

Cuckoo Sandbox Lab

Technical Requirements:

Cuckoo Sandbox

File Link: https://drive.google.com/file/d/1Z9apAlet5YAfj3T-gPMTCb8_q0kgfbkq/view?usp=sharing

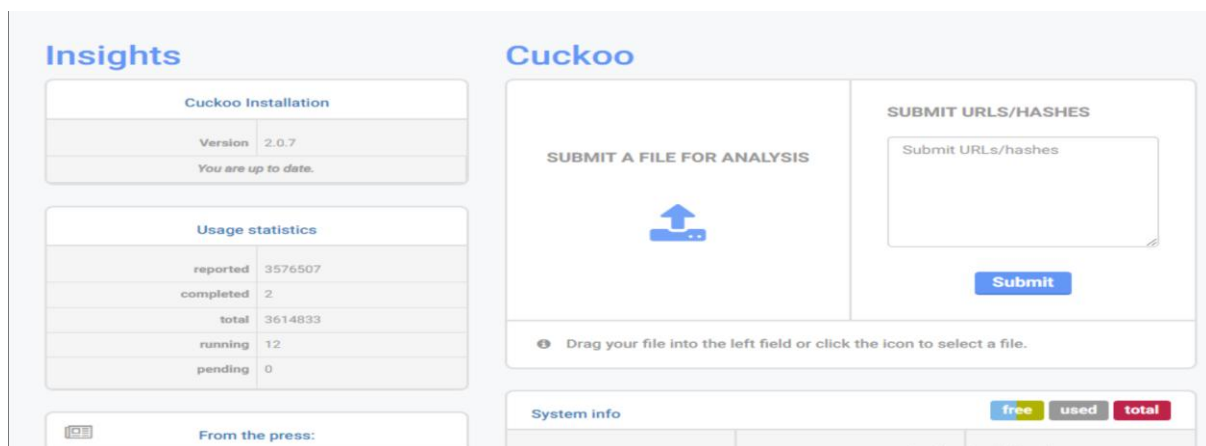
Don't extract the file.

Objective:

To load and analyse malware in the cuckoo sandbox.

Task 1: Upload the Malware Sample

- Open Cuckoo Sandbox in your browser.
- Locate the submit file window.
- Drag and drop the AgentTesla.exe (ZIP) file into the window.
- Click the Submit button to upload the file.



2. Select Analysis Options

- After submission, you will be redirected to a new page with various analysis options.

Configure the following:

- **Network Routing:** (by default, It is selected as INTERNET. if not, manually select it)
- **Timeout:** Adjust if needed, default settings are usually sufficient.
- **Additional Options:** (Optional, leave as default for standard analysis)
- **Machine Selection:** From the dropdown, select Windows as the target system.
- **Analyze:** select it at the top right corner of the screen

submit file

configure

analysis

Configure your Analysis

Reset

Analyze

Package

Priority

LOW

MEDIUM

HIGH

Timeout

SHORT

MEDIUM

LONG

30

SECONDS

Options

Remote Control

Enable connectivity of the VM

Enable Injection

Enable behavioral analysis

Process Memory Dump

Full Memory Dump

Enable Timeout

Enable Simulated Human Interaction

EXTRA OPTIONS

What can I test?

Machine

Submit

AgentTesla.zip

ARCHIVE 183.0 KB

Selection

Search selection

EXTENSION

AGENTTESLA.ZIP

cuckoo

Dashboard

Recent

Pending

Search

Submit

Import

submit file

configure

analysis

Summary

✓ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
6032903	04/03/2025 03:05	0a13ea4fa8362c49dc0ace6bda604ea41e8f5fe78a2691bf7c808c7b88efbf1.exe @ AgentTesla.zip	exe	✓ reported
6032901	04/03/2025 03:05	AgentTesla.zip	7z	completed
Done				

