

Analysis Agent Tesla

Amin El Kassimi

CyberSecurity EN
Paolo Rampino
Feb 1, 2026

Executive summary

Mission Status

Analisi statica di base, non reversing profondo e non analisi dinamica.

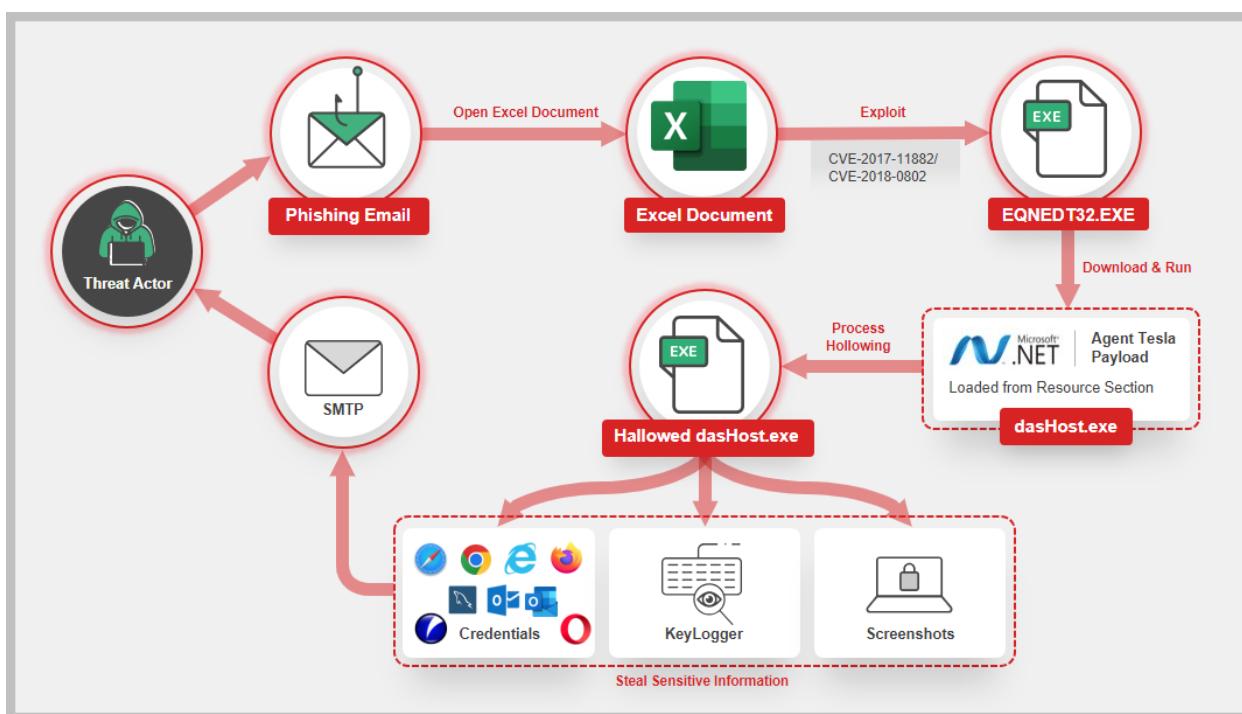
Tradotto:

- **NON eseguire** il malware
- **NON fare debugging**
- **OSSERVARE** il file come oggetto

Si rispondendo alla domanda:

“Che cosa *sembra* essere questo sample, prima di lasciarlo agire?”

Questo è esattamente ciò che fa un SOC o un malware analyst **nei primi 30 minuti**



Malware: Agent Tesla

Agent Tesla è principalmente un **RAT + infostealer**, scritto in .NET.

In pratica è un coltellino svizzero del cybercrimine:

- **Keylogger:** intercetta tutto ciò che viene digitato.
- **Credential stealer:** ruba credenziali da browser, client email (Outlook, Thunderbird), FTP client, VPN, ecc.
- **Clipboard monitor:** osserva cosa copi/incolla (utile per password e crypto wallet).
- **Screenshot grabber:** cattura periodicamente lo schermo.
- **RAT (Remote Access Trojan):** permette all'attaccante di controllare la macchina da remoto in forma "light".

