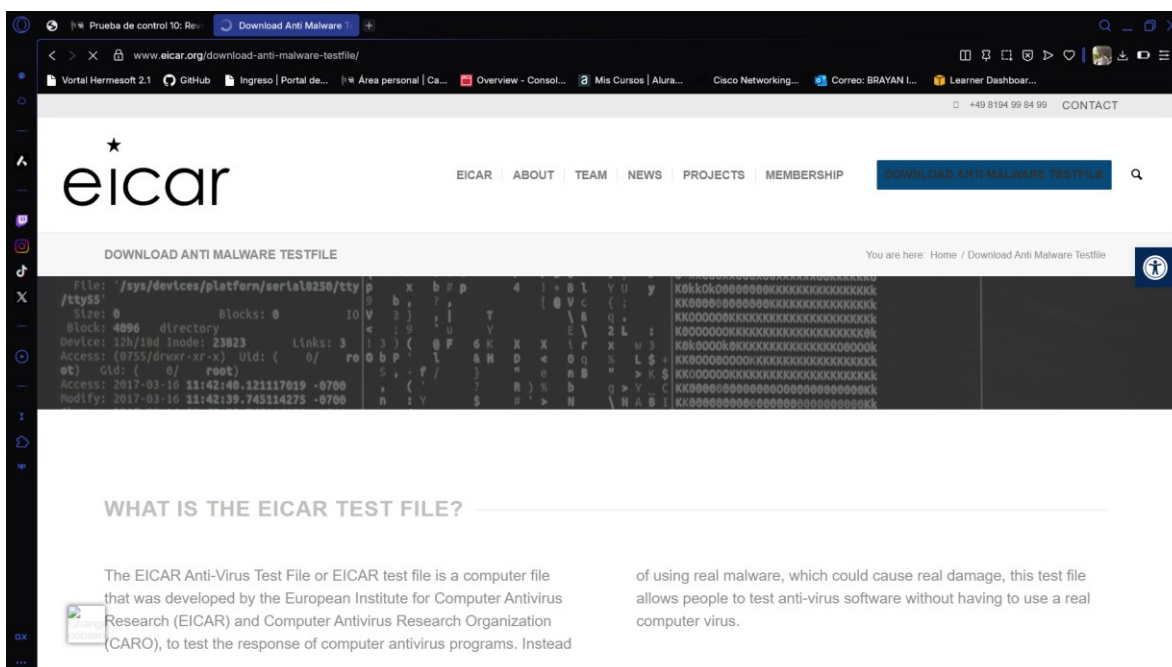
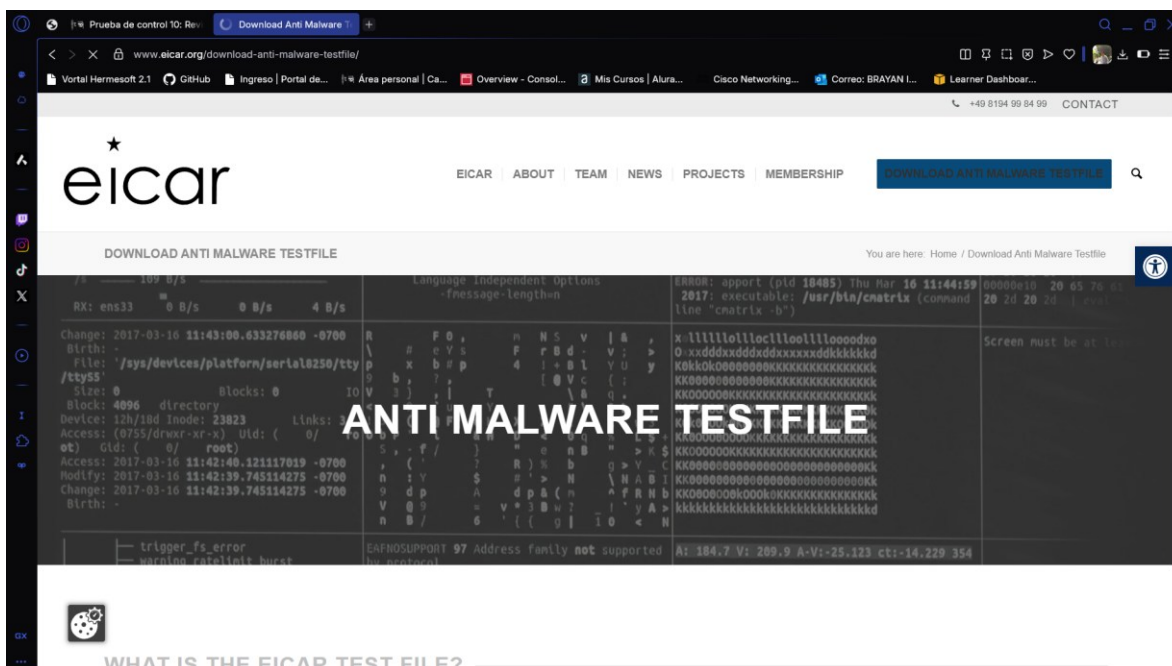