Cuckoo will analyze the executable, and you can track its progress on the right side of the screen next to the file entry. Since the file is in a ZIP format, Cuckoo needs to extract it before starting the actual analysis, which may take some extra time. Once the status changes to "Completed" and then "Reported, go to the "Recent" tab. Look for the extracted executable file, not the ZIP file, using the Task ID, then click the highlighted URL to open the report.

cuckoo

Dashboard

Recent

Pending

Search

Submit

Import

Files

URLs

Score 0 - 4

Score 4 - 7

Score 7 - 10

6032921	2025-03-04 03:06	36e5660806d89d8584f28036fbc85588	AgentTesla.zip	reported	score 7
6032920	2025-03-04 03:06	-	0a13ea4fa8362c49dc0ace6bda604ea41e8f5fe78a2691bf7c808c7b88efbf1.exe @ AgentTesla.zip	reported	score 10
6032461	2025-03-03 22:27	bae817b22faaf860068519813438621	reCAPTCHA.exe	reported	score 0
6032457	2025-03-03 22:25	b55a7837f5cf7592ef31fb99a8e39bfff	509e657a03305cb5_lfahghq.exe	reported	score 9.9
6032456	2025-03-03 22:23	0506634c39f79648712d64f845e287e4	228ce077b0c4fee7_ain.exe	reported	score 4.1
6032454	2025-03-03 22:24	e8bbd229766409a68b62a553499f3fff	83bf417f5fd208e_wuauclt.exe	reported	score 10
6032453	2025-03-03 22:23	de2d86c54e513591e43dc2cd2857132d	282e16491fb871ec_microsofthelp.exe	reported	score 10
6032452	2025-03-03 22:23	5e88cc072bd1262c78fdda559ae43b3	59230c9c42cabef3_rewok.exe	reported	score 10
6032451	2025-03-03 22:23	b565e0bef53b20b422b8319345d21bcb	c8a6dc2541d25baa_rtdcpl64.exe	reported	score 10
6032450	2025-03-03 22:19	05b8982856e4b38ce88a485459e6275b	9448c74588e61f5_TempDefault Programs.lnk	reported	score 0.7
6032449	2025-03-03 22:19	4e05029a3859f6a3591559351809ee81	53f49bd996c3cb11_TempSpeech Recognition.lnk	reported	score 0.7
6032448	2025-03-03 22:16	8e86dde040cf8962cecd34789ab63db5	7d09891f5565f1db_rlminfo.5053	reported	score 0.1
6032446	2025-03-03 22:16	731d073a71af52992f7c3ddc5c95cf1f	f47f6e19241a8042_unicom-34149.exe	reported	score 10
6032445	2025-03-03 22:16	7e63f647d832c07e58338d1d9c3d17ee	8f432e8c2cdded81_unicom-22687.exe	reported	score 10
6032444	2025-03-03 22:15	e9dffa4c1b27b33d361df9a45b22dfb2	5470f9770a39ea8e_csrsll.exe	reported	score 10
6032443	2025-03-03 22:15	1d4f33cb43661ebba747a08f5848848e	b1410d39deae57_pjipecd.exe	reported	score 9.7
6032441	2025-03-03 22:12	865b70535cac91a7fb0a5e7453798edc	random.exe	reported	score 10

Task 2: Reviewing Executable summary.

Once you are redirected to the executable summary page, please notice the file score which shows that this executable has, and this would give an initial idea of how suspicious/malicious this file is.

The screenshot shows the Cuckoo Sandbox Summary page. The file being analyzed is 'Archive 0a13ea4fa8382c49dc0ace6bda604ea41e8f5fe78a2691bf7c809c7b88efbf1.exe @ AgentTesla.zip'. The summary table shows the following details:

Property	Value
Size	183.0KB
Type	PE32 executable (GUI) Intel 80386 Mono/Net assembly, for MS Windows
MD5	187f8b4f33a8ad137084823a6a66386
SHA1	580ca77154fe2252083f3d81174f66a7946399
SHA256	9a13ea4fa8382c49dc0ace6bda604ea41e8f5fe78a2691bf7c809c7b88efbf1
SHA512	Show SHA512
CRC32	e178e897
ssdeep	None
PDB Path	C:\Users\VICTOR\Documents\CryptoObfuscator_Output\FAFA234.pdb
Yara	None matched

On the right, the Score is 10 out of 100, with a warning: 'This archive is very suspicious, with a score of 10 out of 100'. Below the score is a Feedback section.

