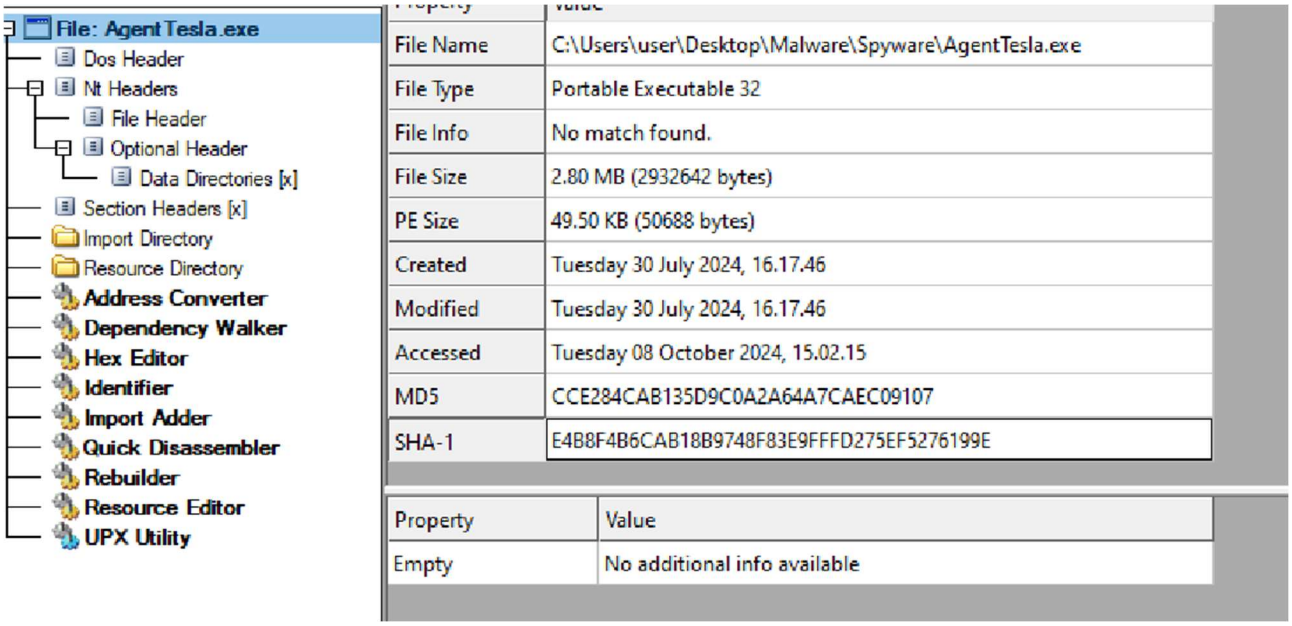
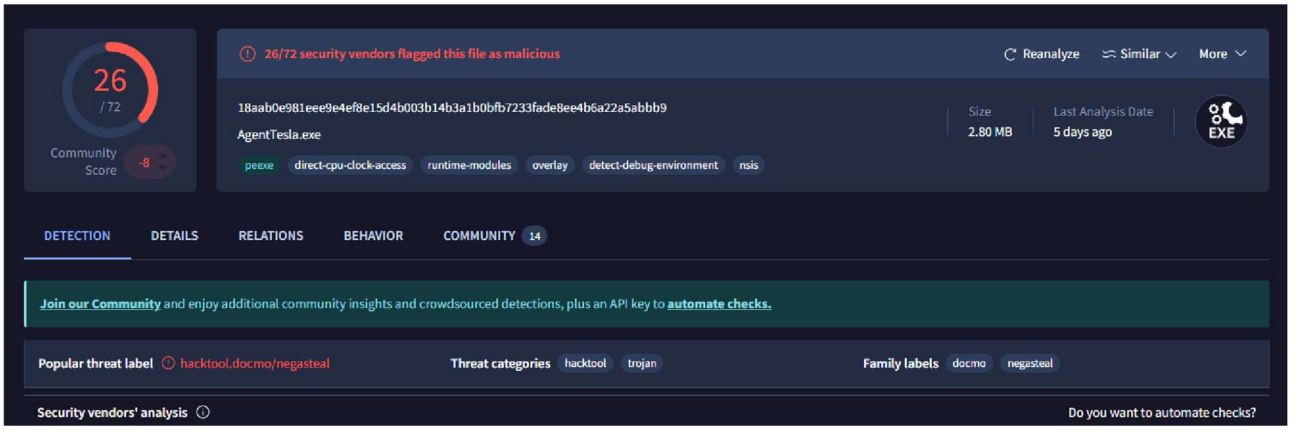
