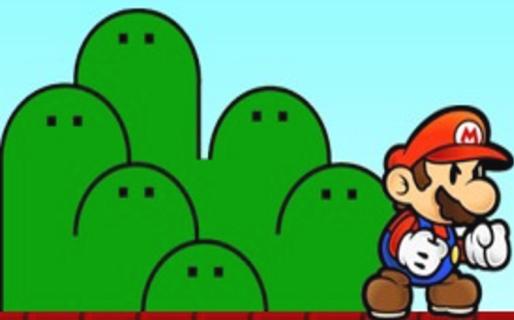




Fishing Phishers

2.0 EVIL EDITION

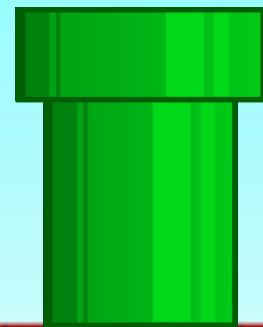


Índice

- Índice
- Disclaimer
- Who are We?
- Phishing
- Got Ya!
 - Análisis de un Phishing Real
 - OSINT
 - Análisis de Malware
 - Esquema
- How do Bad Guys Work?
 - Explicación de nuestra idea del taller y como evoluciono
 - Estructura de los VPS que vamos a utilizar
 - Pasos a Seguir
 - Securización
 - Instalación
 - Despliegue
 - Demo
- Ideas Futuras
- Agradecimientos



WHO ARE WE?



DISCLAIMER

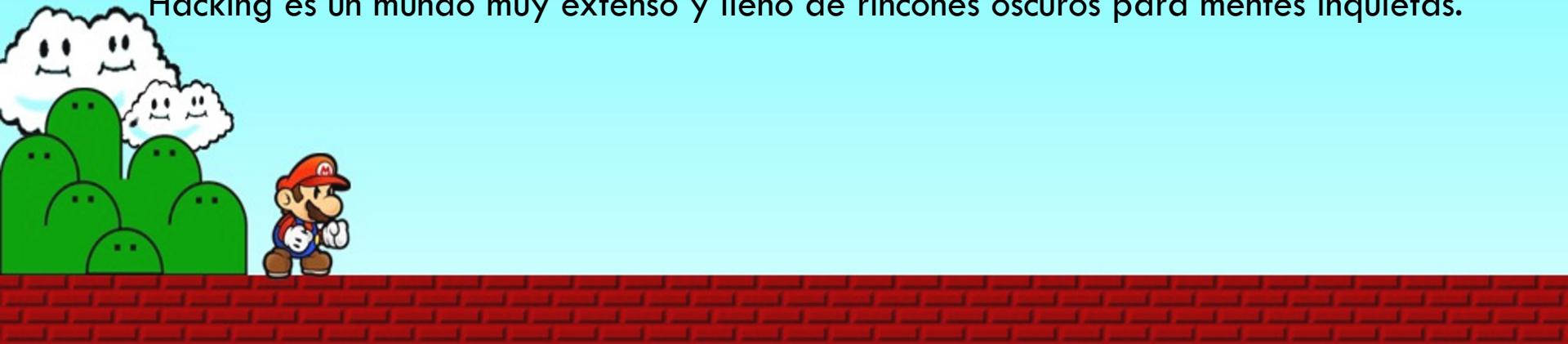
Se que no hace falta decirlo pero por si acaso preferimos curarnos en salud:

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.



Carol12Gory

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

- Pentester / Hacker ético

- Presidenta del congreso de Seguridad :



- Estudiante del Master en Ciberseguridad de la información de la UCLM.

- Actualmente Pentester en :

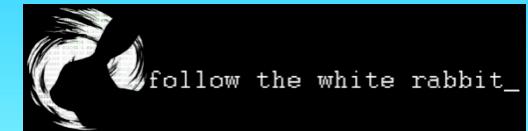
- Ponente en :

Deloitte.



Nebu_73

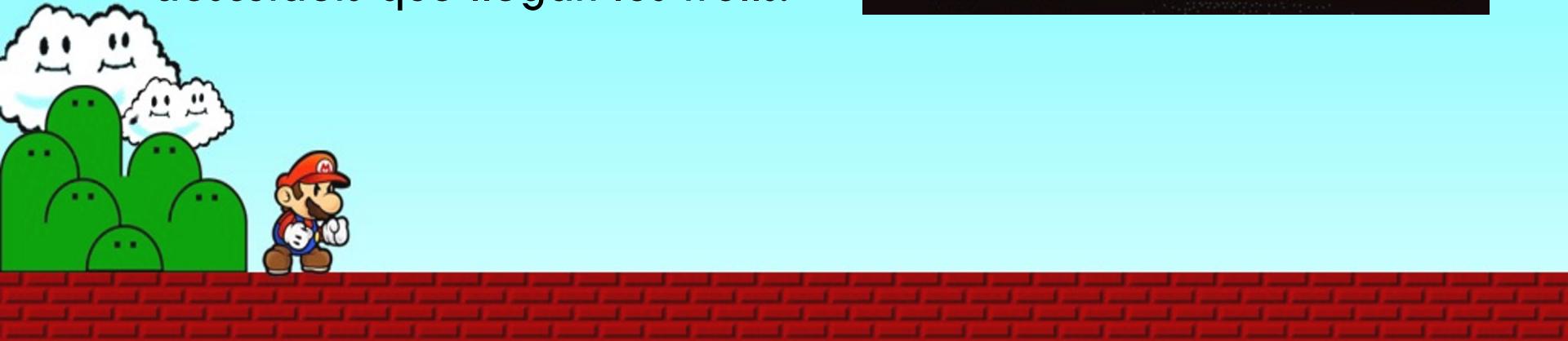
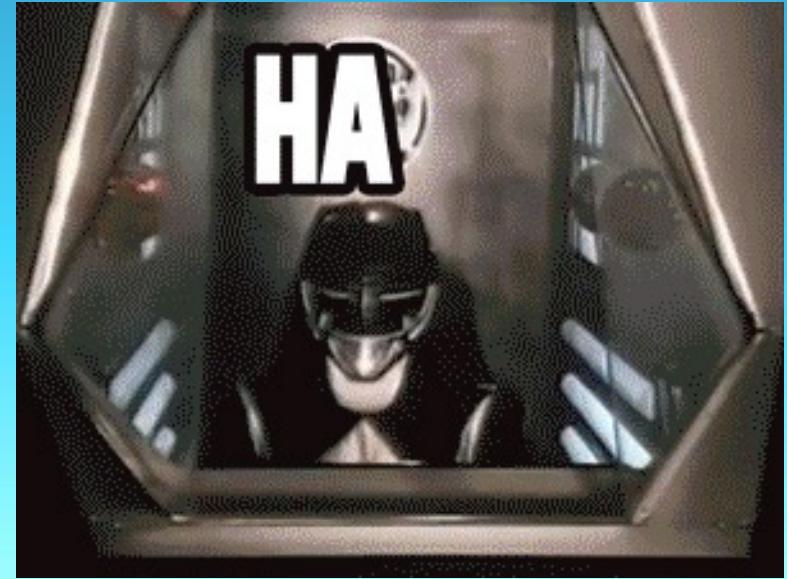
- Username : Alvaro Alonso (A.K.A. - Nebu73)
- Twitter/Telegram : @Nebu_73
- Pentester / Hacker etico
- Cibercooperante de Incibe (I4SK)
- Master en Ciberseguridad - Cybersoc de Deloitte
- Experto en Seguridad de la Información - UCLM
- Certified Ethical Hacker - EC Council
- OSWP - Offensive Security Wireless Professional
- Administrador y escritor del blog de seguridad Informática - [follow the white rabbit_](#)
- 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.