At the bottom, there is a table for 'Information on Execution':

Category	Started	Completed	Duration	Routing	Logs
ARCHIVE	March 4, 2025, 3:05 a.m.	March 4, 2025, 3:06 a.m.	59 seconds	Internet	Show Analysis Log Show Debug Log

Scroll down to the Signatures Section to review detailed insights about the file's behavior. The signatures are ordered by severity, with the most critical ones highlighted in red, indicating highly malicious activity.

For the current AgentTesla sample, one key observation is that it allocates read-write-execute memory, which suggests it may be injecting code or unpacking itself in memory. This behavior can be further analyzed by reviewing the file signatures to understand how the malware operates.

Answer the following questions by observing the Summary tab and the Signatures section.

Question 1: Does the malware use process injection techniques? If so, which APIs does it utilize?

Under Allocates read-write-execute memory in the signature section, APIs used NtProtectVirtualMemory and NtAllocateVirtualMemory.

Please observe the rest of the signatures marked in red to understand more about the executable being analysed.

Question 2: How many antivirus engines flagged this file as malicious in the IRMA (Incident Response & Malware Analysis) scan?

The file was flagged as malicious by 11 antivirus engines in the IRMA scan

Question 3: Is the malware packed or obfuscated? If yes, what tool or method does it appear to use?

Yes, the malware is obfuscated using CryptoObfuscator, as indicated in the PDB path.

You can now select static analysis from the left pane to view file details view details such as Sections, imports and the strings that are found within this executable. We can also inspect different executable details such as its behavioural analysis response and dropped buffer details.

The screenshot shows the Cuckoo Sandbox interface with the 'Static Analysis' tab selected. The left sidebar contains various analysis options, and the main area displays static analysis results for a file named 'FAFA234.pdb'.

Static Analysis

Static Analysis | Strings | Antivirus | IRMA

PE Compile Time: 2025-03-03 02:25:09

PDB Path: C:\Users\VICTOR\Documents\CryptoObfuscator_Output\FAFA234.pdb

PE Imphash: f34d5f2d4577ed6d9ceec516c1f5a744

Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x00002000	0x0002d19c	0x0002d200	7.93764816604
.reloc	0x00030000	0x0000000c	0x00000200	0.101910425663
.rsrc	0x00032000	0x00000598	0x00000600	4.07407604454

Resources

Name	Offset	Size	Language	Sub-language	File type
RT_VERSION	0x000320a0	0x00000030c	LANG_NEUTRAL	SUBLANG_NEUTRAL	data
RT_MANIFEST	0x000323ac	0x000001ea	LANG_NEUTRAL	SUBLANG_NEUTRAL	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators

Answer the following questions by observing the static analysis tab.

Question 4: What does the PDB path reveal about the malware?

The PDB path suggests that the malware was built using CryptoObfuscator, a tool used to hide code and evade detection. The presence of "VICTOR" in the path may indicate the developer's system username.

Question 5: The .text section of the executable has an entropy value of 7.93. What does this indicate?

An entropy value of 7.93 in the .text section indicates that the executable is likely packed or obfuscated, as high entropy suggests compressed or encrypted code.

Question 6: What is the overall behavior of the malware?

The malware manipulates memory permissions and injects code into other processes to run stealthily. It is obfuscated using CryptoObfuscator to avoid detection and allocates read-write-execute memory, likely to unpack itself or execute code within another process.

We can also export the analysis results by click on 'Export Analysis' and downloading the analysis files such as the logs, suricata files and pcap dumps.