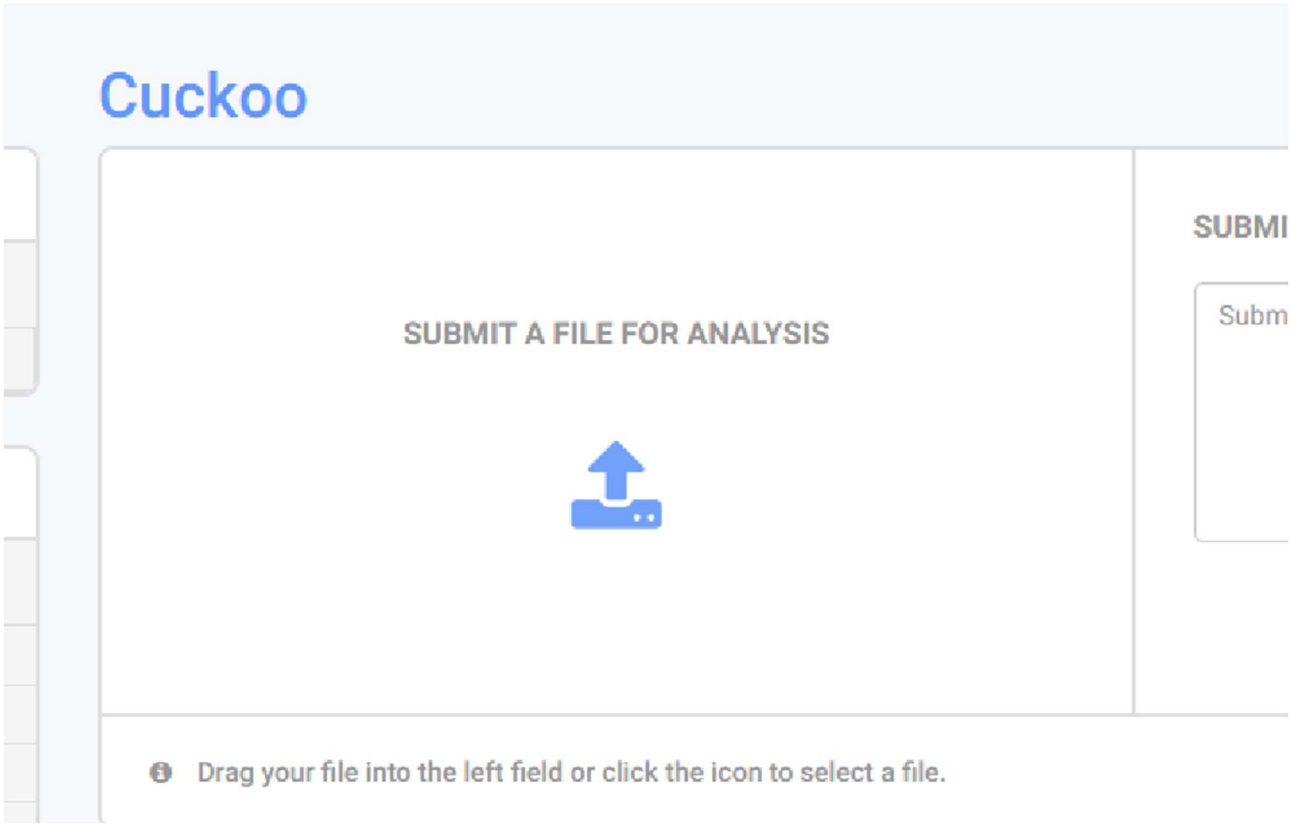
Analisi statica