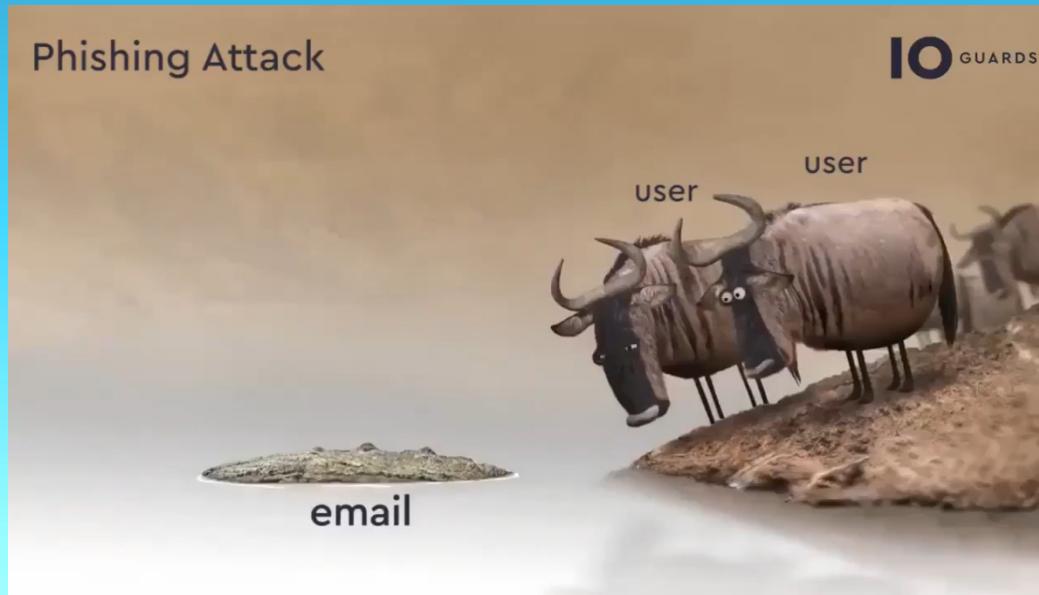
Phishing

¿Eso se come?



¿Qué es el Phishing?

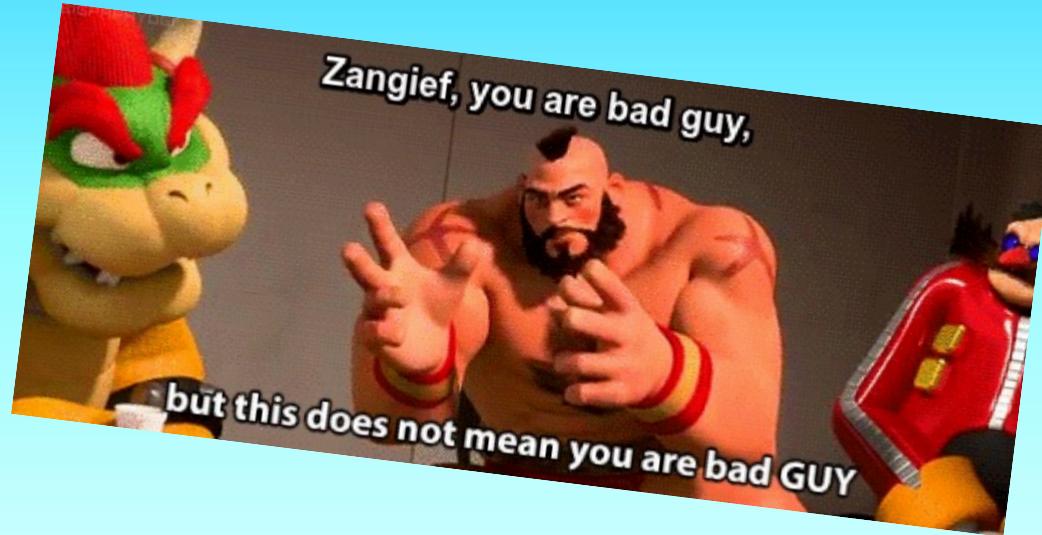
- Por ilustrar que es el phishing antes de una explicación mas técnica:



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.

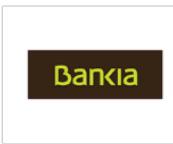
What's going on?

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,

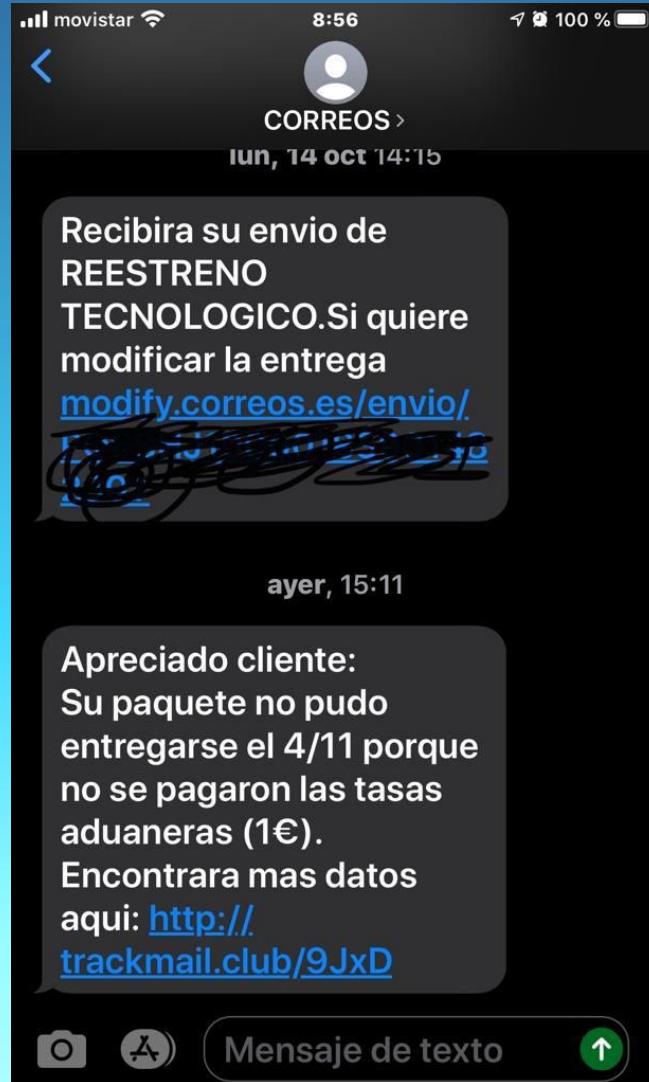
Este mensaje es para informarle que su cuenta bancaria ha sido sujeta a una ejecución debido a una violación de los acuerdos de Bankia.
Esta violación fue señalada a la atención del Equipo de Políticas y Acuerdos de Bankia.
Le rogamos a usted que revise y Confirme los detalles de su cuenta lo antes posible para evitar la suspensión inmediata.
—> [Consulta el Espacio de su Cuenta](#)

Sinceramente

Gracias por usar Bankia



• Correos



• Amazon

RE : [Monthly Statement Added] Alert: An order was issued for Your Amazon account on Friday, November 08, 2019
29484127 [FWD]

C

customer-service@amazon.com <earesrvcseahe-18139@spajalah.org

>

Vie 08/11/2019 18:18

user@domain.com

↶ ↷ → ...



Customer Support

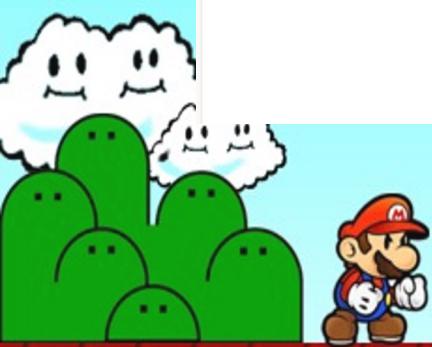
Hello Dear Customer,

We have faced some problems with your account, So Please update your account details. If you do not update your account within 24 hours (from opening this email) will be officially permanently disabled.

Update Now

We hope to see you again soon.

Amazon.com



¿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.



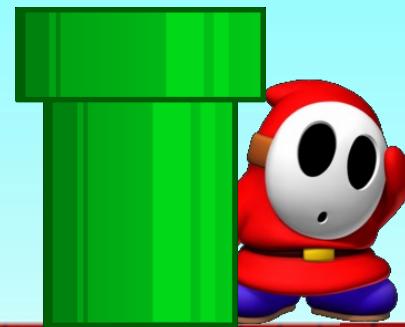


Got Ya!



