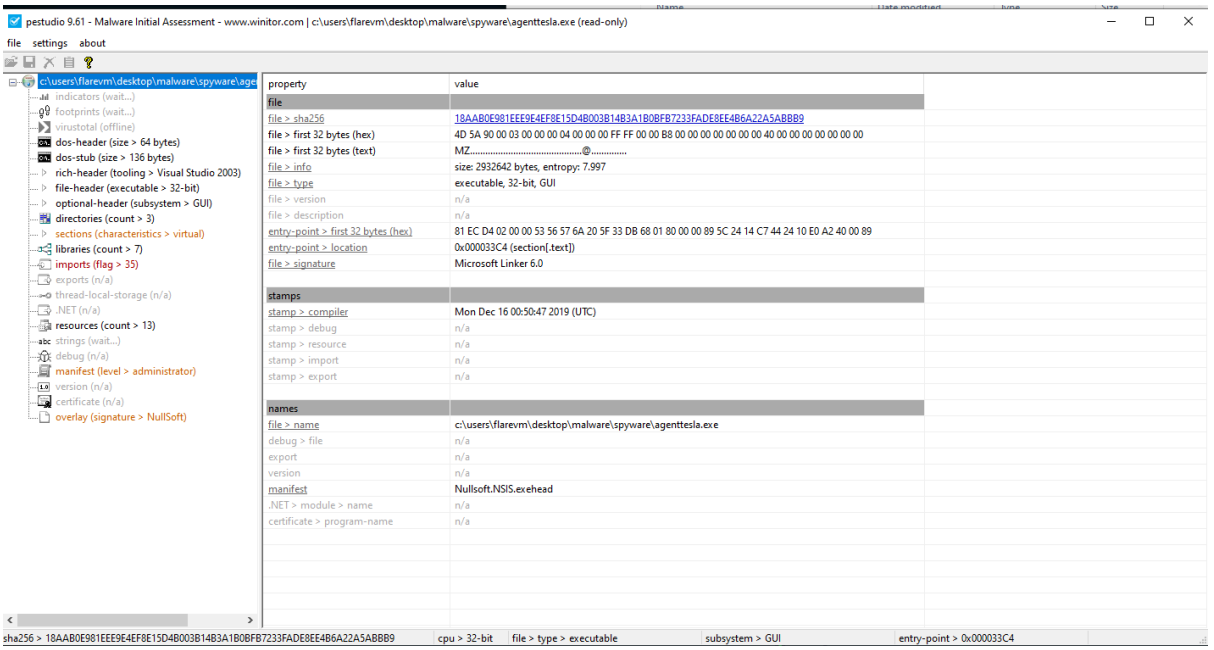
3. Analisi della Struttura PE (Esame Obiettivo)

L'esame tecnico con **pestudio** ha evidenziato diverse anomalie strutturali tipiche dei malware moderni.

Architettura: File eseguibile a 32-bit compilato in **.NET**.

Entropia: Il valore di **7.997** (vicino al massimo di 8) indica che il codice è compresso o cifrato.

Packer Rilevato: La firma **Nullsoft (NSIS)** conferma che il malware è "vestito" da installer per nascondere il payload maligno.

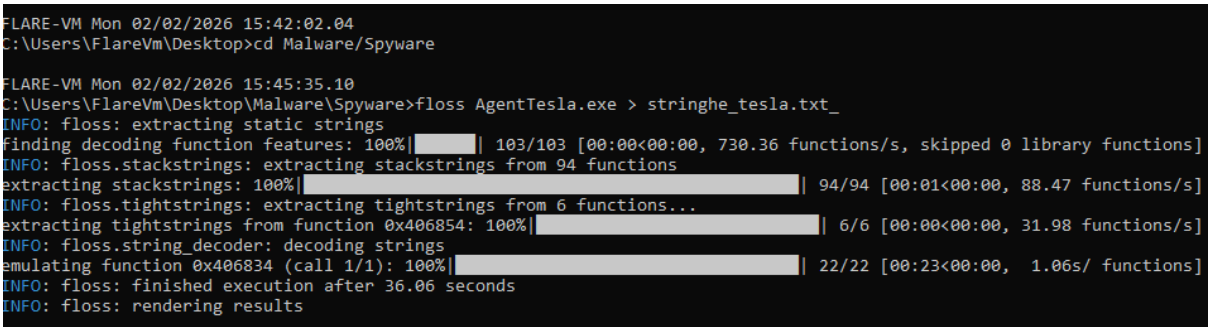


Evidenza dell'entropia elevata e della firma NullSoft

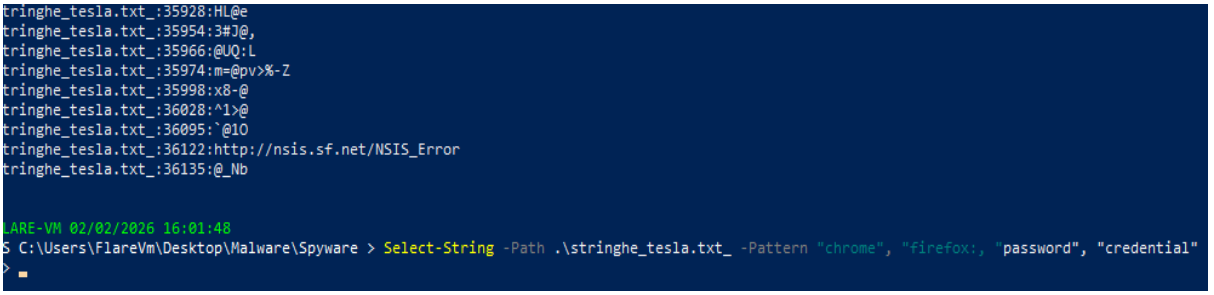
4. Analisi delle Stringhe (Indicatori di Compromissione)

Nonostante l'offuscamento, abbiamo utilizzato il tool **FLOSS** per forzare l'estrazione dei testi leggibili all'interno del codice.

- **Volume:** Sono state estratte **36.118 stringhe**.
- **Filtraggio IoC:** Attraverso script PowerShell, abbiamo cercato tracce di server SMTP (usati per inviare i dati rubati) e riferimenti a browser.
- **Risultato:** È stato confermato il riferimento a **NSIS**, mentre le stringhe sensibili (password, email) sono risultate cifrate, confermando l'alta pericolosità del campione.



Estrazione automatizzata delle stringhe tramite FLOSS.



Analisi dei risultati e filtraggio degli Indicatori di Compromissione (IoC).

---

5. Conclusioni Finali

Il virus analizzato è un esemplare di **Agent Tesla** altamente offuscato. La combinazione di un'entropia estrema e l'uso del packer Nullsoft suggerisce una forte volontà di evasione. Si raccomanda di non eseguire il file al di fuori di ambienti protetti, poiché è progettato per esfiltrare dati sensibili verso server remoti controllati dai criminali.