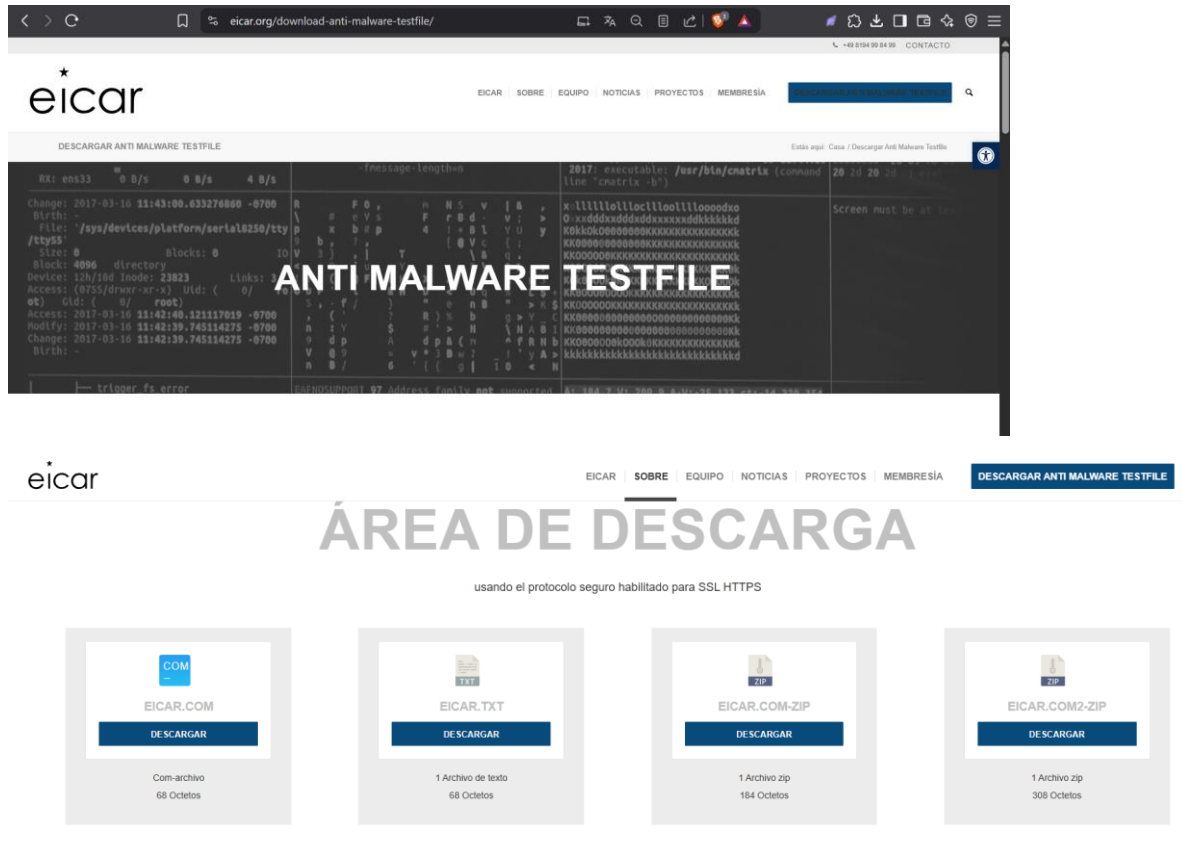


Laboratorio 10

Nos dirigimos a la siguiente página, ahí descargamos un archivo con virus de prueba:



The screenshot shows the EICAR website's download area. The page title is "DESCARGAR ANTI MALWARE TESTFILE". The main heading is "ÁREA DE DESCARGA". Below the heading, it says "usando el protocolo seguro habilitado para SSL HTTPS". There are four download options, each with a "DESCARGAR" button:

- EICAR.COM**: Com-archivo, 68 Octetos.
- EICAR.TXT**: 1 Archivo de texto, 68 Octetos.
- EICAR.COM-ZIP**: 1 Archivo zip, 184 Octetos.
- EICAR.COM2-ZIP**: 1 Archivo zip, 308 Octetos.

