

Hispasec]



DOCUMENTACIÓN

Writeup UAM

OSINT
Enero 2024

Informe técnico

Cláusula legal

La información contenida en este documento es de carácter confidencial y va dirigida de manera exclusiva a su destinatario, quedando sujeta al secreto profesional. Queda prohibida por Ley la distribución, divulgación, copia o reproducción del contenido de este documento sin la correspondiente autorización por parte de su autor.

Documentación

Informe técnico

Índice

1. Datos del reto.	3
1.1. Especificaciones técnicas.	3
2. Proceso de resolución del reto.	4
2.1. Encontrar la plataforma de retos	4
2.1.1. Búsqueda del usuario	4
2.1.2. Búsqueda de información en Twitter (X)	6
2.2. Flags	9
2.2.1. Revisión de metadatos en ficheros	9
2.2.2. Búsqueda de información sobre el nuevo usuario	12

1. Datos del reto.

1.1. Especificaciones técnicas.

A continuación se detalla el alcance y el conjunto de especificaciones del reto, así como las normativas de aplicación.

Alcance	
Activo/s:	OSINT
Categoría:	OSINT
Fecha de inicio:	26/01/2024.
Cumplimiento normativo:	Las contraseñas y otra información sobre los usuarios no son almacenadas en cumplimiento con la ley de protección de datos (Reglamento General de Protección de Datos, RGPD). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Proceso de resolución del reto.

A continuación se detalla la manera intencionada en la que se espera que el usuario resuelva el reto. Cada entrada viene encabezada por la descripción detallada del punto en concreto, acompañado de los pasos a seguir para reproducirlo.

2.1. Encontrar la plataforma de retos

El primer paso es encontrar y registrarse en la web de la UAM que contiene la plataforma de retos.

2.1.1. Búsqueda del usuario

Resolución

A continuación, se puede visualizar una captura de pantalla del blog de la [UAD](#) donde, revisando el código fuente o simplemente subrayando el texto (en una zona donde se ve que hay más hueco de lo normal) se hace referencia a un nombre de usuario y de que este usuario ha comenzado su actividad maliciosa en redes sociales:

- **Dos categorías:** una para personas con conocimientos (nivel avanzado) y otras para quienes se estén iniciando (nivel principiante). Los retos son los mismos en ambos casos.
- **Cantidad de retos:** doce, uno para cada mes del año 2024. Quienes participen seguirán una historia, juegos y pistas por temáticas.
- **Retos acompañados de documentación:** una vez llegue la fecha en la que se dé por terminado el reto, se subirá al [GitHub de UAM](#) un documento *writeup* con la resolución intencionada.

Como ya avisamos, a partir de ahora los retos seguirán una línea temporal con una historia que enlazará cada uno de los retos. En esta historia incluiremos a nuestros usuarios de manera que asuman el rol de un investigador que colaborará en el proceso de busca y captura de un reconocido cibercriminal: **3sp1n3t3**.

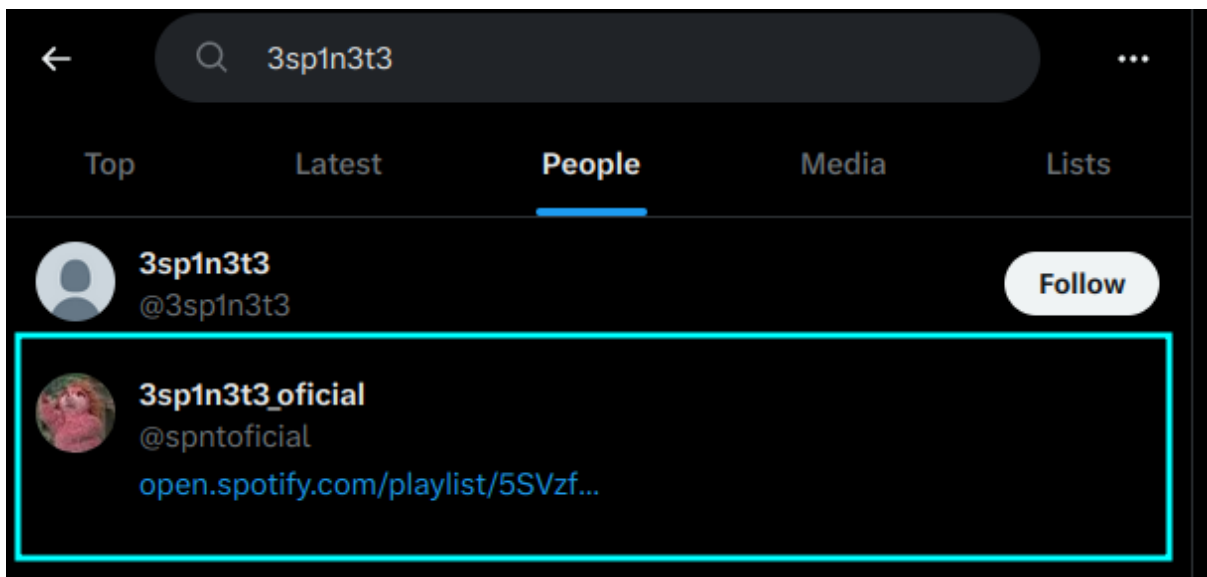
Hemos detectado que 3sp1n3t3 ya ha comenzado con su actividad maliciosa en algunas redes sociales, ¿puedes ayudarnos a encontrar dónde?