OSINT

O cómo se más 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



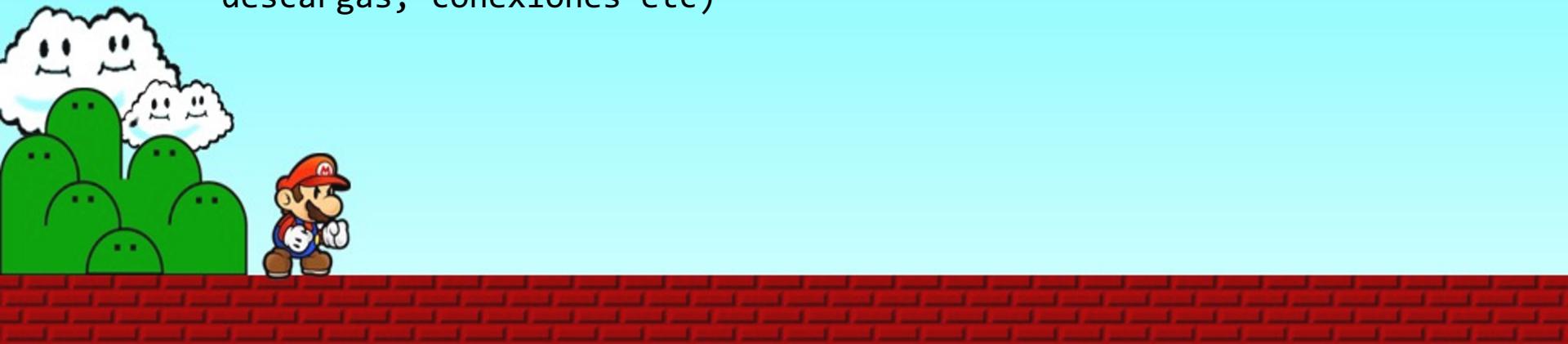
Análisis de Malware

Bitxito Dissection

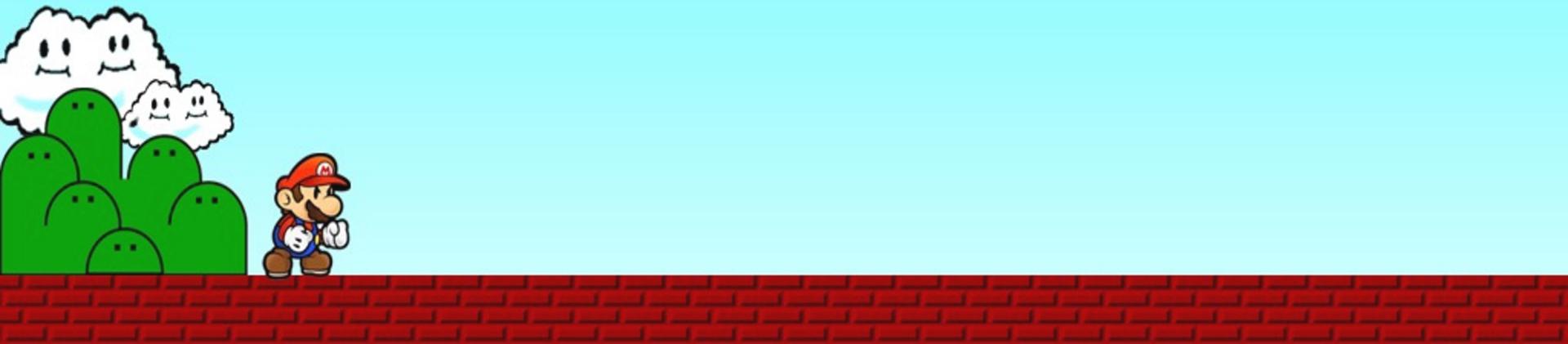


Herramientas Básicas

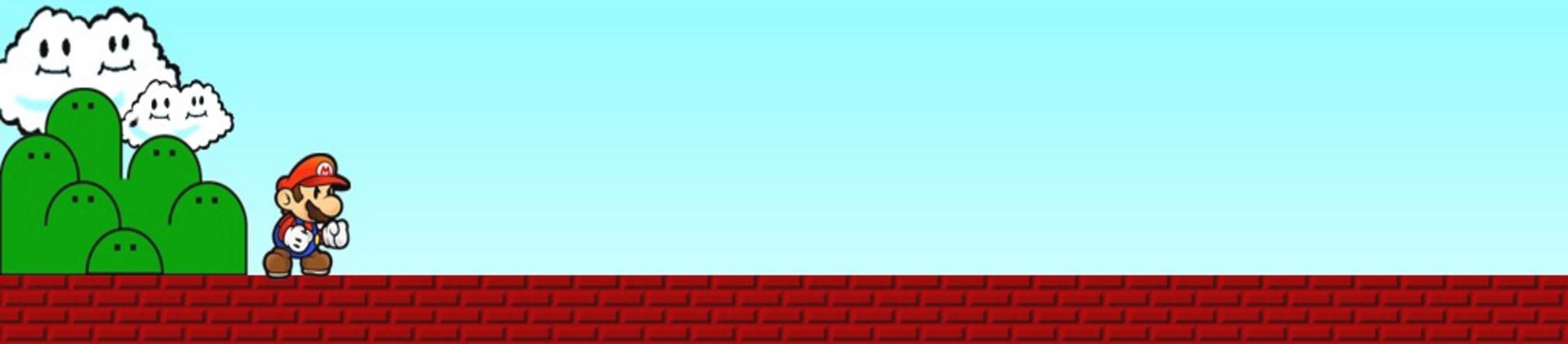
- Analizadores online
 - <https://www.virustotal.com>
 - <https://www.hybrid-analysis.com>
 - Para analizar cualquier muestra con sospecha de malware
- Analizador Dinámico ONLINE
 - <https://any.run/>
 - Permite analizar y ejecutar una muestra en una maquina en la nube, viendo lo que ocurre tras su ejecución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



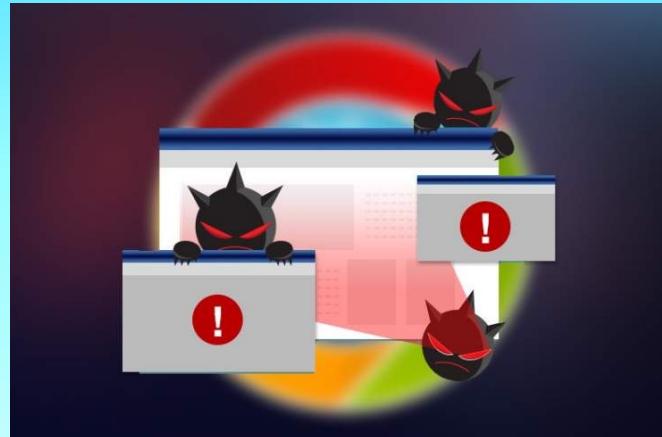
- Calculadora de Hashes:
 - <https://www.slavasoft.com/hashcalc/>
- Strings
 - <https://docs.microsoft.com/en-us/sysinternals/downloads/strings>
 - Sirve para poder sacar los datos de un Ejecutable que no han sido Ofuscados tales como IPS, comandos o Dlls a los que hace referencia.
- PEiD
 - <https://www.aldeid.com/wiki/PEiD>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