Non è un ransomware, non è un wiper, non fa fuochi d'artificio. È silenzioso, persistente, e **vive di esfiltrazione dati**.

Cosa fa tecnicamente (vista dall'analista)

A grandi linee, quando viene eseguito:

1. Si insedia

- Copia se stesso in directory "normali" (AppData, Roaming)
- Imposta persistenza (registry run keys, talvolta scheduled task)

2. Raccoglie dati

- Hook su tastiera (keylogging)
- Estrazione credenziali da:
 - browser (Chrome, Firefox, Edge)
 - client email
 - software di rete
- Screenshot periodici
- Clipboard scraping

3. Esfiltra

- SMTP (email)
 - FTP
 - HTTP/HTTPS
 - Talvolta Telegram Bot API
- Questa varietà è didatticamente *oro*.

4. Offusca

- Packing leggero
- Stringhe criptate

- Anti-analysis basilari (sleep, check ambienti)
-

Perché è perfetto come *primo malware* di un corso

Agent Tesla è scelto perché è didatticamente “onesto”.

Non è banale, ma nemmeno opaco come un rootkit kernel-mode o un loader polimorfico. Ti permette di imparare **tutti i fondamentali**, uno per uno.

1. È estremamente diffuso

- Esiste da anni
 - Migliaia di varianti
 - Usato in campagne reali
- Questo significa: quello che impari **serve davvero**.

2. Tocca quasi tutte le tecniche base

Con un solo sample puoi studiare:

- fingerprinting
- static analysis
- .NET reversing
- string decryption
- config extraction
- persistence
- C2 logic
- behavioral analysis

Pochi malware coprono così tanto terreno.

3. È leggibile (relativamente)

Essendo .NET:

- puoi usare **dnSpy / ILSpy**
- vedi classi, metodi, flussi logici
- non stai ancora combattendo contro assembly offuscato al livello “stregoneria”

È come imparare anatomia su un corpo reale ma non carbonizzato.

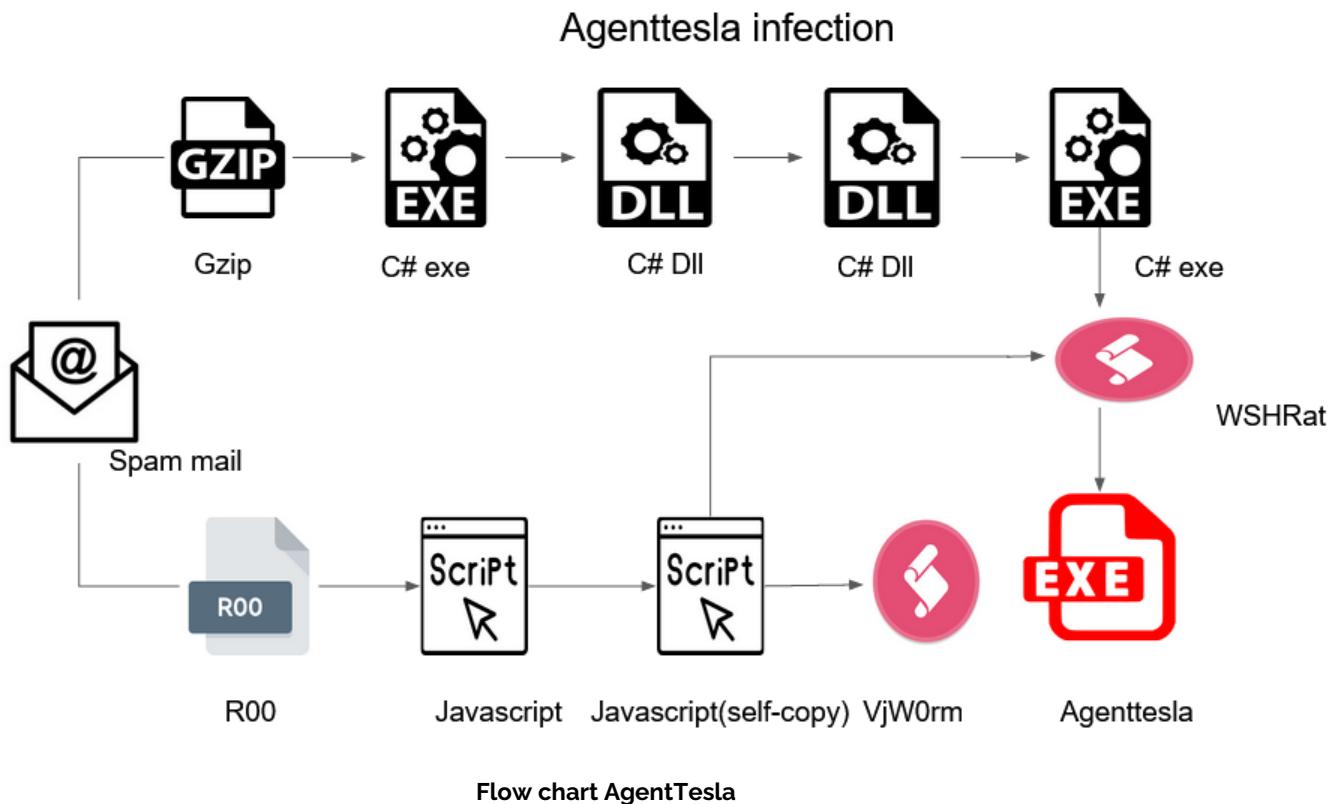
4. È “real world malware”