## Laboratorio #10

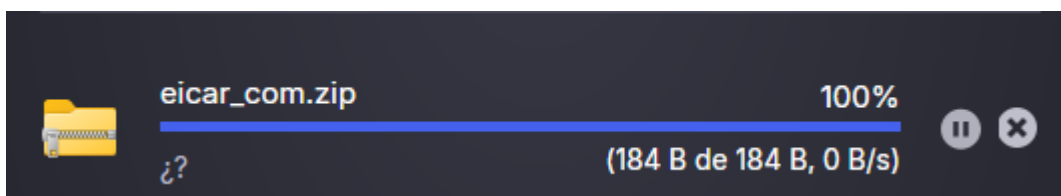
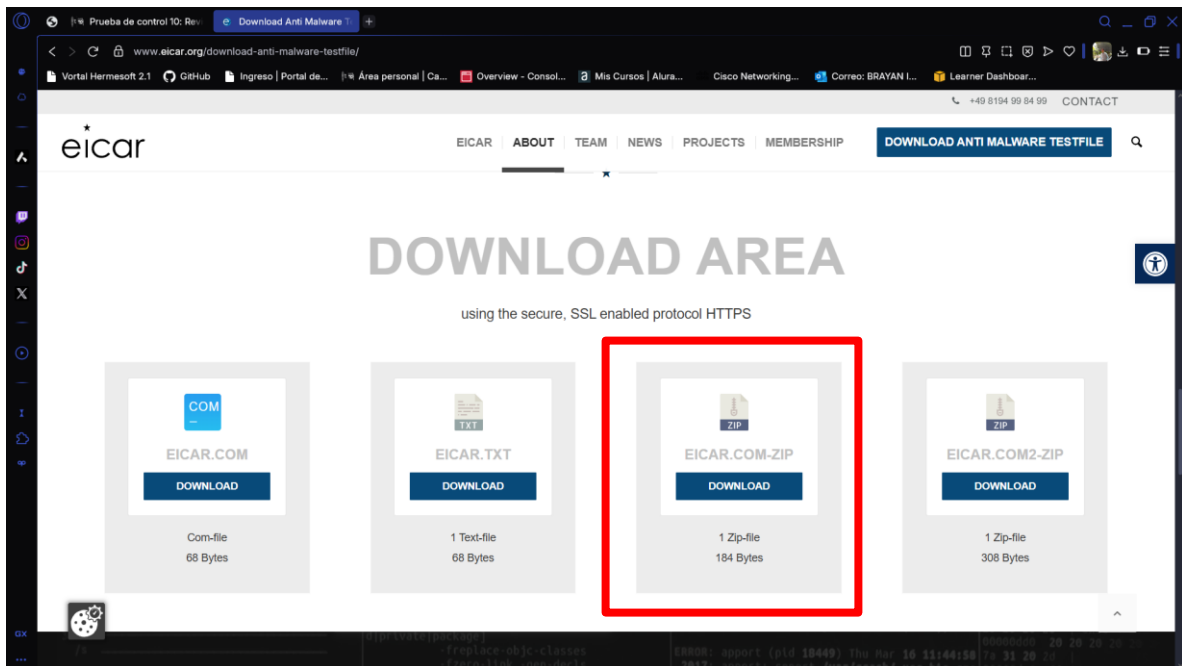
Entrar a la página <https://www.eicar.org> para las pruebas del malware.