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/10.0.14292.0;
```

Cerrar

- Utilizamos herramientas para el análisis de cabeceras y reputación:

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

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

<https://www.kitterman.com/spf/validate.html>

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

Caja de herramientas de G Suite Messageheader

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

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

MX TOOLBOX

Upgrade Delivery Center

Home MX Lookup Blacklists Diagnostics Domain Health Analyze Headers Free Monitoring DMA

Email Header Analyzer

Paste Header:

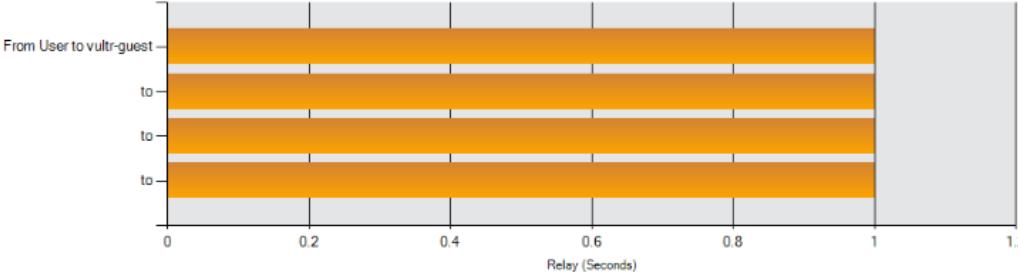
```
Received: from SN1NAM04HT121.eop-NAM04.prod.protection.outlook.com (2603:10a6:6:16::24) by DB6PR0801MB1414.eurprd08.prod.outlook.com with HTTPS via DB6PR07CA0131.EURPRD07.PROD.OUTLOOK.COM; Thu, 31 May 2018 15:57:23 +0000 Received: from SN1NAM04FT021.eop-NAM04.prod.protection.outlook.com (10.152.88.55) 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

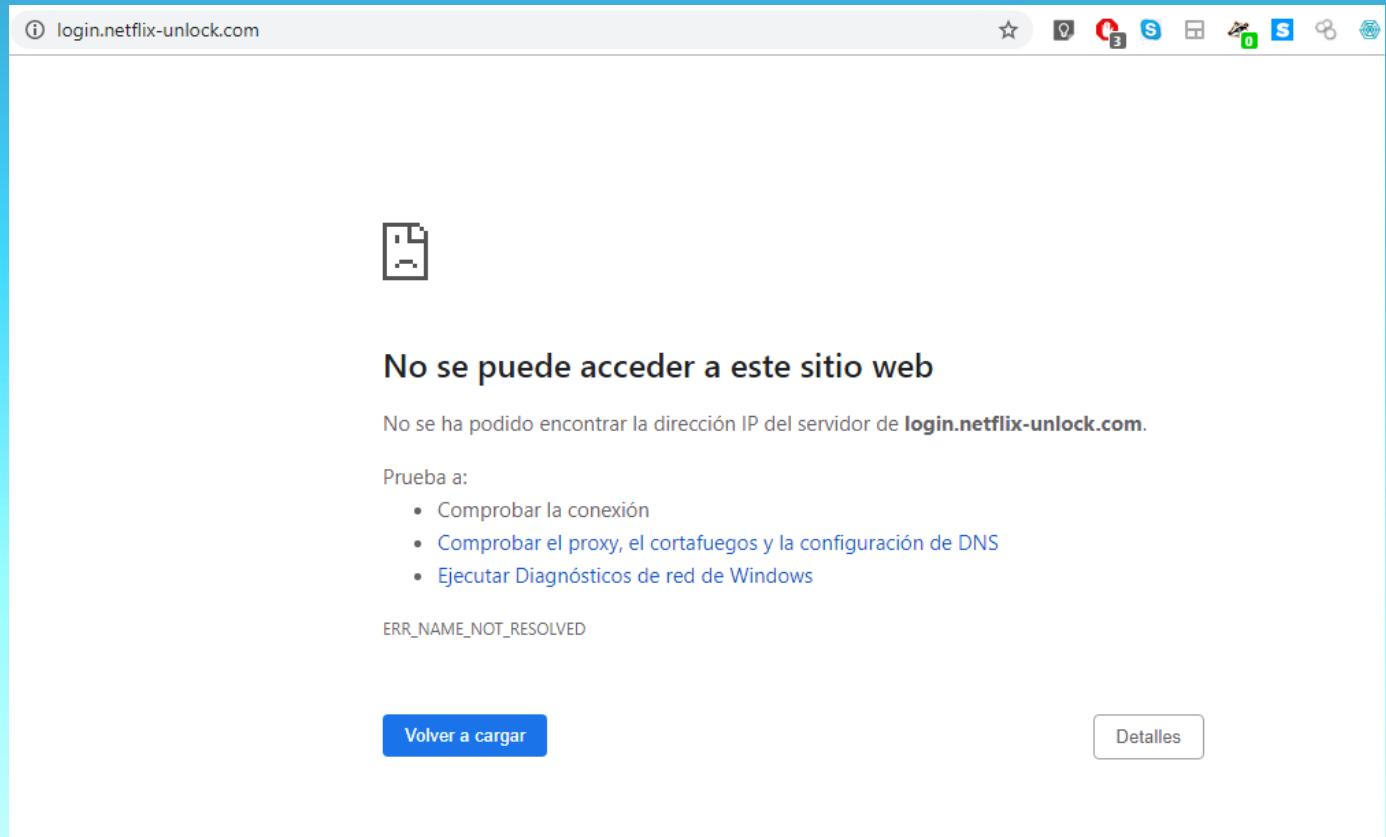
Received Delay:	0 seconds																																			
																																				
<table border="1"> <thead> <tr> <th>Hop</th><th>Delay</th><th>From</th><th>By</th><th>With</th><th>Time (UTC)</th><th>Blacklist</th></tr> </thead> <tbody> <tr> <td>1</td><td>*</td><td>User 95.179.134.243</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

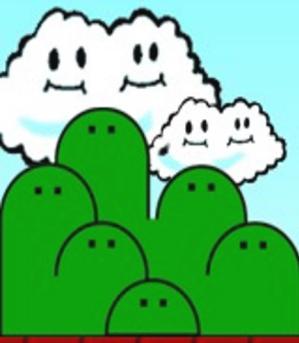
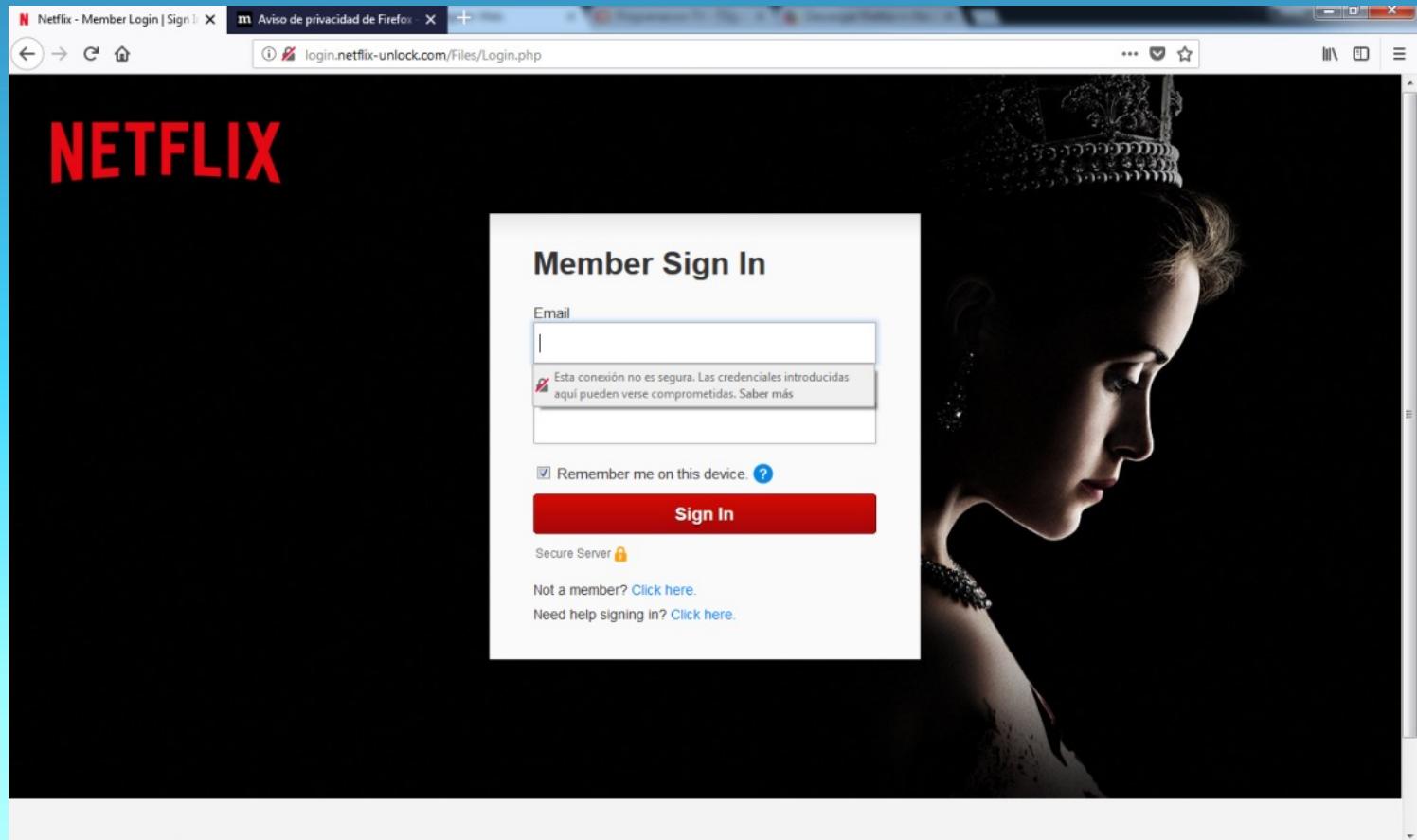