Campaña Capture The Famous Bandit!

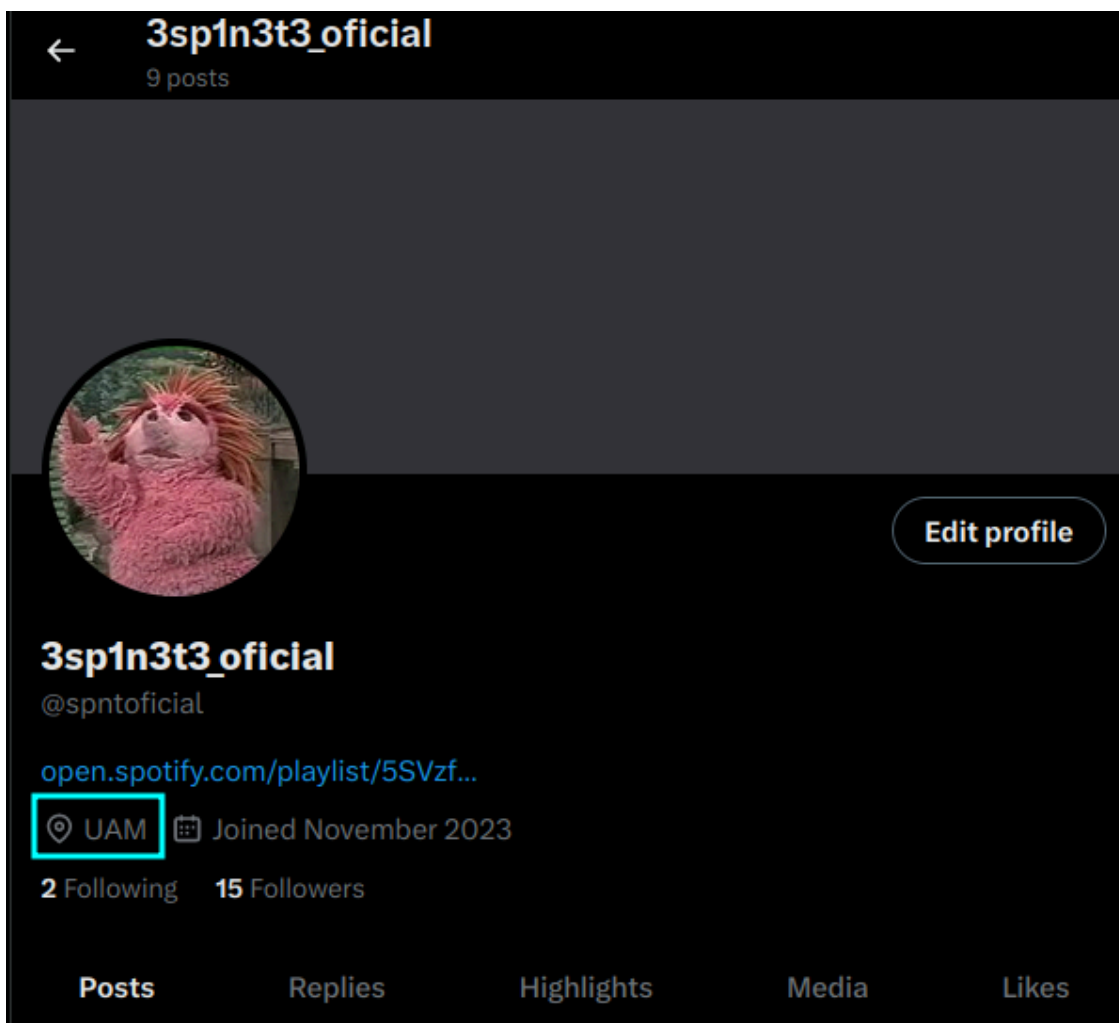
Hispacec lanza **Capture The Famous Bandit! #CTFBandit**, una serie de 12 retos de ciberseguridad donde tanto usuarios, profesionales, como más de 1000 alumnos y alumnas de centros educativos, tendrán que ir descubriendo pistas a lo largo de los 12 meses de 2024.