Molti studenti si aspettano malware spettacolari.

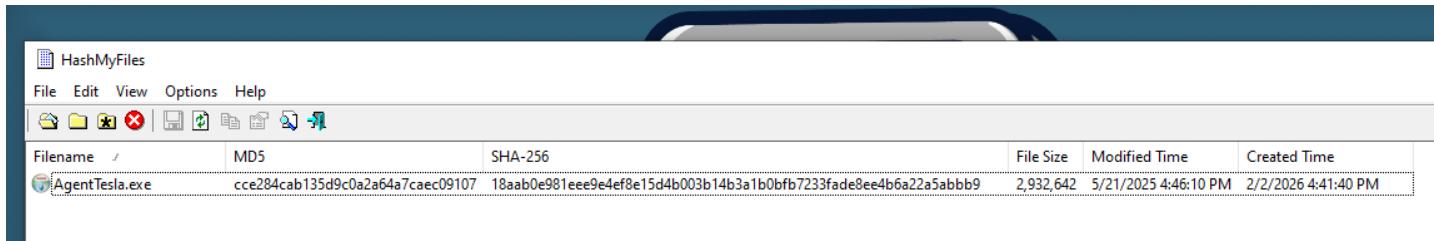
La realtà è questa:

Il crimine informatico vive di furti silenziosi, non di esplosioni.

Agent Tesla insegna **la noia pericolosa** del malware vero.



Fingerprinting



Screen shot dashboard HashMyFiles

Il fingerprinting consente di identificare in modo univoco il sample senza eseguirlo. Gli hash crittografici (MD5 e SHA-256) vengono utilizzati per:

- verificare l'integrità del file durante l'analisi
- confrontare il sample con database di malware noti (VirusTotal, MalwareBazaar, ecc.)
- correlare il campione con altre analisi o campagne già documentate

SHA-256 è preferito per l'univocità crittografica, mentre MD5 è mantenuto per compatibilità e rapidità di lookup.

Algoritmo Hash

MD5 cce284cab135d9c0a2a64a7caec09107

SHA256 18aab0e981eee94ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

Strumenti: Tasto destro sul file hashMyFiles

Analisi Struttura PE

pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\flarevm\Desktop\agenttesla.exe (read-only)

file settings about

c:\users\flarevm\Desktop\agenttesla.exe

- indicators (wait...)
- footprints (wait...)
- virusTotal (score > 27/70)
- dos-header (size > 64 bytes)
- dos-stub (size > 136 bytes)
- rich-header (tooling > Visual Studio 2003)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 3)
- sections (characteristics > virtual)
- libraries (count > 7)
- imports (flag > 35)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (count > 13)
- strings (wait...)
- debug (n/a)
- manifest (level > administrator)
- version (n/a)
- certificate (n/a)
- overlay (signature > NullSoft)