IPS	Dominios	Usuarios
95.179.134.243	vultr-guest	User
45.76.183.37	login.netflix-unlock.com	

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



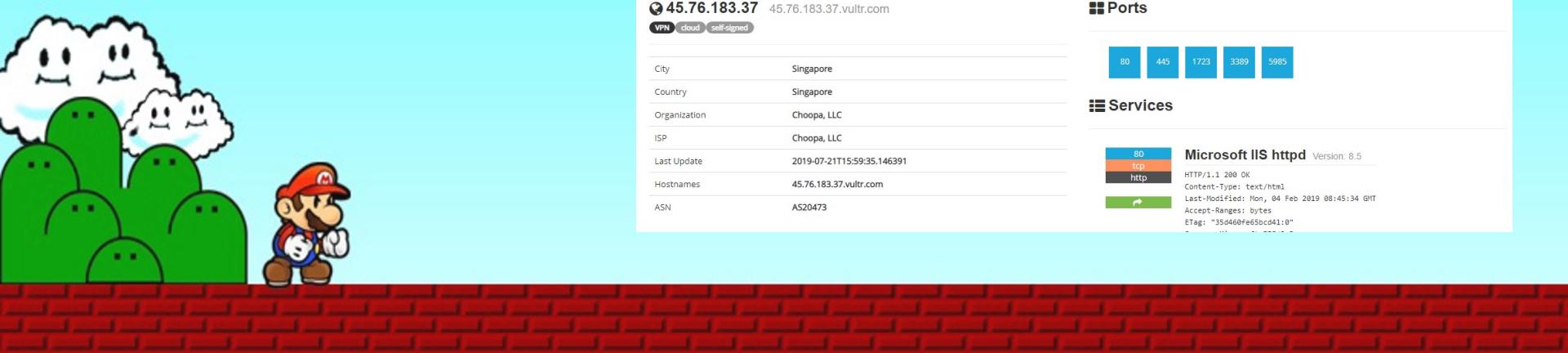
- Por suerte tenemos capturas de lo que suponía esta pagina:



- 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)

Remote Desktop Protocol
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:

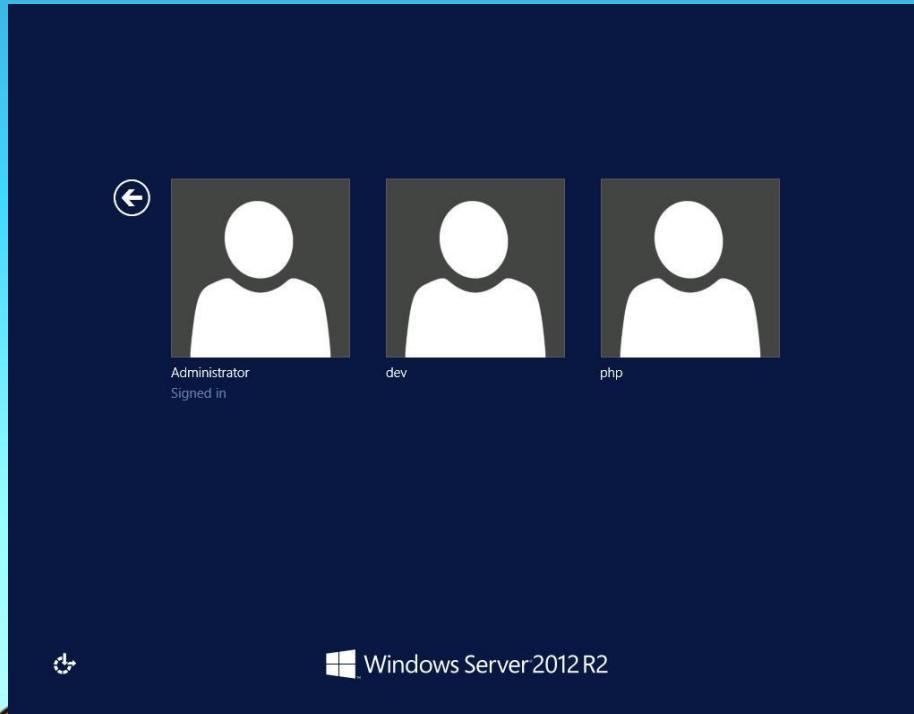
- 80 (tcp, http)

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

573081 IOC

388859 Total time

CHANGE LOG

May TODAY WE ARE READY TO RELEASE OUR API!

RECENTLY

Revenge-RAT v0.5.exe

2193

No threats

Trendin

at

303 times

152 times

14

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>

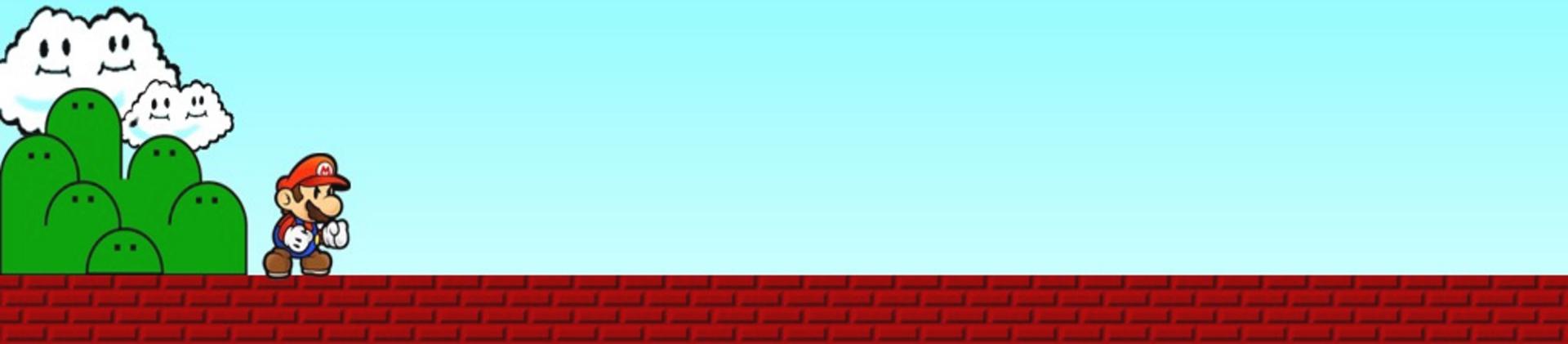
<https://app.any.run/tasks/b0e9bf3c-47b8-45a1-b5d8-b595818b1563/>