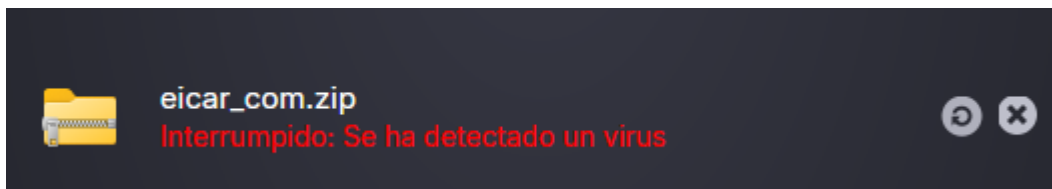
Nos dirigimos al apartado de descargas

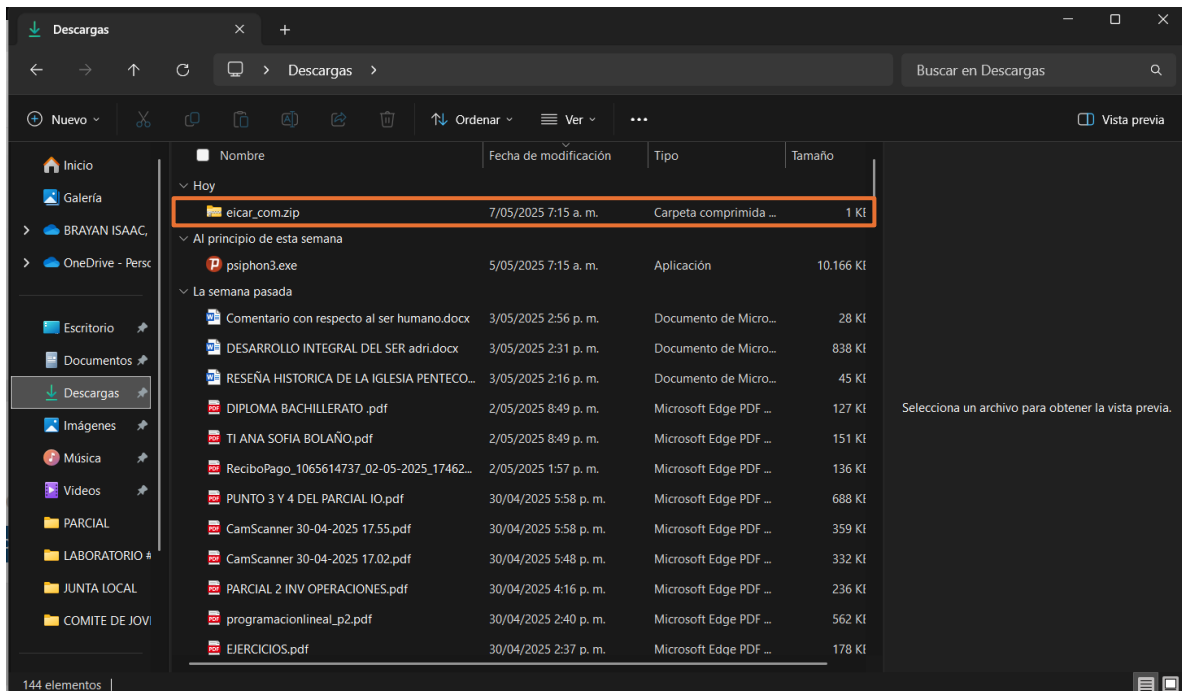


Y nos ubicamos en los archivos de prueba

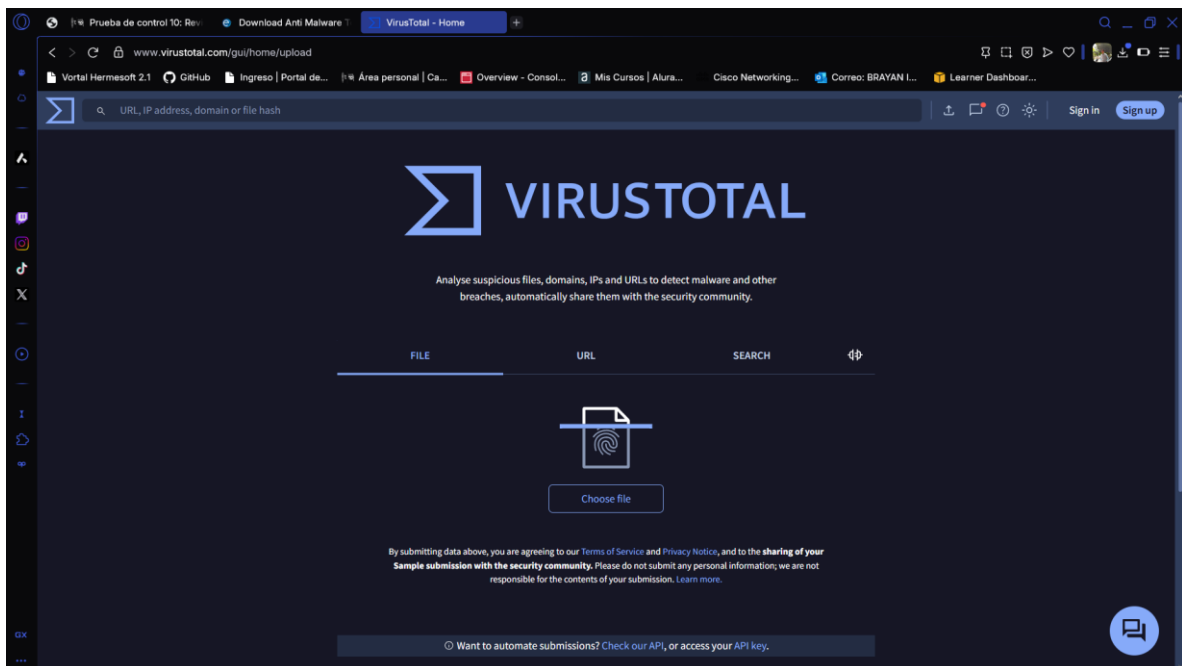


