ALERTA TEMPRANA-BANCOBILLULLO

Equipo de inteligencia:

Gracias a las habilidades de uno de nuestros agentes encubiertos, se está llevando de cerca la interacción con uno de los afiliados del grupo identificado como OCELOT APT. Nuestro agente nos comparte información de inteligencia recabada de primera mano acerca de la posible filtración de bases de datos de clientes de Banco Billullo. Su deber como Analista es seguir la pista que nuestro agente encubierto trajo, para así poder dar con información de las presuntas bases con las que cuenta dicha entidad siguiendo cada uno de los objetivos.

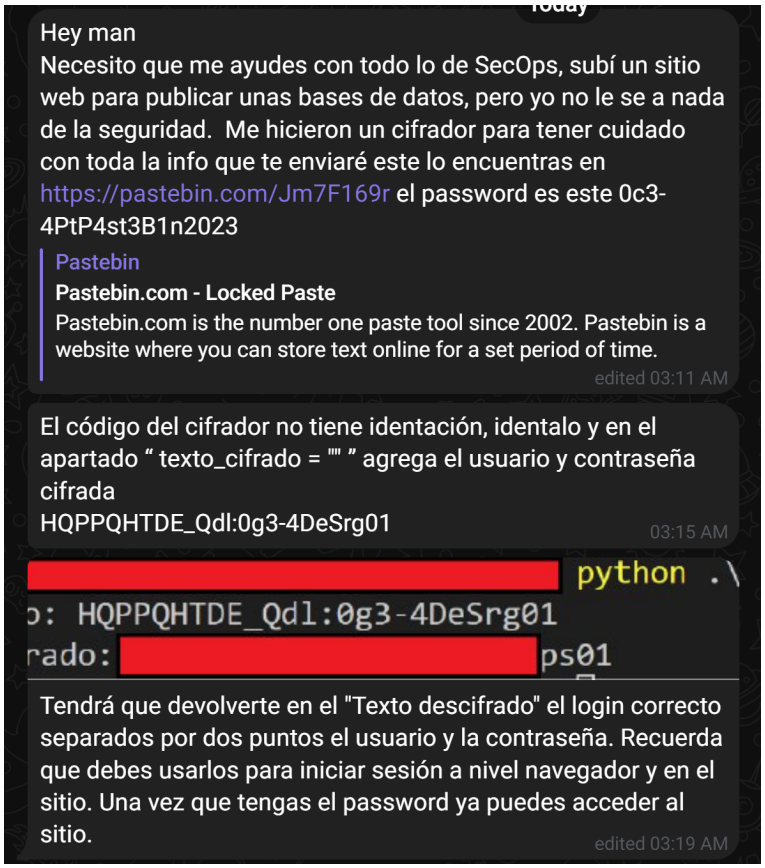

Figura 1. Interacción con entidad mediante Telegram

El primer objetivo es; obtener el usuario y contraseña reales para poder acceder al sitio, como pista, se tiene que dicho "password" debe terminar con "ps01". -Resultado: "OCELOTAPT_Ops:0c3-4PtOps01"

La conversación de la entidad y el agente encubierto continúa, aquí la entidad revela la URL de su presunto sitio, sin embargo, es muy claro que tiene manera de monitorear los inicios de sesión no exitosos. Por su parte nuestro agente encubierto nos comunica que el archivo de DB es el mismo archivo en todos los casos.