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

<https://vk.cc/9zwchq>

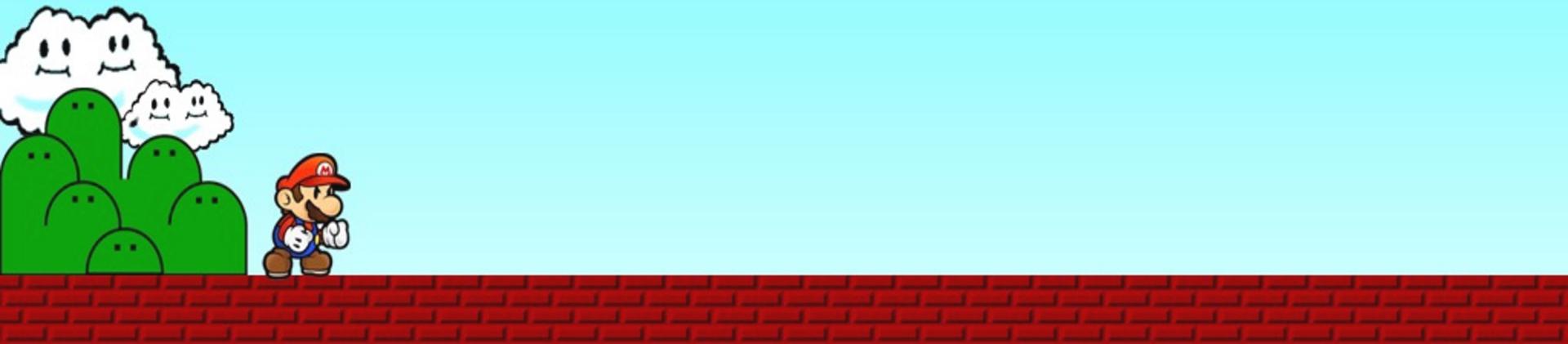
- Y así podríamos continuar hasta llegar al punto en el que demos con servidores

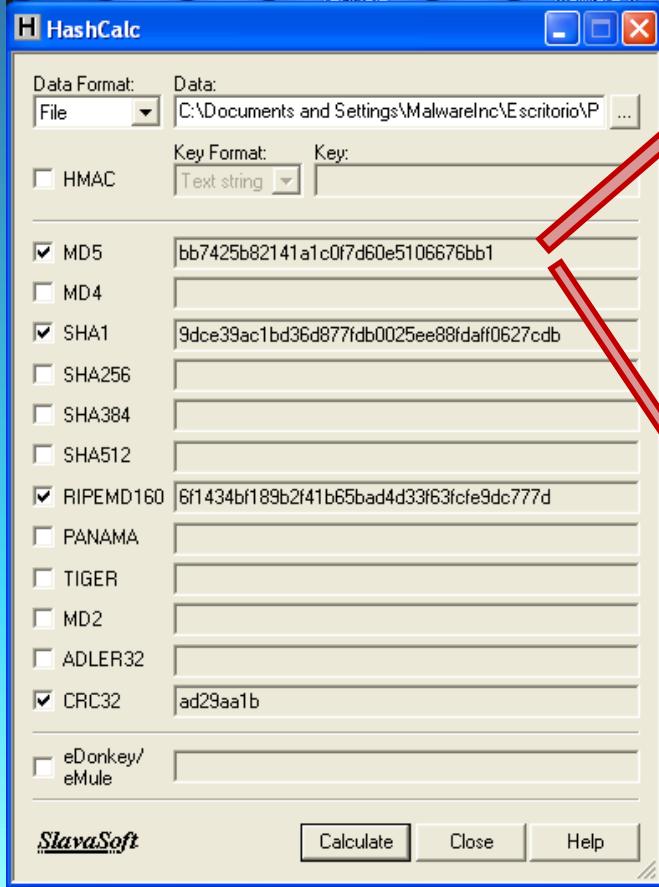


Caso 3: Es un binario

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



The screenshot shows the VirusTotal analysis results for the file 'Lab01-01.exe'. At the top, it says '40 engines detected this file'. Below is a table of detection results:

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

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

The screenshot shows the Hybrid Analysis tool interface. At the top, it says 'HYBRID ANALYSIS' and 'Analysis Overview'. Below is a summary of the submission:

- 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

On the right, there is a 'malicious' label with threat score 82/100, AV detection 53%, and a link to '#mhu'. Below are sections for 'Anti-Virus Results' and three vendor reports:

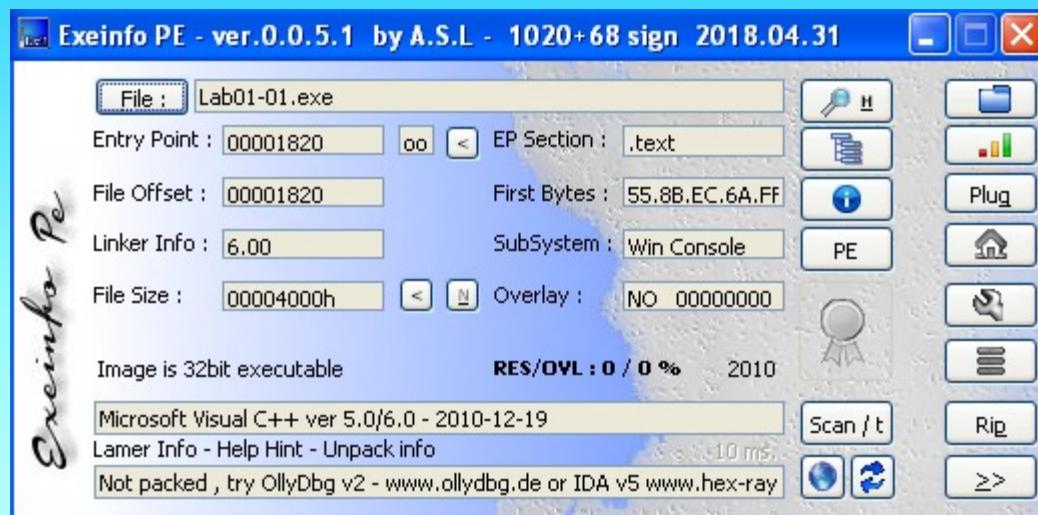
- CrowdStrike Falcon**: N/A
- MetaDefender**: 58% Multi Scan Analysis
- VirusTotal**: 57% Multi Scan Analysis

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

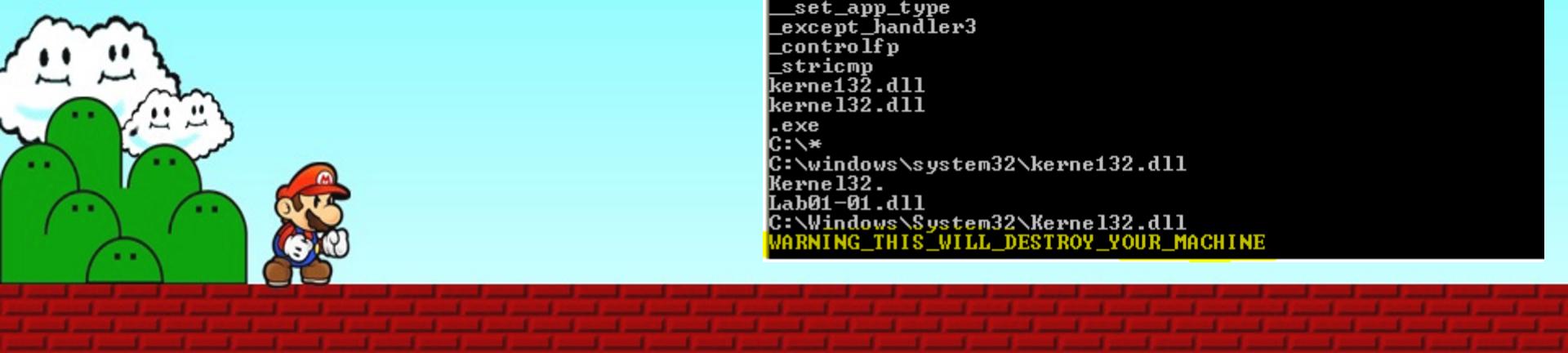
<https://www.hybrid-analysis.com/sample/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/>