Como es un archivo malicioso el navegador lo bloquea

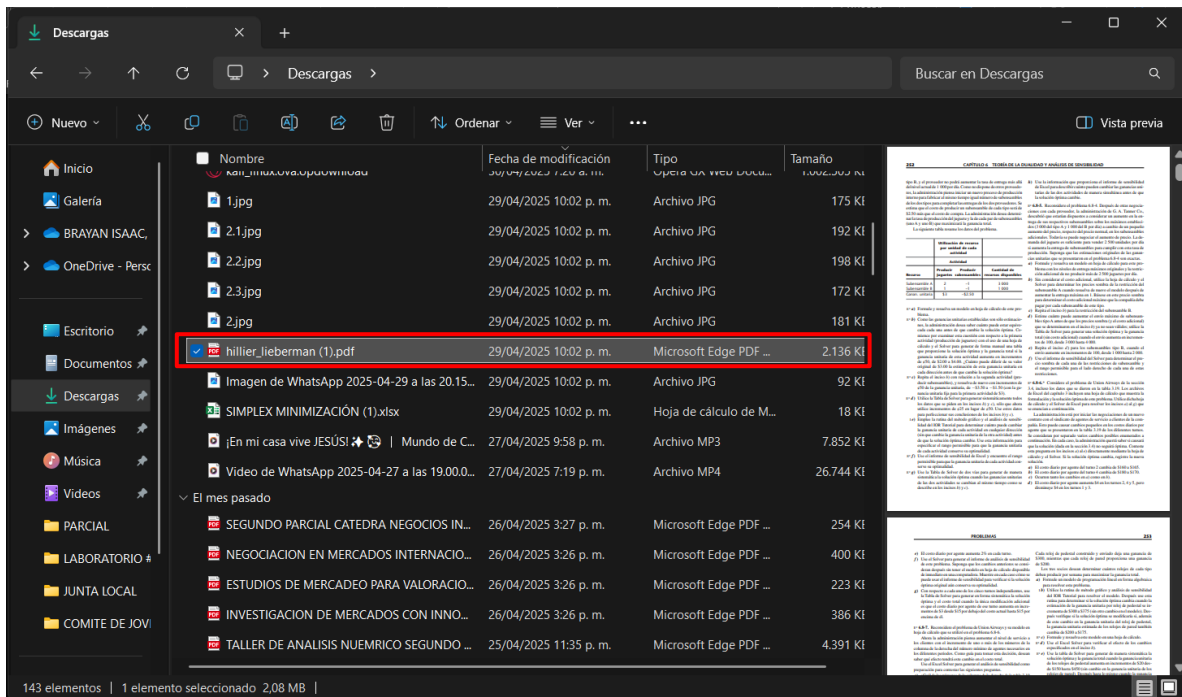




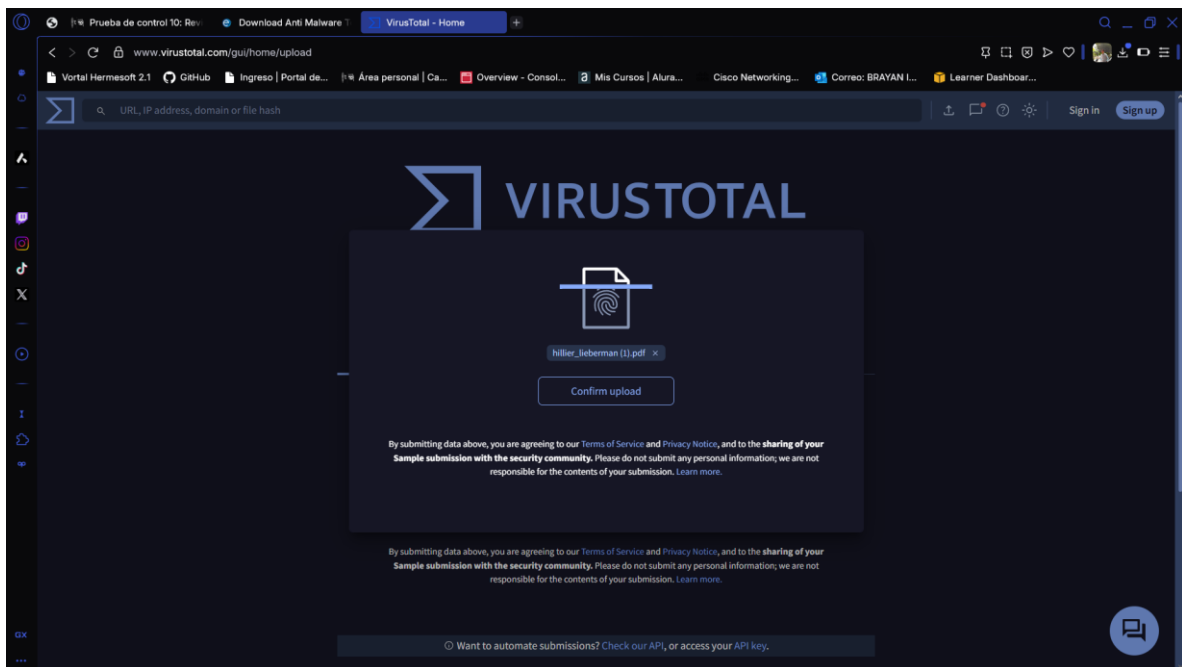
Ahora vamos a analizar documentos para observar la