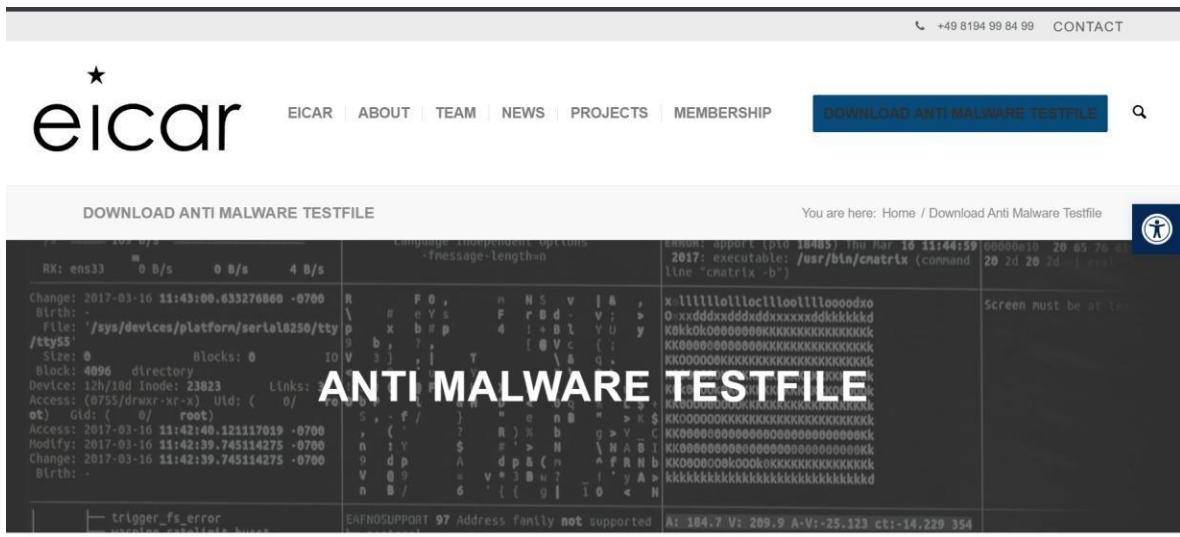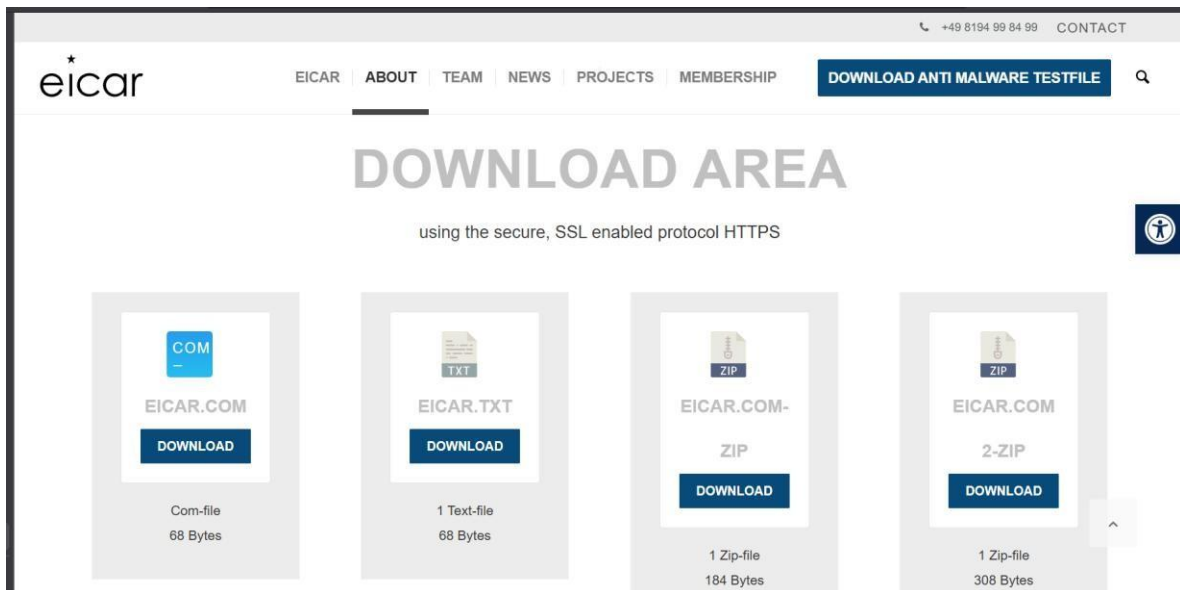# LABORATORIO 10