property	value	detail
general		
subsystem	0x0002	GUI
magic	0x010B	PE
file-checksum	0x00000000	0x002D94BB (expected)
<u>entry-point > location</u>	0x000033C4	section [.text]
<u>base-of-code > location</u>	0x00001000	section [.text]
<u>base-of-data</u>	0x00008000	section [.rdata]
size-of-code	0x00006400	25600 bytes
size-of-initialized-data	0x00022A00	141824 bytes
size-of-uninitialized-data	0x00000800	2048 bytes
size-of-image	0x0004C000	311296 bytes
size-of-headers	0x00000400	1024 bytes
size-of-stack-reserve	0x00100000	1048576 bytes
size-of-stack-commit	0x00001000	4096 bytes
size-of-heap-reserve	0x00100000	1048576 bytes
size-of-heap-commit	0x00001000	4096 bytes
section-alignment	0x00001000	4096 bytes
file-alignment	0x00000200	512 bytes
<u>directories > count</u>	0x00000010	16
LoaderFlags	0x00000000	0x00000000
Win32VersionValue	0x00000000	0x00000000
image-base	0x00000000	0x00000000

CFF Explorer VIII - [AgentTesla.exe]

File Settings ?

AgentTesla.exe

Property	Value
File Name	C:\Users\FlareVm\Desktop\AgentTesla.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	2.80 MB (2932642 bytes)
PE Size	49.50 KB (50688 bytes)
Created	Monday 02 February 2026, 16.41.40
Modified	Wednesday 21 May 2025, 15.46.10
Accessed	Tuesday 03 February 2026, 15.03.37
MD5	CCE284CAB135D9C0A2A64A7CAEC09107
SHA-1	E4B8F4B6CAB18B9748F83E9FFF275EF5276199E

Property	Value
Empty	No additional info available

File: Agent Tesla.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

Architettura (x86 / x64)

Valore

- **x86 (32-bit)**

Evidenze

- file-header (executable, 32-bit)
- Portable Executable 32
- cpu > 32-bit

Questo è *classico* Agent Tesla.

I malware commodity scelgono spesso x86 perché:

- gira su **qualsiasi Windows**, anche vecchio
- compatibilità massima con API legacy
- meno problemi di hooking e injection

Non è una scelta tecnica brillante. È una scelta **economica**.



⌚ Timestamp di compilazione

Valore

- **Mon Dec 16 00:50:47 2019 (UTC)**

Nota – È realistico?

👉 Probabilmente NO (o comunque non affidabile)

Perché?

- Agent Tesla è continuamente ricompilato
- i builder spesso **falsificano il timestamp**
- serve a:
 - confondere il timeline analysis
 - simulare "software vecchio e innocuo"

☰ Entry Point

Valore

- **0x000033C4**
- Sezione: **.text**
- Prime istruzioni: codice apparentemente "normale"

Nota (interpretazione)

Questo è molto importante:

- entry point **nella .text**
- nessun salto immediato in sezioni strane
- niente stub visibilmente sospetto

👉 Questo suggerisce:

- packing leggero o assente
- oppure loader semplice (tipico dei .NET malware)

Agent Tesla spesso delega la "vera logica" più avanti, dopo l'inizializzazione del runtime.

💻 Subsystem

Valore

- **GUI**

Nota – GUI o Console?

👉 GUI, ma non perché mostri finestre

Qui è uno dei trick più comuni:

- GUI = nessuna console visibile
- nessun "flash" nero
- l'utente non vede nulla

Il malware **vuole sembrare silenzioso**, non interattivo.

Campo	Valore	Note
Architettura	x86 (32-bit)	Massima compatibilità Windows
Timestamp compilazione	16/12/2019 00:50:47 UTC	Potenzialmente falsificato
Entry Point	0x0000033C4 (.text)	Nessun packer evidente
Subsystem	GUI	Nessuna console visibile