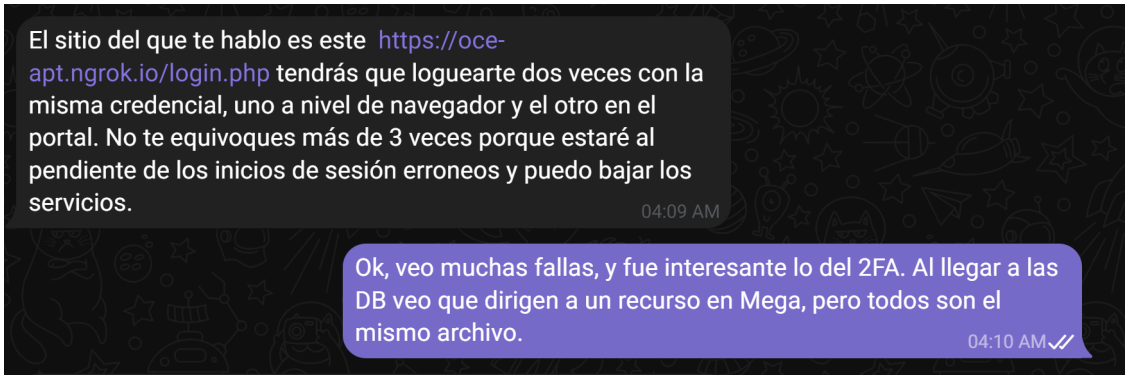

Figura 2. Interacción con entidad quien revela su sitio

El segundo objetivo es; iniciar sesión en el recurso de la entidad, siendo precavidos, **---no se puede usar fuerza bruta---** ya que podría comprometer la investigación.

Resultado: Primera autenticación

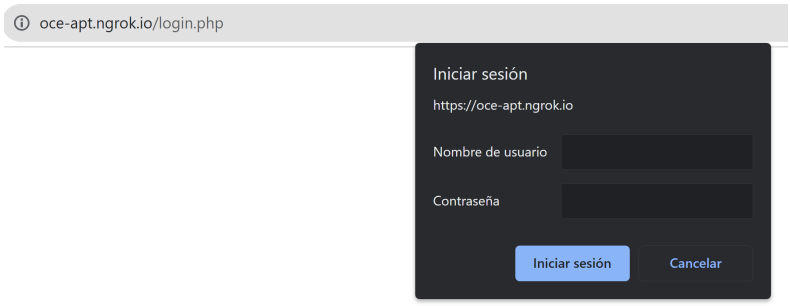

Figura 3. Primera autenticación

Resultado: Segunda autenticación

Figura 4. Segunda autenticación

Resultado: Sitio paso.html

Figura 5. Sitio paso.html

En el sitio paso.html hay código morse, si esos caracteres se envían a cualquier sitio de traducción de código morse podrán leer que no existe un PIN, solo deben dar clic en acceder, y que solo deben quitarle el último punto a la página siguiente

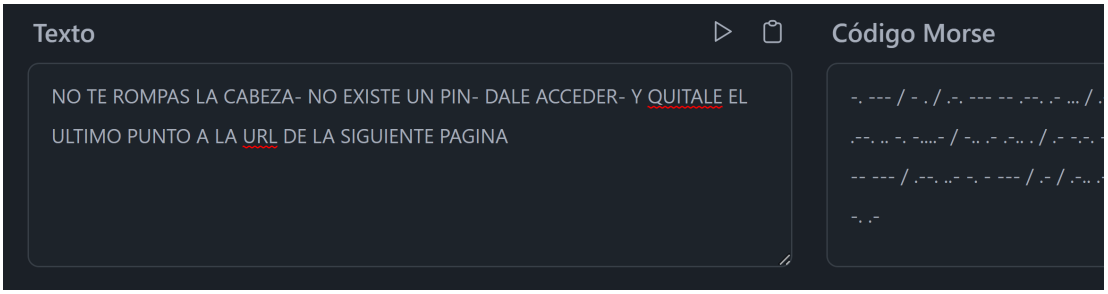

Figura 6. Código morse

Si no lo hacen solo verán una respuesta 404 al darle clic en Acceder, o bien al ingresar PINs al azar el botón acceder pierde su funcionalidad.