presencia de virus, esto lo haremos con la herramienta <https://www.virustotal.com/>



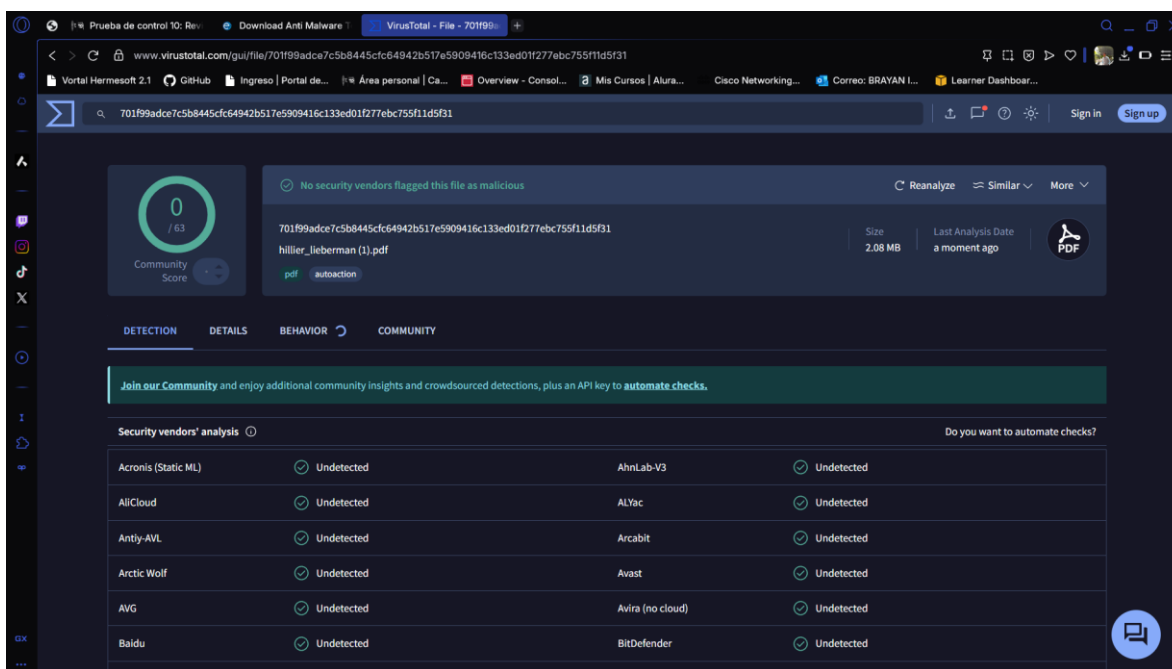
Se selecciona un documento sin presencia de virus para la comparación