# CIBERSEGURIDAD
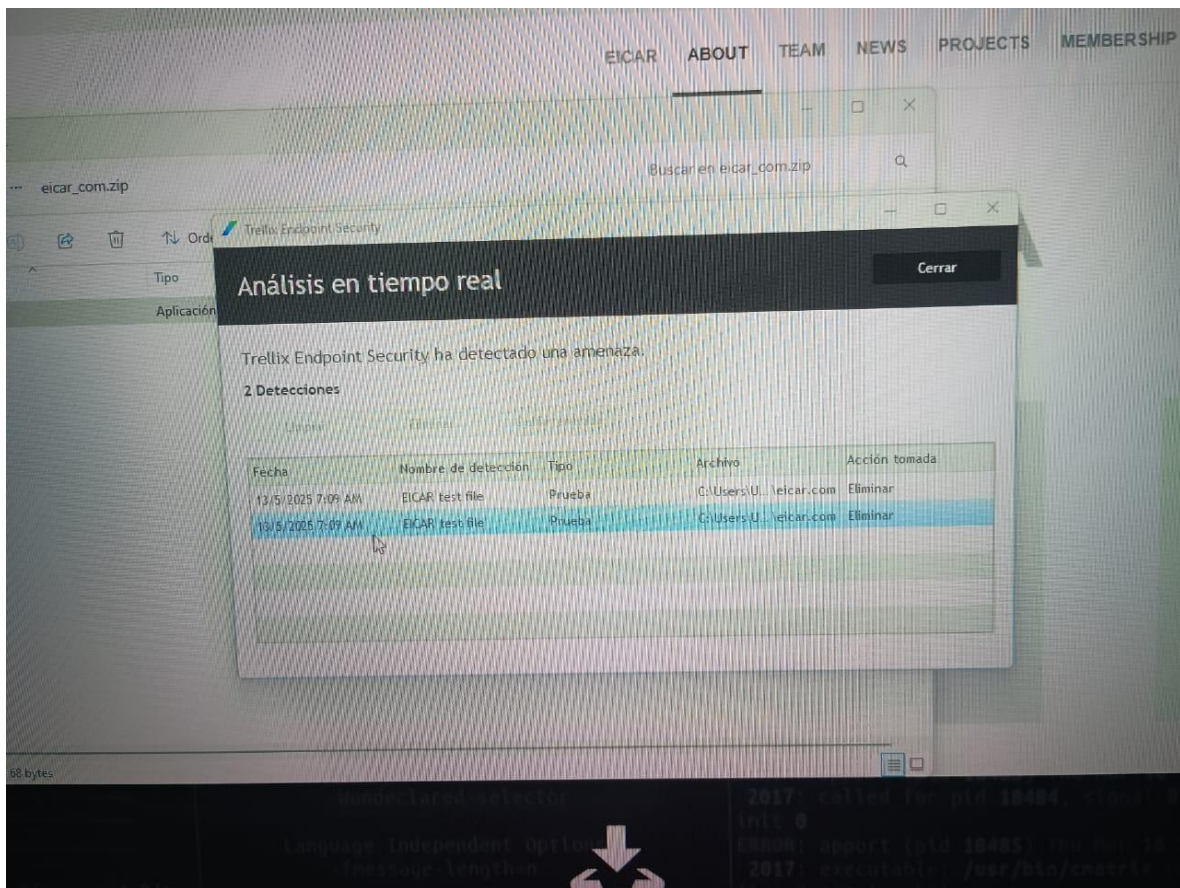

# FABIAN ANDRES BENJUMEA


# UNIVERSIDAD POPULAR DEL CESAR
# VALLEDUPAR
# 2025

**Descargamos el "eicar.com.zip"**

# Despues de descomprimirlo descargamos VirusTotal y vemos como lo reconoce:

# Vemos como escanea y nos muestra todas las amenazas que nos trae lo descargado

## Basic properties ⓘ

| | |
|---|---|
| MD5 | e4968ef99266df7c9a1f0637d2389dab |
| SHA-1 | bec1b52d350d721c7e22a6d4bb0a92909893a3ae |
| SHA-256 | e1105070ba828007508566e28a2b8d4c65d192e9eaf3b7866382b7cae747b397 |
| Vhash | 9e43b16498374c2c95504aaceb63eeab |
| SSDEEP | 6:59QykoBveYMTpDAJuOgzskozj9sY//zpW+llt9xvQ1loBLI+IE/iS/BGpfAdkz9sQcaY9xvwBBRaE/ |
| TLSH | T182E05B052D6F5415D00B003935BD4EE7363C52D95C555F54D68C70B04C574CE1EDBB5C |
| 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 | 308 B (308 bytes) |

## History ⓘ

| | |
|---|---|
| First Seen In The Wild | 2011-04-11 07:49:38 UTC |
| First Submission | 2006-05-23 07:42:50 UTC |
| Last Submission | 2025-05-12 16:43:54 UTC |
| Last Analysis | 2025-05-12 13:31:44 UTC |
| Earliest Contents Modification | 2000-07-11 21:33:36 |
| Latest Contents Modification | 2000-07-11 21:33:36 |

## Names ⓘ

eicarcom2.zip
eicar.zip
eicar2.zip
eicarcom2 (1).zip
ILwCOGhGCKsD.zip
0bGoWcIje12V.zip
eicarcom2(1).zip
eicar-zip2.zip
Niet bevestigd 422619.crdownload
HappyCats.zip

---

e4cc05b192e9ea13b7866382b7cae747b397