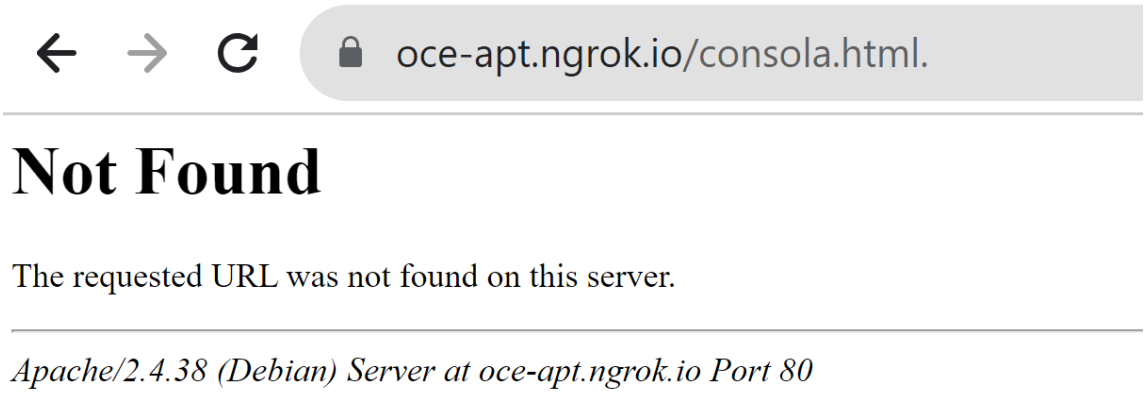

Figura 7. Error 404

Finalmente, nuestro agente encubierto nos comparte este tercer fragmento de la conversación, en donde se nos indica que la entidad aún no ha cargado las bases reales, pero que una vez llegando a un grupo nos dará la última llave.

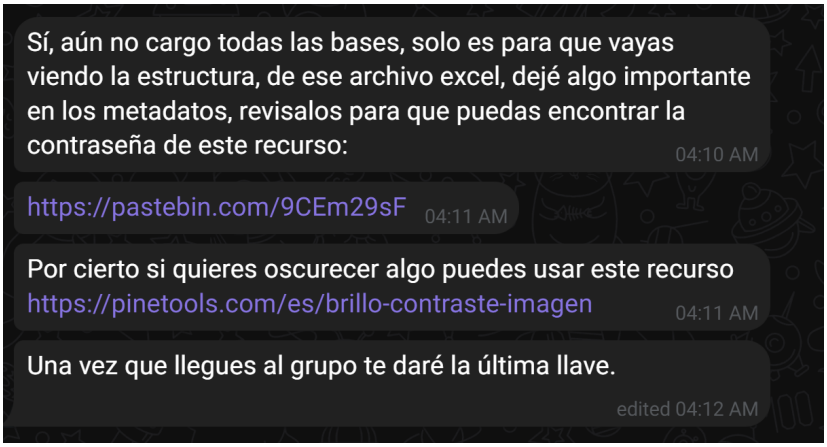

Figura 8. Interacción con entidad quien revela existencia de un sitio

El tercer objetivo es; Encontrar el archivo de Excel de la DB y validar sus metadatos

Resultado: En la pagina de consola.html, tienen que hacer un QUERY directo en la página, algo como:

SELECT empresa, leak_size, tipo_leak, enlace FROM tabla_ofertas WHERE empresa = 'Banco Billullo';
Les dará este resultado:

Figura 9. Respuesta del server al hacer QUERY valida

En donde encontramos la URL de la presunta DB que debemos descargar y mirar sus metadatos
https[:]//mega[.]nz/file/IdhVyRqB#Az80_4AmjGInJSad6e6HbMw778znIuU4xXwpDDY_jas

En los metadatos te menciona que busques la imagen llamada origen , que debes bajarle el brillo y que te mostrará el password del pastebin