Analisi dinamica



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	Show Analyzer Log Show Cuckoo Log

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)

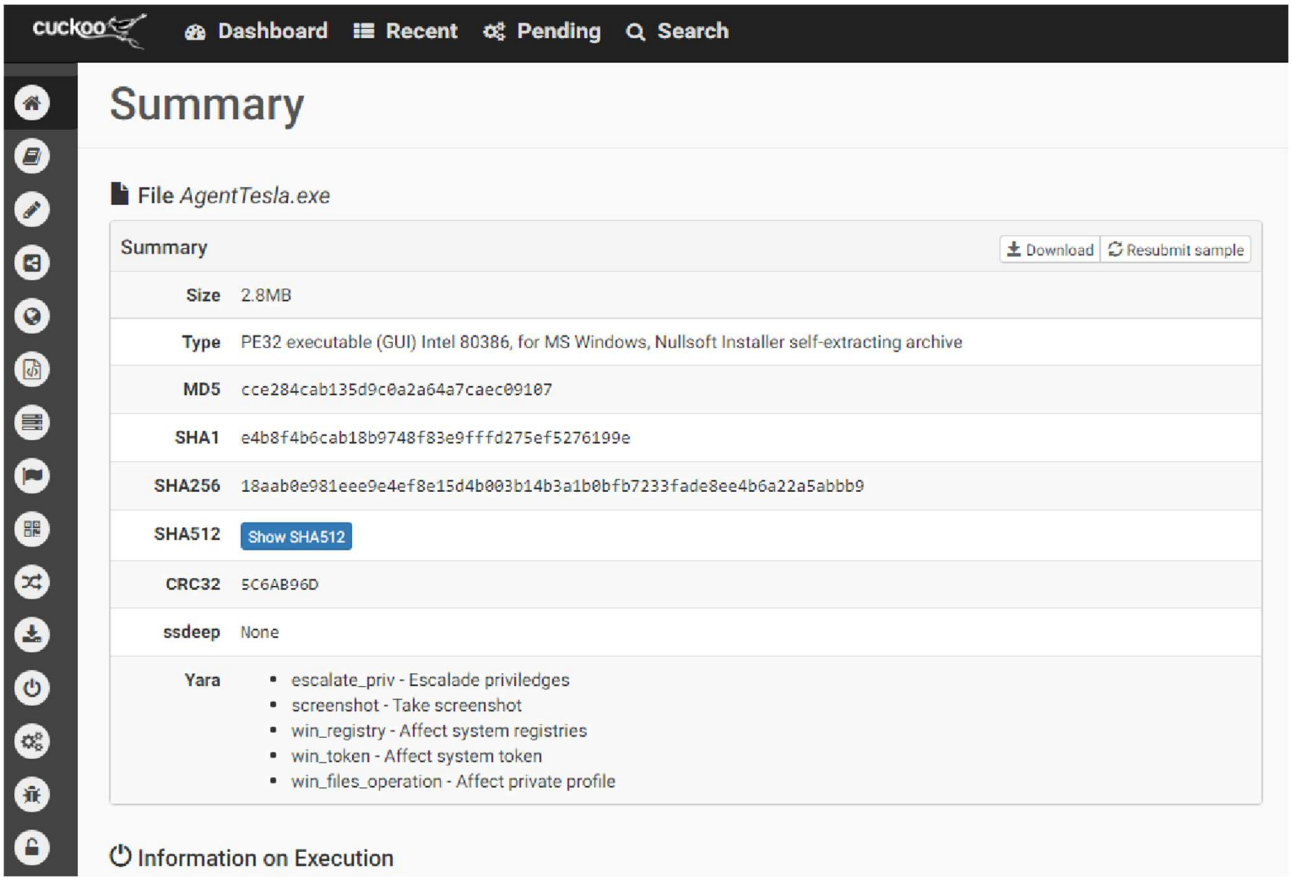
Screenshots

Signatures

Yara rules detected for file (5 events)

description	Escalade priviledges	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)


cuckoo
Dashboard
Recent
Pending
Search
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 priviledges
screenshot - Take screenshot
win_registry - Affect system registries
win_token - Affect system token
win_files_operation - Affect private profile
Information on Execution