Luego vemos que el antivirus del computador nos advierte del virus:



The screenshot shows the Trellix Endpoint Security interface. The main heading is "Análisis en tiempo real". Below the heading, it says "Trellix Endpoint Security ha detectado una amenaza." and "1 Detecciones". There are three buttons: "Limpiar", "Eliminar", and "Quitar entrada". Below the buttons is a table with the following data:

Fecha	Nombre de detección	Tipo	Archivo	Acción tomada
7/5/2025 7:15 AM	EICAR test file	Prueba	---	Eliminar

Saul Hernandez Castilla

Después nos dirigimos a la página Virus Total, en donde analizaremos detalladamente el archivo:

The image displays the detailed analysis results for a file named 'eicar_com.zip' on VirusTotal. The file's SHA-256 hash is '5c347dd322f1da2d5a4baf41dbda9b2c4d861f47d5e68f1044b73b7949dc2'. It has a size of 220 B and was analyzed 'a moment ago'. The Community Score is 59/65, with a note that '59/65 security vendors flagged this file as malicious'. The file is categorized as a 'virus' with family labels 'eicar' and 'test'. A table below shows the analysis results from various security vendors.

Security vendors' analysis	Threat categories	Family labels
AhnLab-V3	Virus/EICAR_Test_File	Misc.Eicar-Test-File
Antiy-AVL	TestFile/WIN32.EICAR	EICAR-Test-File (not A Virus)
Avast	EICAR Test-NOT Virus!!!	Eicar
AVG	EICAR Test-NOT Virus!!!	Eicar-Test-Signature
Baidu	Win32.Test.Eicar.a	EICAR-Test-File (not A Virus)
ClamAV	Win.Test.EICAR_HDB-1	Eicar.test.file
CTX	Zip.virus.eicar	Malicious (score: 99)
DrWeb	EICAR Test File (NOT A Virus!)	Eicar
Emisoft	EICAR-Test-File (not A Virus) (B)	EICAR-Test-File
ESET-NOD32	Eicar Test File	EICAR_TEST_FILE
GData	EICAR_TEST_FILE	Detected
Gridinsoft (no cloud)	Trojan.U.EICAR_Test_File.dd	TEST/AVEngTestFile/EICAR

7.00

Community Score

5c347dd322fd1da2d6a4ba41dbdac9b2c4d861f47d5e68ff1044b73b7949dc2

eicar_com.zip

zip

Size

220 B

Last Analysis Date

a moment ago

ZIP

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties

MD5	c799358de0d7e95e03415f35686c8f38
SHA-1	fb124a1efca2863c54bd83825b3dfb2e4e6148fc
SHA-256	5c347dd322fd1da2d6a4ba41dbdac9b2c4d861f47d5e68ff1044b73b7949dc2
Vhash	ab2a0636ef36c7e5323d917feeb19f9a
SSDEEP	3:vh9NeYh/CTpA/cAJraNvsgzsVqSwHqzON9eYh/IIzGEpSfXmPBSsEzCz/+IKI/-59eYMTpDAJuOgzskozTY4pbb+Ikt/
TLSH	T1B3D02218470E8520F20E603822FD45D72724009D08B13FB4A1C83170CCA70C40CABB4C
File type	ZIP compressed zip
Magic	Zip archive data, at least v1.0 to extract, compression method=store
TrID	ZIP compressed archive (100%)
Magika	ZIP
File size	220 B (220 bytes)

History

First Submission	2025-05-07 12:23:18 UTC
Last Submission	2025-05-07 12:23:18 UTC
Last Analysis	2025-05-07 12:23:18 UTC
Earliest Contents Modification	2000-05-24 19:07:00
Latest Contents Modification	2000-05-24 19:07:00

Names

eicar_com.zip

Bundle info

Contents Metadata

Contained Files	1
Uncompressed Size	68 B
Earliest Content Modification	2000-05-24 19:07:00
Latest Content Modification	2000-05-24 19:07:00

Contained Files By Type