- 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



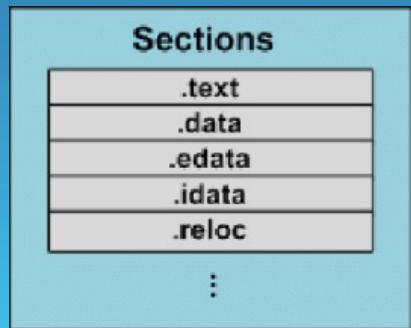
- Extraemos los Strings interesantes del binario
 - Ips
 - URLs
 - Cadenas de texto que nos indiquen comentarios del código
 - Apis de Sistema (MSDN Is your new Friend)



```
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



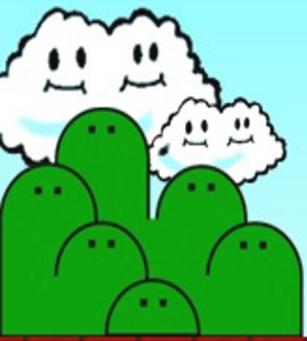
- Tenemos ya un montonazo de llamadas de las apis del sistema (Windows) ahora toca la parte tediosa que es buscarlas una a una y mirar que hace cada una para saber si se trata de algo malicioso o no.

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



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**

How do Bad Guys Work?

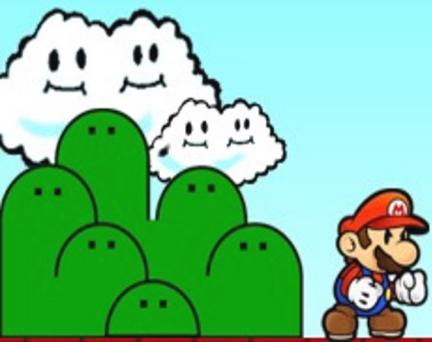


Explicación de nuestra idea del taller

- Bueno todos habéis leído que eran unos scripts, y demás para analizar los correos maliciosos que nos llegan pero... hubo una vocecilla que nos susurro al oído:

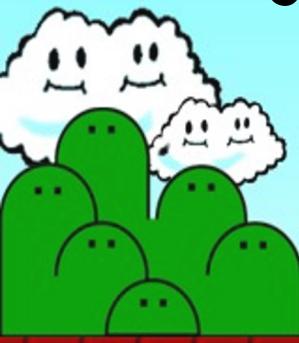
- Y SI APRENDEIS Y DESPUES ENSEÑAIS A HACER COSAS MALAS?

- Y con esa idea nos pusimos manos a la obra.....

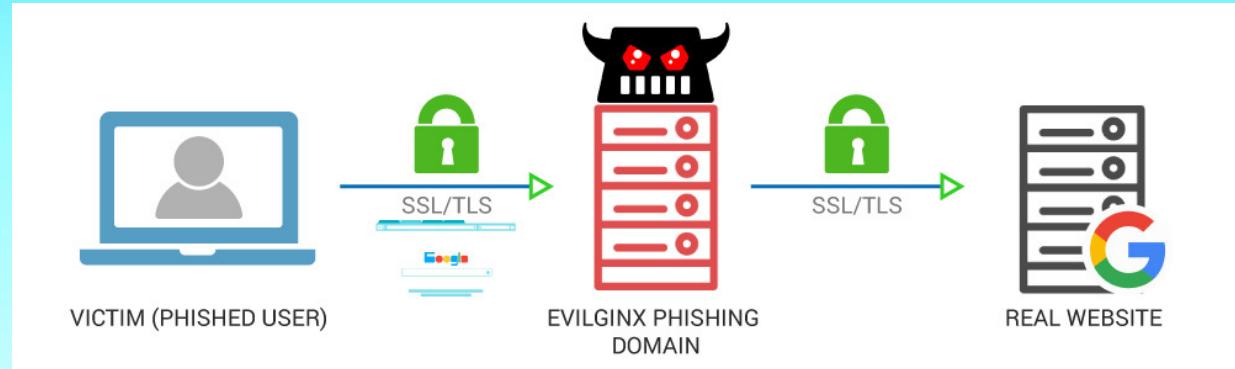


Estructura del laboratorio

- Disponemos de 3 VPS
 - Servidor 1
 - Es nuestro servidor de origen de phishing donde se realizarán las instalaciones y configuraciones de GoPhish y EvilNgix2.
 - Servidor 2
 - En este servidor se realizará el phishing de Facebook.
 - Servidor 3
 - En este servidor se realizará el phishing de Gmail.



- Vamos a utilizar dos herramientas en tandem
 - GOPHISH que nos ayudara en la distribución de correo con fines maliciosos.
 - Evilginx Que nos hará de proxy inverso entre el usuario y la pagina final poniendo de por medio nuestro phishing.



PASOS A SEGUIR



Cherry Tree =>



Fishing Phishers (Fishing Phishers.ctb)

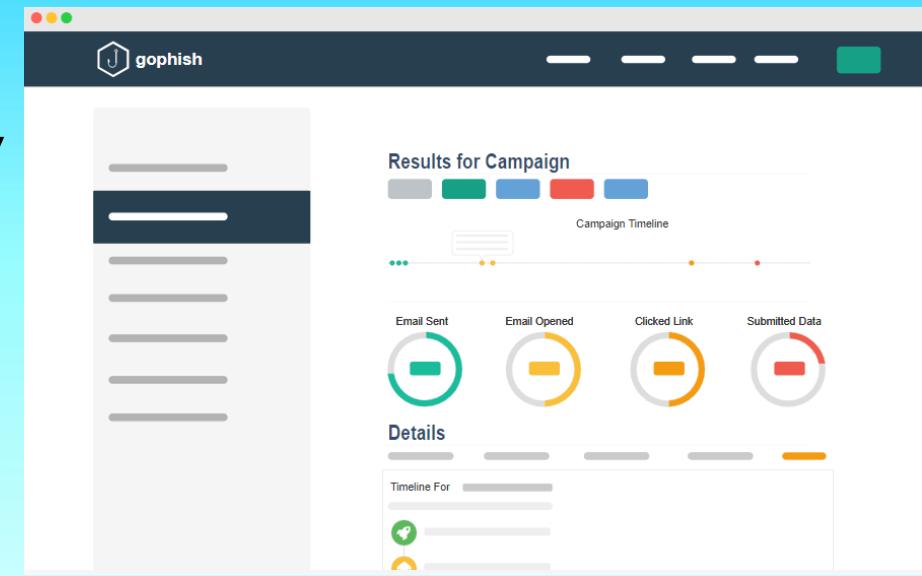


- Como copiar esto a mano es un coñazo y sabemos a todos nos puede la pereza, nos habría gustado proporcionaros un bash que hiciera todo pero por falta de tiempo no esta completo así que os dejamos un cherry tree estructurado para que podáis seguirlo paso a paso.

GOPHISH

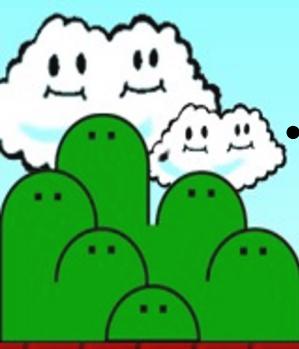
Gophish es un kit de herramientas de phishing de código abierto, potente y fácil de usar, destinado a ayudar a los pentesters y a las empresas a realizar simulaciones de phishing en el mundo real.

<https://getgophish.com/>

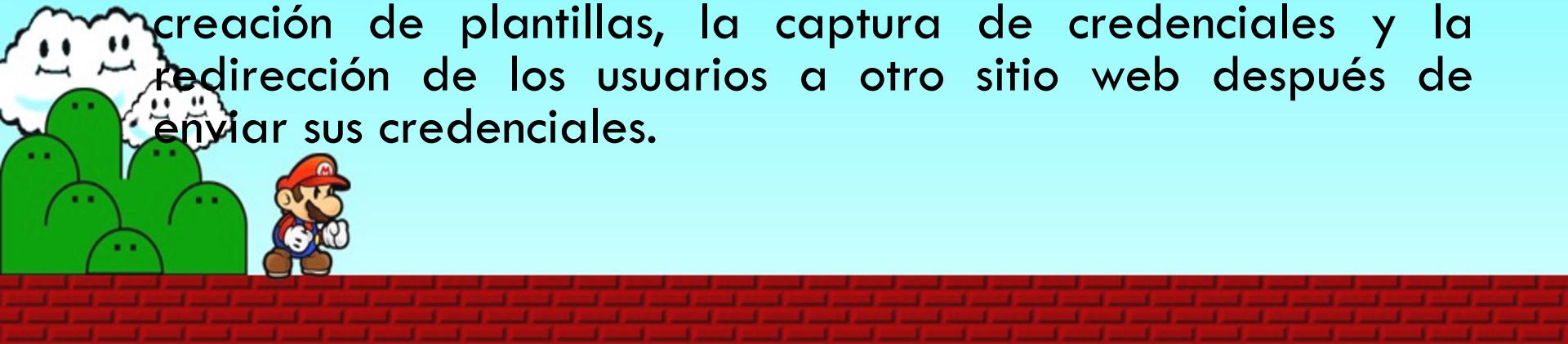


CARACTERISTICAS

- **Instalación con un solo clic:** Gophish puede instalarse con una sola descarga.
- **API completa de REST:** Gophish está alimentado por API REST. Un cliente Python hace que trabajar con la API sea muy sencillo.
- **Interfaz web:** Gophish tiene una interfaz web intuitiva. Importe sitios web y correos electrónicos existentes, habilite el seguimiento de correos electrónicos abiertos y mucho más con un solo clic.