Concienciación y empleabilidad: esta campaña cuenta con la colaboración del Ministerio de Educación, Formación Profesional y Deportes de España y Alianza por la Formación Profesional, con el objetivo de promover estos retos de ciberseguridad entre más de 1000 alumnas y alumnos de los siguientes institutos: C.P.I.F.P. Alan Turing, localizado en Málaga Tech Park, C.D.P. San José, I.E.S. Ciudad Jardín, I.E.S. Gerald Brenan de Alhaurín de la Torre, I.E.S. Los Manantiales de Torremolinos, I.E.S. Romero Esteo de Carretera de Cádiz, I.E.S. Monterroso de Estepona, I.E.S. Juan de la Cierva de Vélez Málaga y el I.E.S. Virgen del Carmen de Jerez, entre otros, a los que se irán sumando otros centros durante el curso.

Al buscar este nombre de usuario en Twitter (x) encontramos los siguientes perfiles:



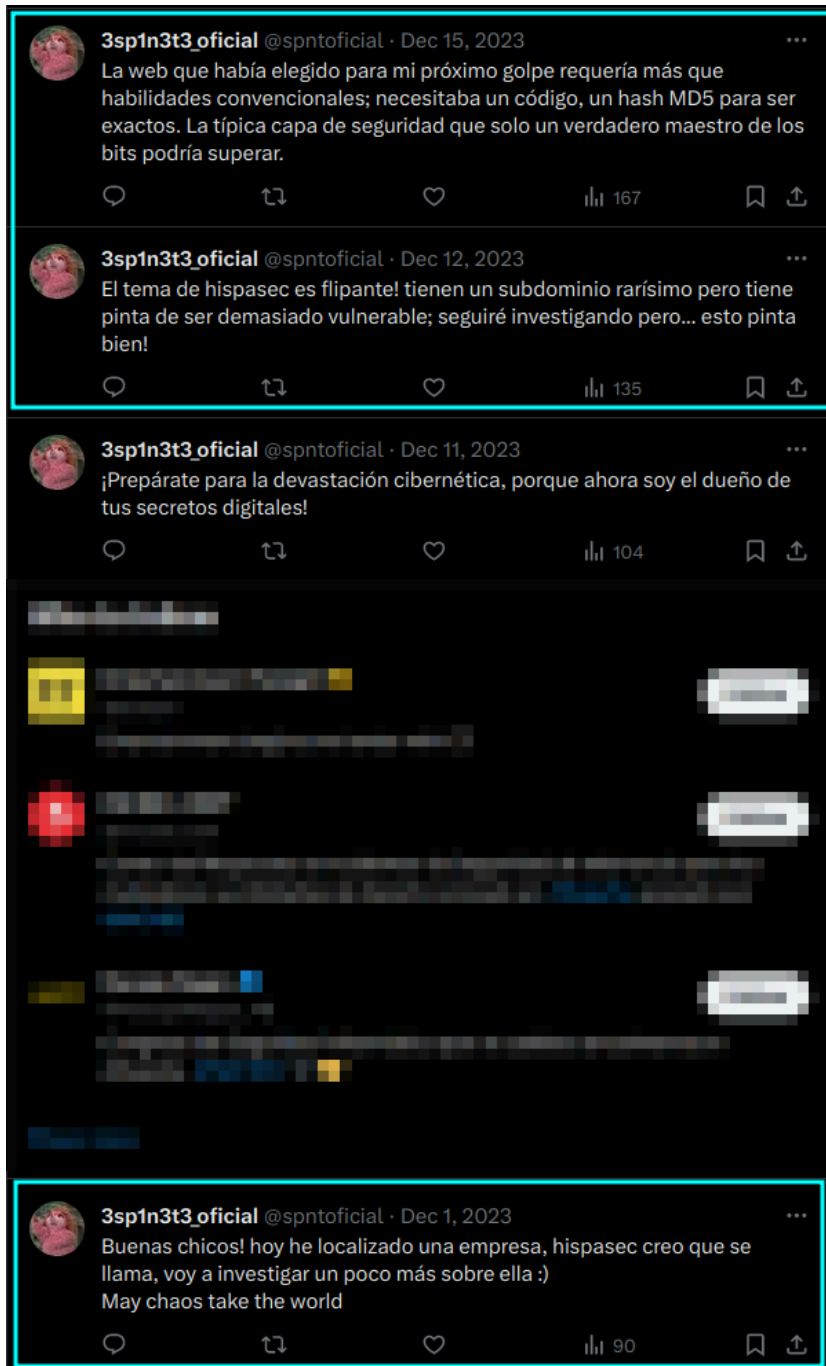
Al entrar en el perfil con foto, se puede ver que se trata del perfil del reto:



2.1.2. Búsqueda de información en Twitter (X)

Resolución

Entre las publicaciones del usuario, hay algunas que llaman mucho la atención:



Si se utiliza la barra de búsqueda de Twitter con el usuario de la cuenta se muestra lo siguiente (también es posible encontrarlo en el mismo perfil de 3sp1n3t3, revisando el apartado “media”):



Se trata de una enumeración de subdominios, al introducir la dirección <https://026d724a98701a407720feac61c59516.hispasec.com/> en la barra de búsqueda encontramos la web que contiene la plataforma de retos:

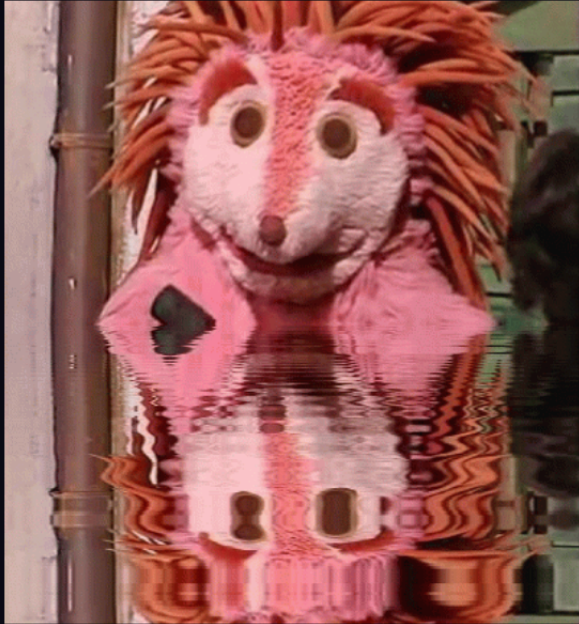
UAM Inicio Usuarios Ranking Retos Notificaciones Registro Inicio de sesión

3SP1N3T3


El juego comienza ahora

Para acceder a mis recursos internos, necesitarás los siguientes objetos:

- Una uña de Espinete
- El balón de Naranjito
- La capa de Súper López



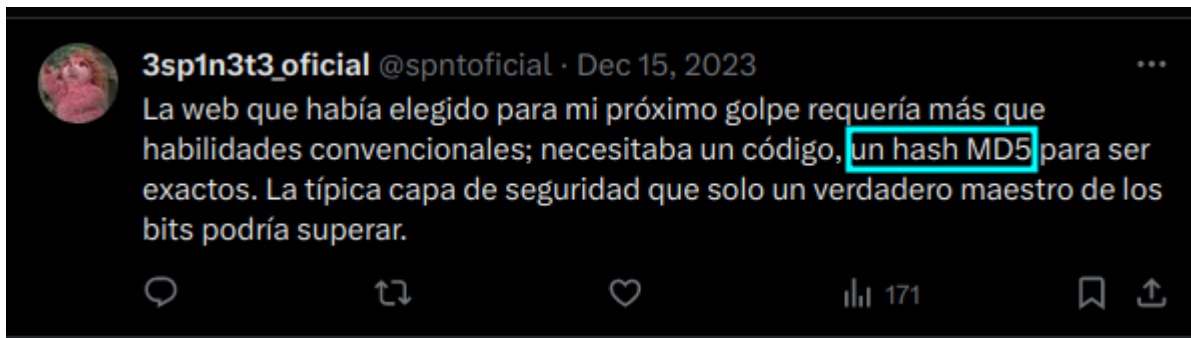
Síguenos en nuestras redes sociales:



2.2. Flags

2.2.1. Revisión de metadatos en ficheros

Al intentar crear una cuenta de usuario en la plataforma se requiere un MD5 al que hace referencia el perfil de Twitter en uno de sus Tweets:



La última publicación es bastante llamativa:



