

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.

The screenshot shows the pestudio interface with the following details:

- File Path:** c:\users\flarevm\Desktop\malware\spyware\agenttesla.exe
- File Properties:**
 - file > sha256:** 18AAB0E981EEE9E4EF8E15D4B003B14B3A1B0FB723FADE8EE4B6A22A5ABB9
 - file > first 32 bytes (hex):** 4D 5A 90 00 03 00 00 04 00 00 FF FF 00 B8 00
 - file > first 32 bytes (text):** MZ.....@.....
 - size:** 293264 bytes, entropy: 7.997
 - file > type:** executable, 32-bit, GUI
 - file > version:** n/a
 - file > description:** 81 EC D4 02 00 00 53 56 57 6A 20 5F 33 DB 68 01 80 00 00 89 5C 24 14 C7 44 24 10 E0 A2 40 00 89
 - entry-point > first 32 bytes (hex):** 0x000033C4 (section:.text)
 - entry-point > location:** Microsoft Linker 6.0
 - file > signature:** n/a
- Stamps:**
 - stamp > compiler:** Mon Dec 16 00:50:47 2019 (UTC)
 - stamp > debug:** n/a
 - stamp > resource:** n/a
 - stamp > import:** n/a
 - stamp > export:** n/a
- Names:**
 - file > name:** c:\users\flarevm\Desktop\malware\spyware\agenttesla.exe
 - debug > file:** n/a
 - export:** n/a
 - version:** n/a
 - manifest:** Nullsoft.NSIS.exehead
 - .NET > module > name:** n/a
 - certificate > program-name:** n/a

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.

```
FLARE-VM Mon 02/02/2026 15:42:02.04
C:\Users\FlareVm\Desktop>cd Malware/Spyware

FLARE-VM Mon 02/02/2026 15:45:35.10
C:\Users\FlareVm\Desktop\Malware\Spyware>floss AgentTesla.exe > stringhe_tesla.txt_
INFO: floss: extracting static strings
finding decoding function features: 100%|██████████| 103/103 [00:00<00:00, 730.36 functions/s, skipped 0 library functions]
INFO: floss.stackstrings: extracting stackstrings from 94 functions
extracting stackstrings: 100%|██████████| 94/94 [00:01<00:00, 88.47 functions/s]
INFO: floss.tightstrings: extracting tightstrings from 6 functions...
extracting tightstrings from function 0x406854: 100%|██████████| 6/6 [00:00<00:00, 31.98 functions/s]
INFO: floss.string_decoder: decoding strings
emulating function 0x406834 (call 1/1): 100%|██████████| 22/22 [00:23<00:00, 1.06s/ functions]
INFO: floss: finished execution after 36.06 seconds
INFO: floss: rendering results
```

Estrazione automatizzata delle stringhe tramite FLOSS.

```
tringhe_tesla.txt_:35928:H!@e
tringhe_tesla.txt_:35954:3#]@,
tringhe_tesla.txt_:35966:@Q!L
tringhe_tesla.txt_:35974:m=@pv>%-Z
tringhe_tesla.txt_:35998:x8-@
tringhe_tesla.txt_:36028:^\!>@
tringhe_tesla.txt_:36095:`@10
tringhe_tesla.txt_:36122:http://nsis.sf.net/NSIS_Error
tringhe_tesla.txt_:36135:@_Nb

FLARE-VM 02/02/2026 16:01:48
$ C:\Users\FlareVm\Desktop\Malware\Spyware > Select-String -Path .\stringhe_tesla.txt_ -Pattern "chrome", "firefox", "password", "credential"
> -
```

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.