## Contacted Domains (1) ⓘ

| Domain | Detections | Created | Registrar |
|---|---|---|---|
| nexus.officeapps.live.com | 0 / 94 | 1994-12-28 | CSC CORPORATE DOMAINS, INC. |

## Contacted IP addresses (5) ⓘ

| IP | Detections | Autonomous System | Country |
|---|---|---|---|
| 142.251.183.94 | 0 / 94 | 15169 | US |
| 52.111.236.24 | 0 / 94 | 8075 | IE |
| 52.111.236.25 | 0 / 94 | 8075 | IE |
| 52.111.243.25 | 0 / 94 | 8075 | NL |
| 52.111.243.26 | 0 / 94 | 8075 | NL |

## Execution Parents (77) ⓘ

| Scanned | Detections | Type | Name |
|---|---|---|---|
| 2024-04-04 | 53 / 65 | ZIP | wwwroot.zip |
| 2022-08-14 | 0 / 59 | Shell script | u.sh |
| 2025-01-22 | 55 / 72 | Win32 EXE | PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* |
| 2024-02-08 | 34 / 58 | ISO Image | Core-current - Copy.iso |
| 2022-08-29 | 31 / 60 | Shell script | extended-diagnostics-v0.9-2-gbab9bec-compact.AppImage |
| 2024-01-03 | 34 / 70 | Win32 EXE | eicar_obfuscated_level3.exe |
| 2024-08-22 | 40 / 60 | ZIP | 0b5bfabd13818438345921b75655884f9ef79a04263ed6d7d51ec8f5e313f529 |
| 2020-11-18 | 13 / 48 | ISO image | home.iso |
| 2023-03-31 | 52 / 63 | ZIP | TD3010_20220429103944_USWFMR_TIME01_DUT8G2l.zip |
| 2023-09-28 | 47 / 72 | Win32 EXE | PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* |

● ● ●

## Bundled Files (1) ⓘ

| Scanned | Detections | File type | Name |
|---|---|---|---|
| ⌄ 2025-05-13 | 61 / 65 | ZIP | eicar_com.zip |