También hay una pequeña pista en el código de la propia web de retos:

```

141     <span class="d-sm-block d-md-none d-lg-block">
142       <i class="fas fa-sign-out-alt pr-1"></i>
143       <span class="d-lg-none">Desconectarse</span>
144     </span>
145   </a>
146
147   </div>
148 </div>
149 </div>
150
151   <main role="main">
152
153   <div class="container">
154     <div class="row" class="row" class="row">
155
156     <div class="col-md-6 offset-md-3" class="col-md-6 offset-md-3" class="col-md-6 offset-md-3">
157       <div style="padding-bottom: 50px;">
158         <h1 class="neonText" class="neonText" class="neonText">3SP1N3T3</h1>
159       </div>
160       <h3><b><u>El juego comienza ahora</u></b></h3>
161       <p>Para acceder a mis recursos internos, necesitarás los siguientes objetos:</p>
162       <ul>
163         <li>Una uña de Espinete</li>
164         <li>El balón de Naranjito</li>
165         <li>La cana de Súper López</li>
166         <!-- Los puntos anteriores no son reales, nunca encontrarán la pista verdadera... jajajaj -->
167         <li>Los de Broderbund saben como realzar mi figura...</li> -->
168       </ul>
169       <img class="w-100 mx-auto d-block" class="w-100 mx-auto d-block" class="w-100 mx-auto d-block"
170       <h3 class="text-center" class="text-center" class="text-center">
171         <p>Síguenos en nuestras redes sociales:</p>
172
173         <a href="https://x.com/unaaldia" target="_blank" rel="nofollow noreferrer noopener"><i cl
174         <a href="https://github.com/Auditoria-hispasec/UAM" target="_blank" rel="nofollow norefer
175         <a href="https://hispasec.com/" target="_blank" rel="nofollow noreferrer noopener"><i cla
176         <a href="https://t.me/+EuWbNB8zZkQyYmZk" target="_blank" rel="nofollow noreferrer noope
177
178       </h3>
179       <br>
180     </div>
181   </div>
182
183   ...

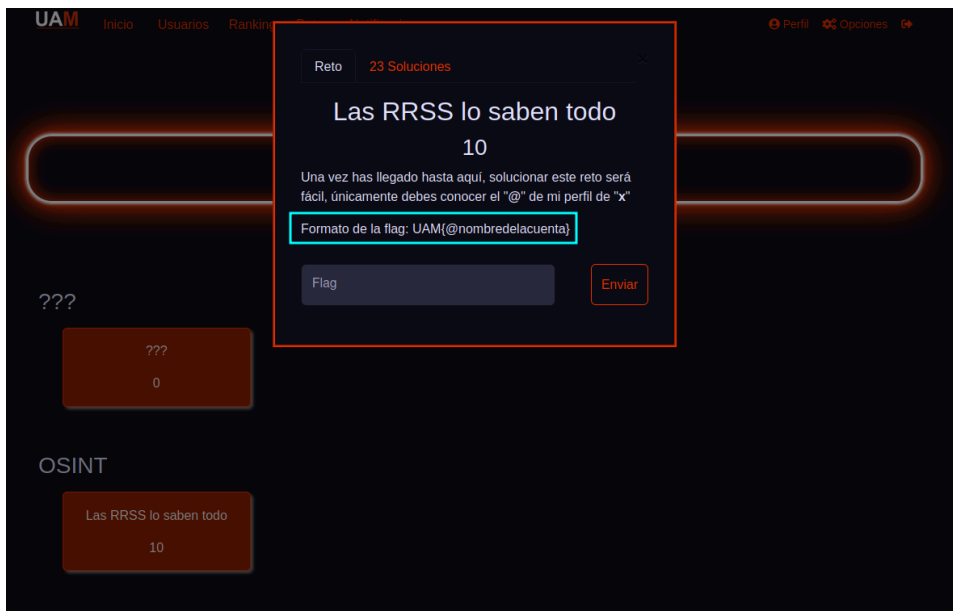
```

Al acceder al enlace se muestra una imagen que es el logo de una empresa de videojuegos, el mensaje del propio perfil da a entender que hay algo oculto en la imagen:

```
exiftool Broderbund_logo.png.png
ExifTool Version Number      : 12.40
File Name                    : Broderbund_logo.png.png
Directory                   : .
File Size                    : 6.0 KiB
File Modification Date/Time  : 2024:01:29 14:34:42+01:00
File Access Date/Time       : 2024:01:29 14:34:42+01:00
File Inode Change Date/Time  : 2024:01:29 14:34:42+01:00
File Permissions             : -rw-rw-r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                  : 320
Image Height                 : 126
Bit Depth                    : 8
Color Type                   : Grayscale with Alpha
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
Gamma                        : 2.2
White Point X                : 0.3127
White Point Y                : 0.329
Red X                        : 0.64
Red Y                        : 0.33
Green X                      : 0.3
Green Y                      : 0.6
Blue X                       : 0.15
Blue Y                       : 0.06
Background Color             : 255
Datecreate                   : 2023-02-17T13:00:08+00:00
Datemodify                   : 2023-02-17T13:00:08+00:00
Author                       : csdgo
Comment                      : 2a1ffc86a354513c51c746d0812cf2ec
Image Size                   : 320x126
Megapixels                   : 0.040
```

El campo **"Comment"** tiene un hash MD5, el perteneciente a la creación de la cuenta.