Se sube a VirusTotal para el respectivo análisis



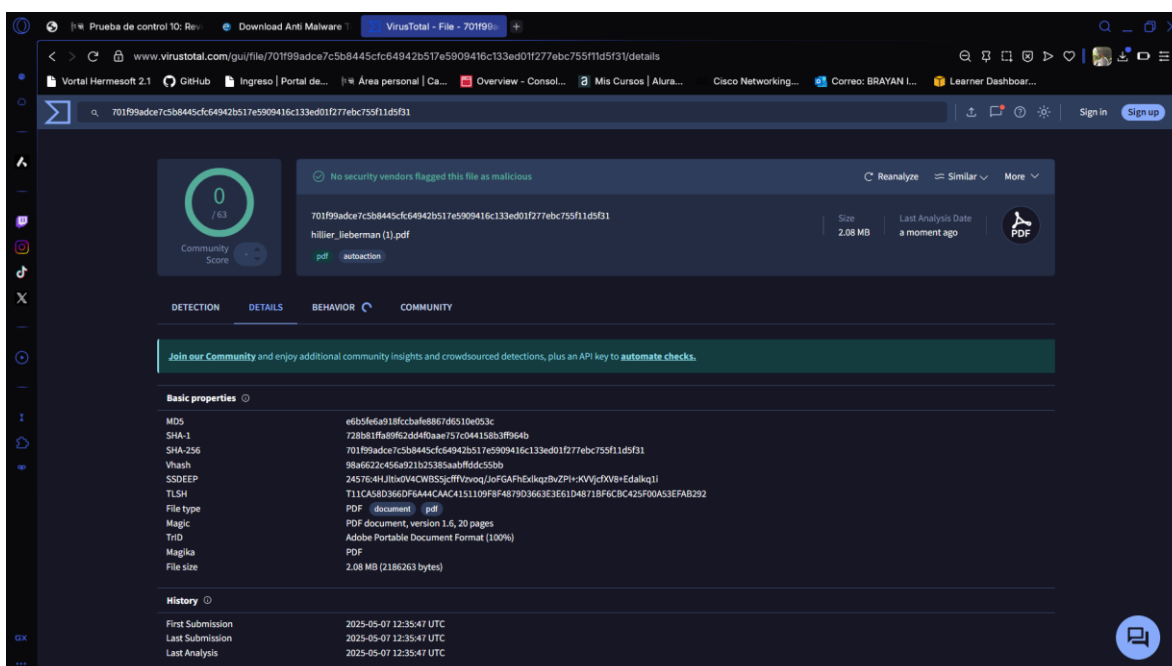
## Se evidencia el resultado del análisis del archivo sin virus



The screenshot shows the VirusTotal web interface for a file analysis. The file is identified as 'hillier\_lieberman (1).pdf' with a size of 2.08 MB. The analysis status is 'No security vendors flagged this file as malicious'. The file is a PDF document, version 1.6, 20 pages, in Adobe Portable Document Format (100%). The file size is 2.08 MB (2186263 bytes).

**Security vendors' analysis**

Vendor	Status	Vendor	Status
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Arctic Wolf	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected



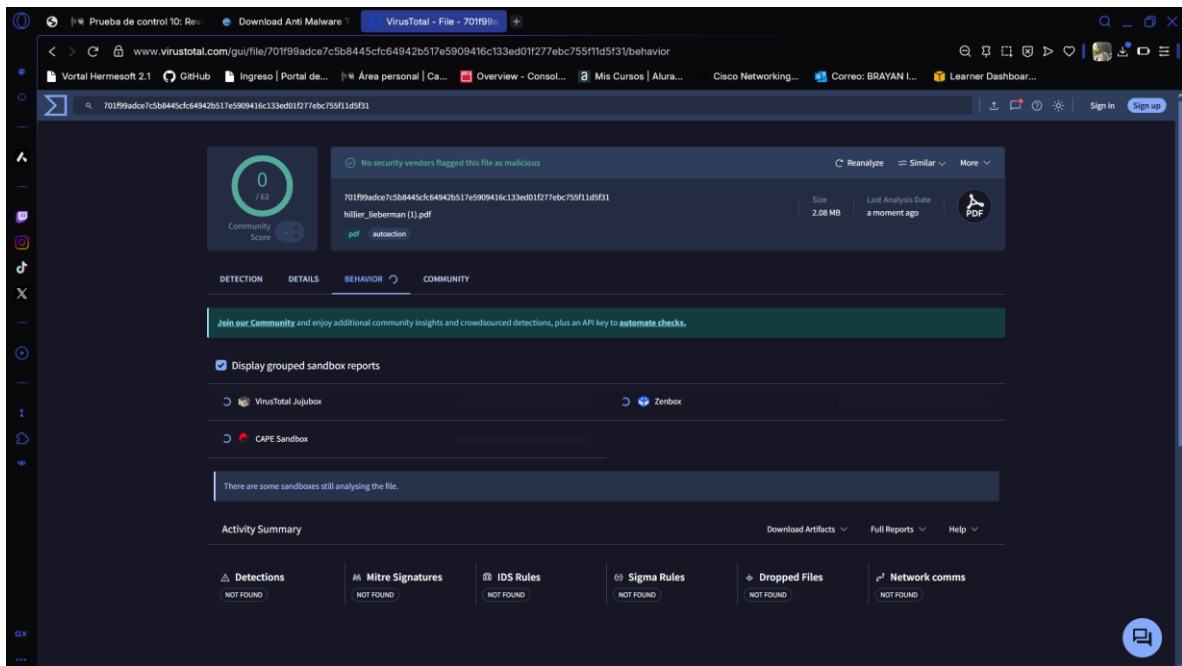
The screenshot shows the VirusTotal web interface for a file analysis, displaying the 'Basic properties' and 'History' sections.

**Basic properties**

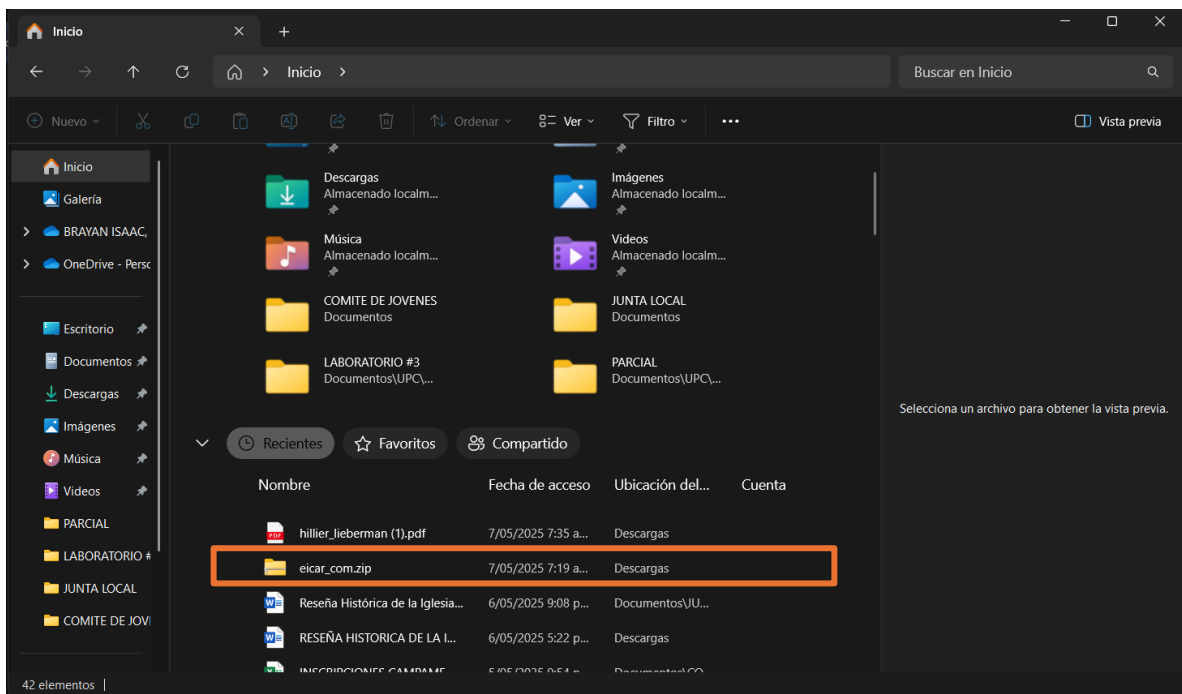
Property	Value
MD5	e6b5f6a918fccbaf68867d6510e053c
SHA-1	728b81ffa89f62d4f0aae757c044158b3f964b
SHA-256	701f99adce7c5b8445cf64942b517e5909416c133ed01f277ebc755f11d5f31
Vhash	98a622c456a921b25385aabf8ddc55b6
SSDEEP	24576:4HJttvQV4CWB55jFFVvvoqJJoFGAPhExdkqzBvZPH-KVvjcfXV9+Edalkq1
TLSH	T11CAS8D366DF6A44CAAC4151109F8F487903663E3E61D4871BF6CB425F00A53EFAB292
File type	PDF (document) (pdf)
Magic	PDF document, version 1.6, 20 pages
Trid	Adobe Portable Document Format (100%)
Magika	PDF
File size	2.08 MB (2186263 bytes)