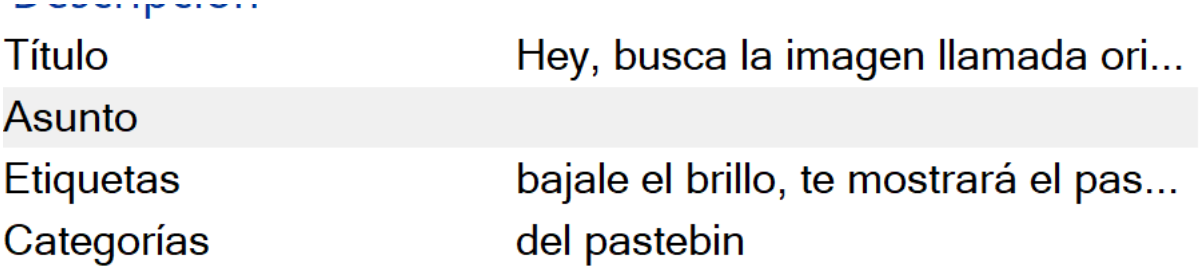

Figura 10. Metadatos del excel

El cuarto objetivo es; encontrar la llave para acceder a dicho recurso pastebin

Resultado: Primero encontramos origen.jpg que está en la URL paso.html

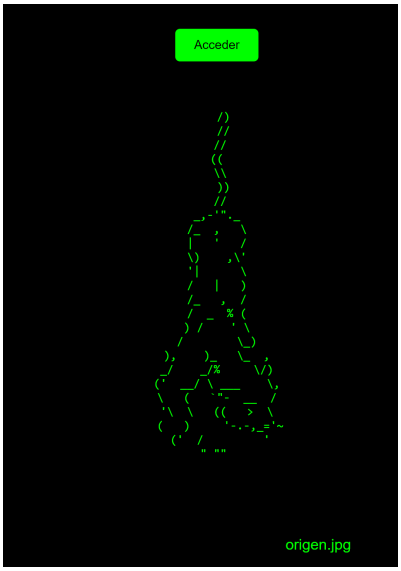

Figura 10. Ubicación imagen "origen.jpg"

Al descargarla y bajarle el brillo y subir el contraste, podemos ver el password del recurso PasteBin.

Figura 11. Password oculto en la imagen

El quinto y último objetivo es; encontrar la supuesta llave.
Al llegar al PasteBin nos damos cuenta que se debe acceder a un grupo de Telegram

text 0.16 KB | Fixit

```
1. "Felicidades, has llegado a la última parte del pequeño reto de OSINT"
2.
3. https://t.me/+HX57My6aQFpiZTFh Ingresa al grupo de Telegram para Obtener la Flag
```

Figura 12. PasteBin final

En el cual ya los espera una Llave que es la Flag

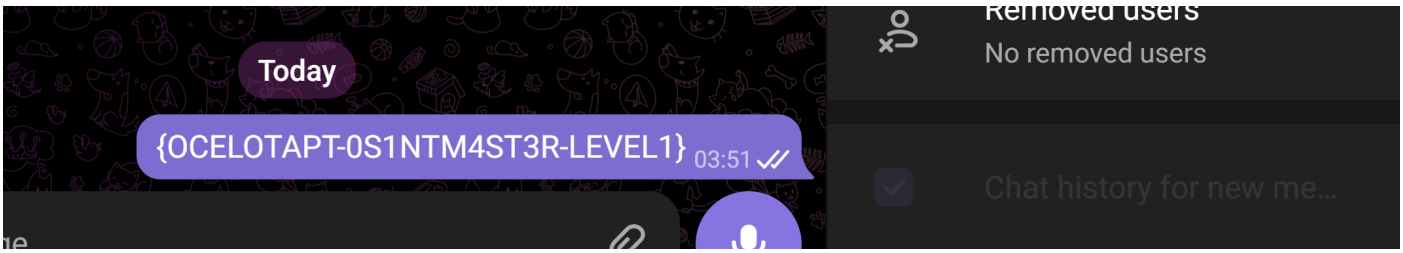

Figura 13. Flag