Una vez creada es posible acceder a la primera flag:



2.2.2. Búsqueda de información sobre el nuevo usuario

Resolución

En el metadato **author** se encontraba el usuario “csdgo”; al buscar el nombre en Google no aparece ningún resultado relevante aparentemente; al enumerar usuarios con herramientas se muestra lo siguiente:

```
root@kali:~/Documents# nexfil -u csdgo
[+] Importing Modules...

NEXFIL

[>] Created By   : thewhiteh4t
[>] --> Twitter  : https://twitter.com/thewhiteh4t
[>] --> Community: https://twc1rcle.com/
[>] Version     : 1.0.6

[!] Loading URLs...
[+] 328 URLs Loaded!
[+] Timeout : 10 secs
[+] Target : csdgo

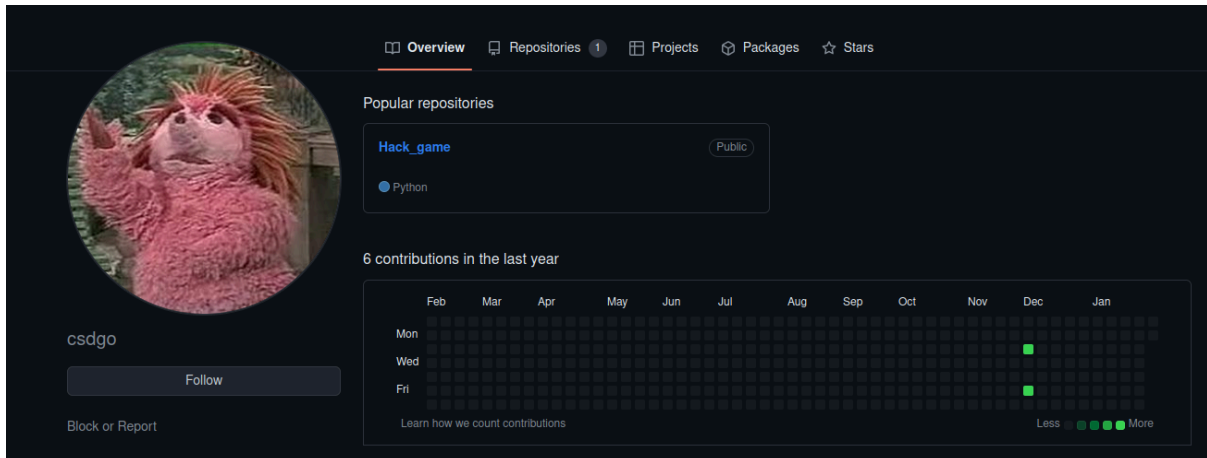
[!] Finding Profiles...

[!] Initializing Chrome Driver...
[-] Chrome not found!
[!] Some websites will be skipped!

https://www.chess.com/member/csdgo
https://www.cnet.com/profiles/csdgo/
https://ok.ru/csdgo
https://github.com/csdgo
https://m.twitch.tv/csdgo
https://baraza.africa/u/csdgo
https://contently.com/
https://archiveofourown.org/users/csdgo
https://t.me/csdgo
https://steamcommunity.com/id/csdgo
https://gist.github.com/csdgo/
https://steamcommunity.com/groups/csdgo
https://lemmy.ml/u/csdgo
https://app.memrise.com/signin?next=/user/csdgo/
https://www.munzee.com/m/csdgo
https://gab.com/04
https://ds9.lemmy.ml/u/csdgo
https://myspace.com/csdgo
https://lemmygrad.ml/u/csdgo
https://lemmy.glasgow.social/u/csdgo
https://consent.youtube.com/m?continue=https://www.youtube.com/csdgo?cbrd%3D1&gl=ES&m=0&pc=yt&cm=2&hl=es&src=1
https://www.gunsandammo.com
https://www.roblox.com/users/909322659/profile
https://gravatar.com/csdgo
https://hypel.ink/csdgo
https://www.slideshare.net/csdgo
https://ingsrc.ru/main/user.php?user=csdgo
https://lemmy.tedomum.net/u/csdgo
https://www.zhihu.com/people/csdgo
https://www.pinterest.com/csdgo/
[>] Progress : 326
```

Se muestra el siguiente perfil:

