

# Analisi statica

File: AgentTesla.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

Property	Value
File Name	C:\Users\user\Desktop\Malware\Spyware\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	Tuesday 30 July 2024, 16.17.46
Modified	Tuesday 30 July 2024, 16.17.46
Accessed	Tuesday 08 October 2024, 15.02.15
MD5	CCE284CAB135D9C0A2A64A7CAEC09107
SHA-1	E4B8F4B6CAB18B9748F83E9FFFD275EF5276199E

Property	Value
Empty	No additional info available

26

/ 72

Community Score

8

26/72 security vendors flagged this file as malicious

Reanalyze Similar More

18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

Size 2.80 MB

Last Analysis Date 5 days ago

EXE

AgentTesla.exe

peexe direct-cpu-clock-access runtime-modules overlay detect-debug-environment nsis

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 14

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label hacktool.docmo/negasteal

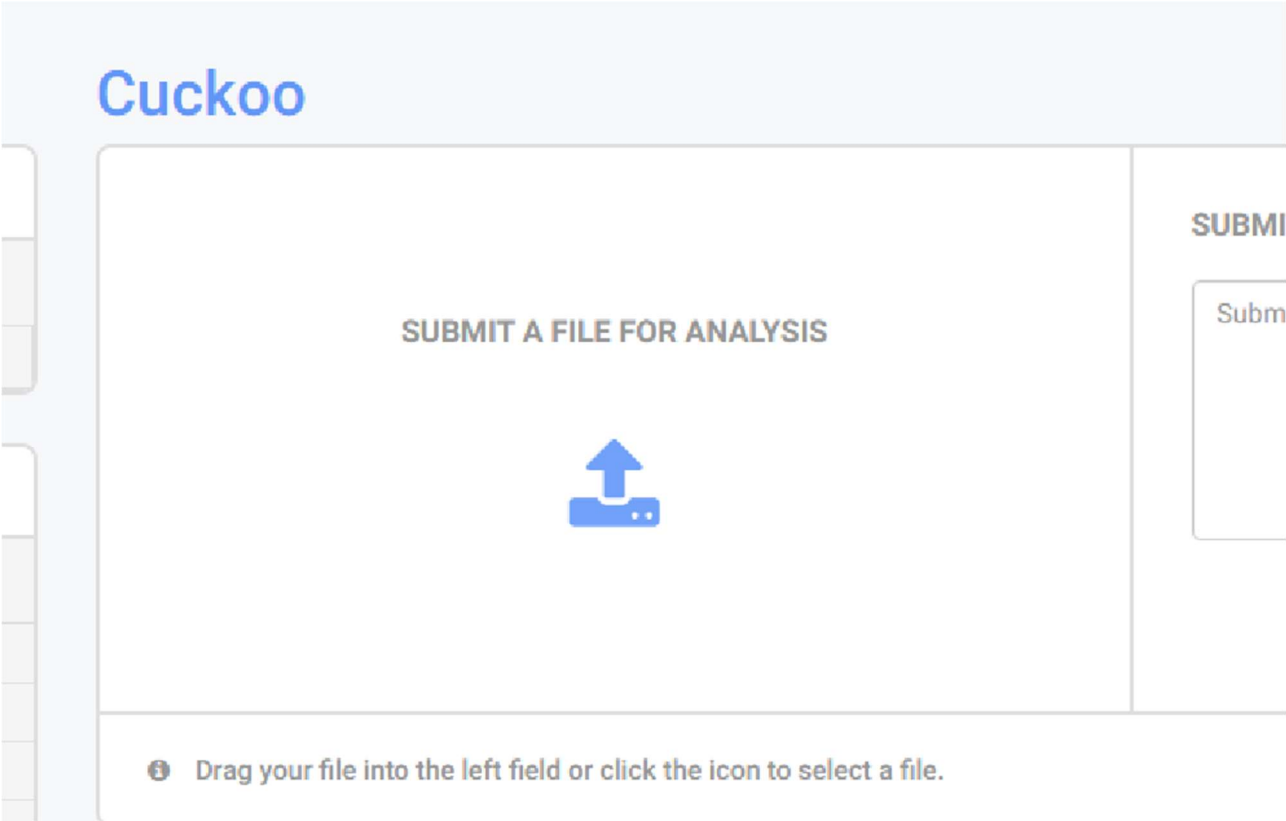
Threat categories hacktool trojan

Family labels docmo negasteal

Security vendors' analysis

Do you want to automate checks?

# Analisi dinamica



## Configure your Analysis



🕒 Information on Execution

Analysis					
Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 8, 2024, 5 p.m.	Oct. 8, 2024, 5:01 p.m.	67 seconds	internet	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

📄 Signatures

- 📘 Yara rules detected for file (5 events)**
- 📘 Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)**
- 📘 The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)**
- 📘 Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation (6 events)**
- 🚫 File has been identified by 6 AntiVirus engine on IRMA as malicious (6 events)**
- 🚫 File has been identified by 26 AntiVirus engines on VirusTotal as malicious (26 events)**

📷 Screenshots



📄 Signatures

- 📘 Yara rules detected for file (5 events)**
- |             |                          |      |                     |
|-------------|--------------------------|------|---------------------|
| description | Escalade privileges      | rule | escalate_priv       |
| description | Take screenshot          | rule | screenshot          |
| description | Affect system registries | rule | win_registry        |
| description | Affect system token      | rule | win_token           |
| description | Affect private profile   | rule | win_files_operation |
- 📘 Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)**

## Summary

 File *AgentTesla.exe*

### Summary

[Download](#) [Resubmit sample](#)

**Size** 2.8MB

**Type** PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

**MD5** cce284cab135d9c0a2a64a7caec09107

**SHA1** e4b8f4b6cab18b9748f83e9fffd275ef5276199e

**SHA256** 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

**SHA512** [Show SHA512](#)

**CRC32** 5C6AB96D

**ssdeep** None

- Yara**
- escalate\_priv - Escalade privileges
  - screenshot - Take screenshot
  - win\_registry - Affect system registries
  - win\_token - Affect system token
  - win\_files\_operation - Affect private profile

 **Information on Execution**