- **Multiplataforma:** Los binarios Gophish se proporcionan para la mayoría de las plataformas, incluyendo Windows, Mac OSX y Linux.
- **Resultados en tiempo real:** Gophish actualiza los resultados automáticamente. Mediante la interfaz de usuario, puede ver una línea de tiempo para cada destinatario, el seguimiento de la apertura del correo electrónico, los clics de los enlaces, las credenciales enviadas y mucho más.
- **Funciona solo“:** Fácil de usar.



- **Archivo “config.json”**: Se configura la IP y puerto en la que nos conectaremos a GoPhish, se configuran los certificados y la base de datos donde se almacenarán los datos que introduciremos en GoPhish y los resultados de este.
- **Sending Profiles**: Para el envío de correo es necesario la configuración del SMTP relay.
- **Landing Pages**: son las páginas HTML reales que se devuelven a los usuarios cuando hacen clic en los vínculos de phishing que reciben. Las páginas de destino soportan la creación de plantillas, la captura de credenciales y la redirección de los usuarios a otro sitio web después de enviar sus credenciales.



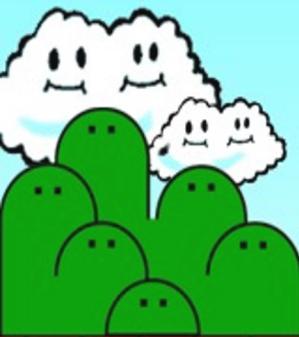
- **Email Templates:** es el contenido de los correos electrónicos que se envía a los destinatarios. Pueden importarse desde un correo electrónico existente o crearse desde cero. También admiten el envío de archivos adjuntos. Además, las plantillas pueden contener imágenes de seguimiento para que Gophish sepa cuando el usuario abre el correo electrónico.
- **Users & Groups:** Se crean los usuarios donde vamos a mandar la campaña de phishing. Se puede crear usuarios uno a uno o mediante un .csv
- **Campaigns:** se trata del envío de mensajes de correo electrónico a uno o más grupos y la supervisión de los mensajes de correo electrónico abiertos, los enlaces en los que se hace clic o las credenciales enviadas.

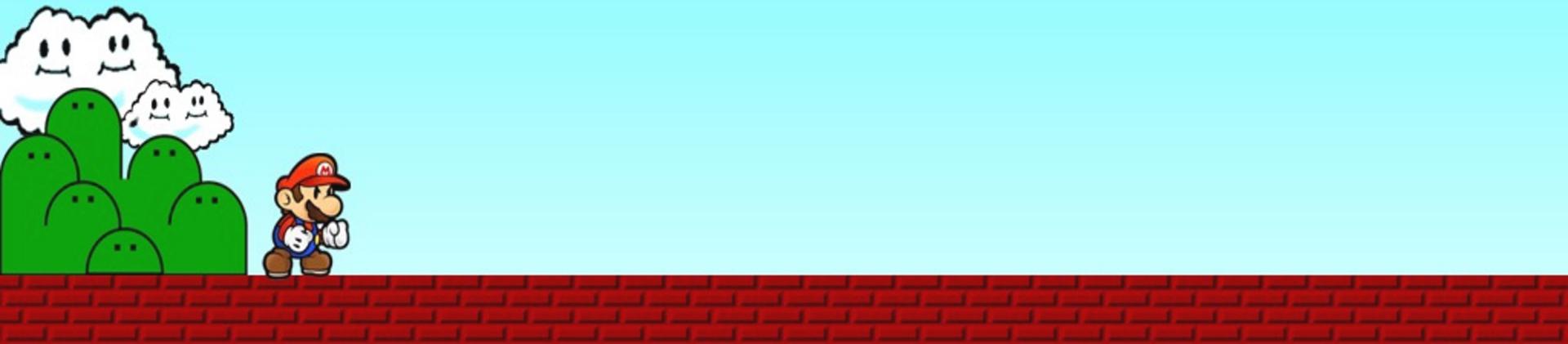
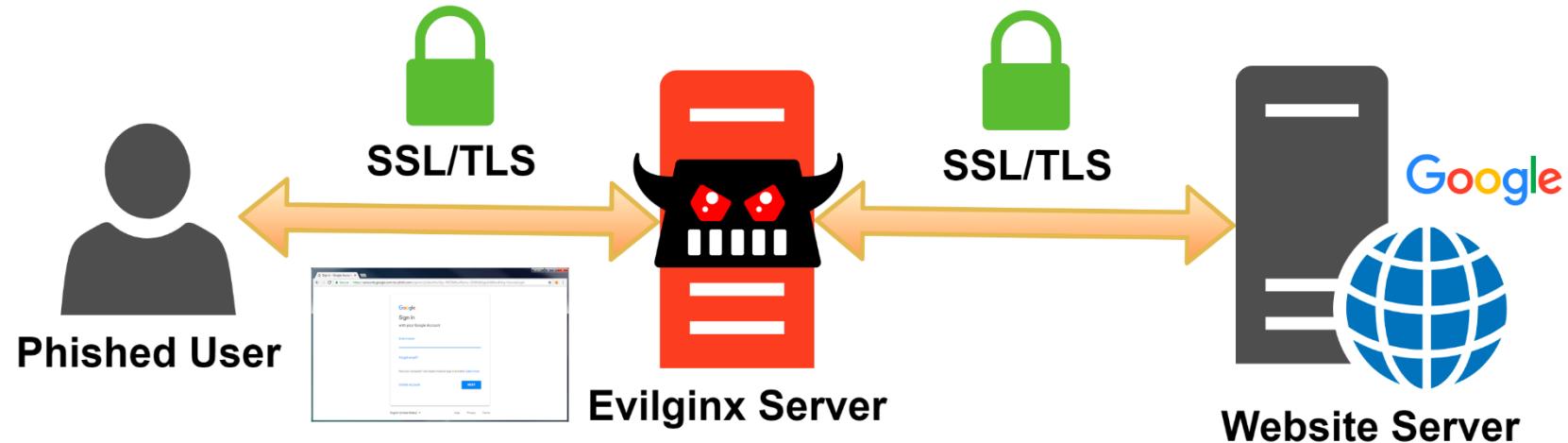


EVILGINX2

Evilginx2 es un framework ofensivo que utiliza el ataque man-in-the-middle para obtener credenciales de inicio de sesión junto con las cookies de sesión, lo cual permite eludir el segundo factor de autenticación.

Envilginx2 es la sucesora de Evilgnix desarrollada en GO donde implementa su propio servidor HTTP y DNS, lo cual facilita tanto la configuración como el uso.





Referencias

- <https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/>
- <https://docs.getgophish.com/user-guide/>
- <https://tecnonucleous.com/2018/02/19/que-es-gophish-como-instalarlo-en-ubuntu-con-ssl/>
- <https://github.com/gophish/gophish>
- <https://github.com/kgretzky/evilginx2>
- <https://kifarunix.com/install-gophish-on-ubuntu-18-04-debian-9-8/>
- <https://certbot.eff.org/lets-encrypt/ubuntubionic-apache.html>
- <https://ninja.style/post/deploygophish/>
- <https://raiolanetworks.es/blog/registro-spf/>