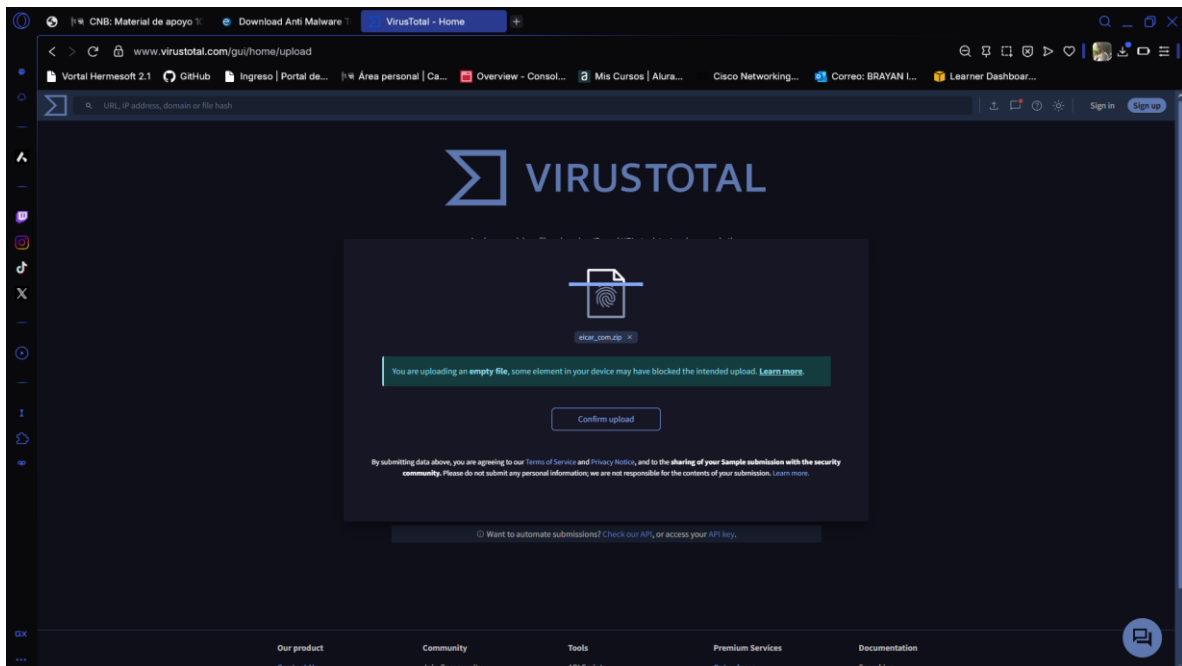
**History**

Event	Date
First Submission	2025-05-07 12:35:47 UTC
Last Submission	2025-05-07 12:35:47 UTC
Last Analysis	2025-05-07 12:35:47 UTC



Ahora, se hará el análisis del archivo eicar\_com.zip para el análisis del virus de prueba





## Captura del análisis de un virus real

61 / 68  
Community Score 486

61/68 security vendors flagged this file as malicious

2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bf44ac23b6e9eedad  
eicar\_com.zip

Size 184 B | Last Analysis Date 1 hour ago | ZIP

zip checks-cpu-name via-tor calls-wmi detect-debug-environment attachment legit sets-process-name

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

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

Popular threat label virus.eicar/test Threat categories virus Family labels eicar test file

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Virus:Win32/EICAR.A
AliCloud	Engtest:Multi/Eicar	ALYac	Misc.Eicar-Test-File
Antiy-AVL	TestFile/Win32-EICAR	ArcaBit	EICAR-Test-File (not a Virus)