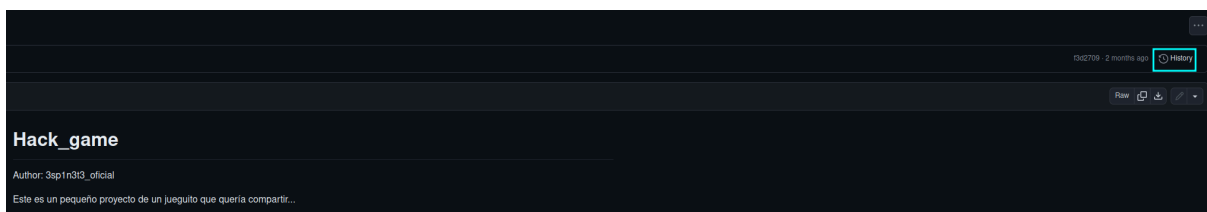
- <https://github.com/csdgo>



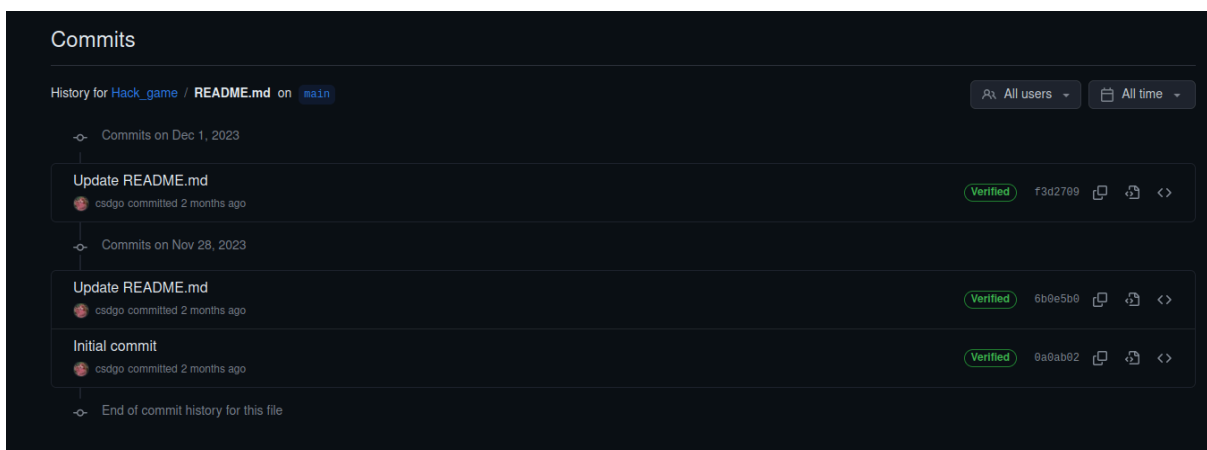
The image shows the GitHub profile page for user 'csdgo'. The profile picture is a pink, spiky-haired character. The page includes a 'Follow' button and a 'Block or Report' link. The 'Popular repositories' section shows 'Hack_game' as the only repository, which is public and written in Python. The '6 contributions in the last year' section shows a calendar grid with green squares indicating contributions on specific days in December and January.

Al acceder a su único proyecto no se encuentra nada relevante en el código, sin embargo, el **README** puede ser interesante debido a que hay un campo **author**.

Al observar la lista de cambios se observa lo siguiente:



The image shows the GitHub repository page for 'Hack_game'. The repository is public and written in Python. The README file is visible, showing the author's name '3sp1n3t3_oficial' and a description: 'Este es un pequeño proyecto de un juego que quería compartir...'. The 'History' button is highlighted in the top right corner.



The image shows the 'Commits' page for the 'Hack_game' repository, specifically for the 'README.md' file on the 'main' branch. The page displays a list of commits, including 'Update README.md' and 'Initial commit', with their respective commit hashes and timestamps. The 'History' button is highlighted in the top right corner.

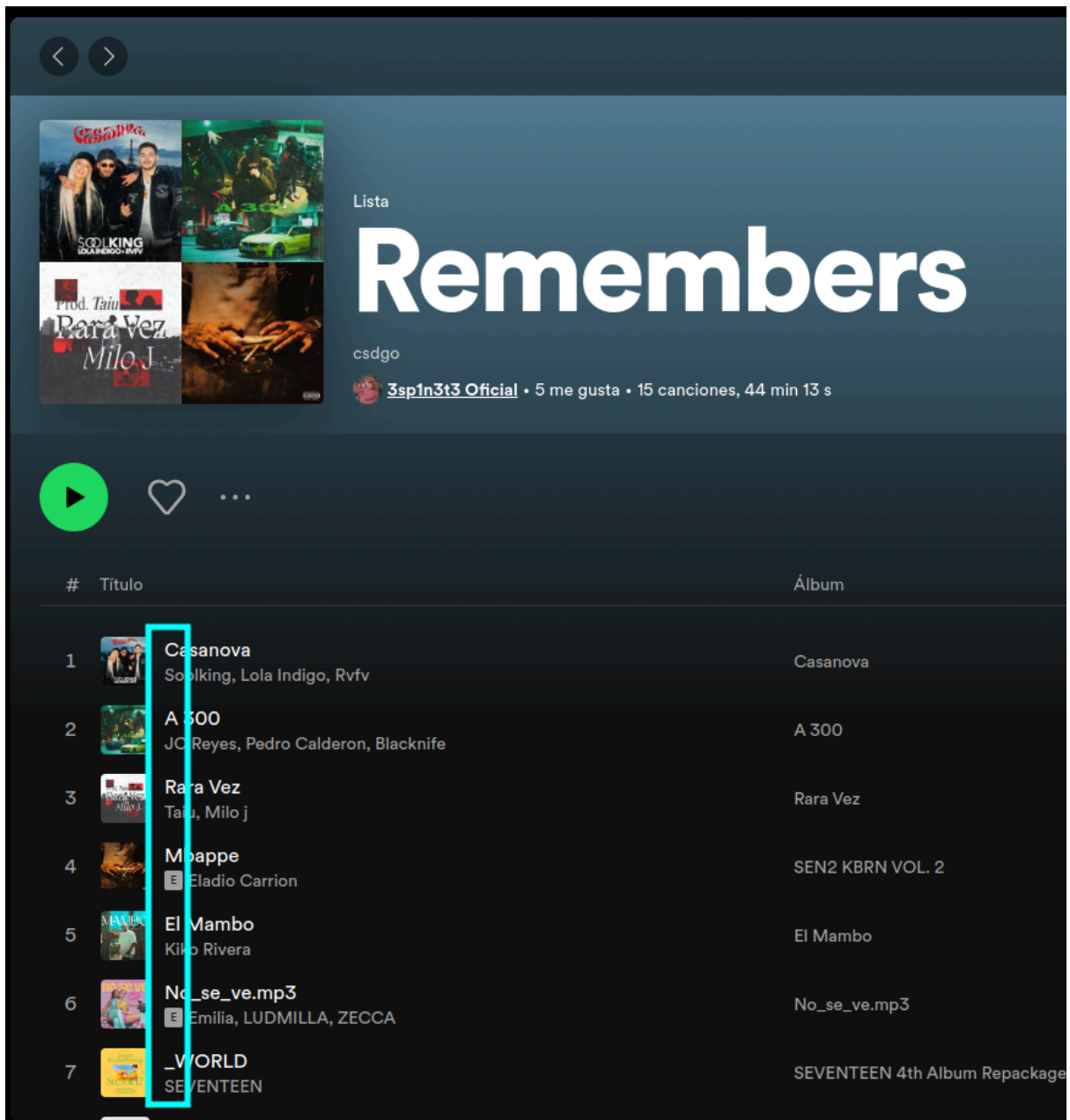
En uno de los *updates* se encuentra el nombre real del atacante:

```
▼ 5 ■■■■ README.md
...  ...  @@ -1 +1,4 @@
1 - # Hack_game
  1 + # Hack_game
  2 + Author: Carmen Sandiego
  3 +
  4 + Este es un pequeño proyecto de un jueguito que quería compartir...
```

¡Flag localizada!

También se puede encontrar esta última flag en la lista de Spotify que tenemos en el perfil de Twitter, cogiendo la primera letra de cada canción podemos formar el nombre de nuestra atacante:





The screenshot shows a Spotify playlist interface. At the top, there are navigation arrows and a header section with album covers and the title 'Remembers' in large white text. Below the title, it says 'Lista' and 'csdgo'. A line of text indicates '3sp1n3t3 Oficial • 5 me gusta • 15 canciones, 44 min 13 s'. Below this is a play button, a heart icon, and a three-dot menu. The main part of the image is a list of songs with columns for '#', 'Titulo', and 'Álbum'. A red box highlights the first three songs in the list.

#	Titulo	Álbum
1	Casanova Soolking, Lola Indigo, Rvfv	Casanova
2	A 300 JC Reyes, Pedro Calderon, Blackknife	A 300
3	Rara Vez Tatu, Milo j	Rara Vez
4	Moappe Eladio Carrion	SEN2 KBRN VOL. 2
5	El Mambo Kiko Rivera	El Mambo
6	No_se_ve.mp3 Emilia, LUDMILLA, ZECCA	No_se_ve.mp3
7	_VWORLD SEVENTEEN	SEVENTEEN 4th Album Repackage

The background of the slide is a dark blue gradient. On the left side, there is a pattern of overlapping, semi-transparent squares and rectangles in a lighter blue color, creating a complex, geometric texture. A large, solid orange triangle is positioned on the right side, pointing towards the bottom right corner. A thick orange diagonal line runs from the top left towards the bottom right, intersecting the other elements.

Hispacec]

Hispacec Sistemas S.L.

C/ Severo Ochoa, 10 - 29590, Málaga

Telf: (+34) 952 020 494

info@hispacec.com