



# CTF WRITE-UP



RETO INSIDER I: Descargamos el fichero y lo descomprimos, dentro encontramos los ficheros DFs46BasdawRT7DpiwRB1asDe.conti y CONTI\_README.txt.txt

Dentro del fichero CONTI\_README Podemos ver la nota de rescate, que nos da la referencia a la cuenta @conti\_es.

Buscamos en twitter la cuenta y no vemos ninguna información de utilidad, pero observando a los seguidores encontramos una cuenta

conleaks de conti: @m1Geelka, es el nombre del insider y la primera flag:  
INT{@m1Geelka}



RETO INSIDER II: En este reto nos pide un ID, Podemos ver varios strings en los posts del usuario y una referencia a un vinculo en anonfiles con el bmp del avatar de conti\_es, el post más reciente llama la atención por tener la misma longitud que los ids de anonfiles por lo que vamos a la ruta

<https://anonfiles.com/7eK111z2yd> y descargamos el fichero m4v8z6AK, este nombre es el id que buscamos y la segunda flag:

INT{m4v8z6AK}



RETO INSIDER III: En este reto nos piden descodificar el contenido del fichero, en el HTML anterior vemos el texto PB: m4v8z6AK, después de caer en que PB es pastebin visitamos la url

<https://pastebin.com/m4v8z6AK> que nos lleva a un texto sobre piezas de coches creado por el usuario M1GEELKA, si pulsamos sobre el usuario nos lleva a sus otros bins, vamos visitandolos sin ver nada en especial hasta llegar al “LARON an otp industrial solutions

company” en este fichero hay una referencia a conti-the-filecrypter-repo.s3.eu-west-3 que claramente apunta a un bucket s3 de amazon, por lo que completamos la url y accedemos a conti-the-filecrypter-repo.s3.eu-west-3.amazonaws.com y vemos la

siguiente información:

```
<ListBucketResult>
  <Name>conti-the-filecrypter-repo</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>>false</IsTruncated>
  <Contents>
    <Key>Configs</Key>
    <LastModified>2022-05-31T13:59:33.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>Configs/key.bk</Key>
    <LastModified>2022-06-01T13:48:28.000Z</LastModified>
    <ETag>"a69dc967fff690043dfe969863b0495e"</ETag>
    <Size>92</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

De aquí Podemos extraer que existe un fichero en la ruta /Configs/key.bk así que lo descargamos y vemos el contenido:

```
"#Conti preshared key for AES256 PKCS7 Electronic Code Book
asdfXKKRgFnJEtDOd17KpJmc4TBm3asd"
```

Con lo que ya tenemos la clave y el tipo de cifrado, solo nos queda realizar la operación de descifrado, para ello vamos a <https://www.devglan.com/online-tools/aes-encryption-decryption>, ponemos el texto, el tamaño de la clave a 256 bits y desciframos, nos devuelve la cadena en base64 SU5Ue19jMG43MV8xNV9kNG42M3lwdTVffQ== que si la decodificamos a texto plano nos da la siguiente flag: INT{\_c0n71\_15\_d4n63r0u5\_}

Reto 15 Soluciones





## IDENTIDAD I

22

**GEOINT**

Las autoridades nos han hecho llegar varias imágenes relacionadas con un viaje previo que habría realizado el insider.

¿A qué lugar corresponden?

Flag

RETO IDENTIDAD I: En este reto nos piden encontrar el lugar del viaje del insider, para ello buscamos metadatos en las imágenes, y encontramos que la imagen 1509582.jpg tiene como autores unas coordenadas GPS 14.3589404, 24.48102987347 introduciendo esas coordenadas cambiando la coma por el subguión tenemos la primera flag: INT{14.3589404\_24.48102987347}

Reto 9 Soluciones

## IDENTIDAD II

48

**OSINT**

Parece que el insider estuvo haciendo turismo y visitó tal zona en algún momento, pero necesitamos confirmarlo.

¿Qué "base" tenemos para afirmar tal cosa?

Flag

RETO IDENTIDAD II: En este reto nos piden encontrar la base para afirmar que el sujeto estuvo en la localización anterior, por lo que buscamos evidencias de que estuviera en la zona, vamos a google maps y buscamos las coordenadas descubiertas: nos lleva a algún punto en Sudan, si alejamos el mapa encontramos un hotel y en las reseñas de google una de alguien que se hace llamar tormenta del desierto con un comentario criptico: "Sal ahí fuera y mira lo que otras personas no ven...." si nos fijamos en la foto del perfil vemos que hay alguna especie de texto dentro.

Si inspeccionamos la foto del perfil vemos su url: <https://lh3.googleusercontent.com/a-/AFdZucrAuFPoXnOlwiTvmMBSLnj62JI7u0MMM3f0AwBV=w60-h60-p-rp-mo-br100> y si modificamos los parámetros de tamaño Podemos verla con el texto en claro:

<https://lh3.googleusercontent.com/a-/AFdZucrAuFPoXnOlwiTvmMBSLnj62JI7u0MMM3f0AwBV=w600-h600-p-rp-mo-br100>



MTAwMDgxODUxMzQ4NDg3== que si lo pasamos de base64 a texto nos da el número 100081851348487 que corresponde a la siguiente flag: INT{100081851348487}

RETO IDENTIDAD III: Aquí nos piden averiguar el nombre real del insider, y nos indican que la flag anterior abre una nueva línea de investigación, para continuar vamos a probar perfiles con el id anterior en las redes sociales, al probar en facebook encontramos una coincidencia en

<https://www.facebook.com/profile.php?id=100081851348487>

Aquí vemos que en detalles nos da otro número

04936018196757075735 y entrando en la información en el apartado detalles sobre Tepunto el siguiente texto: “D.Storm (Pyra Labs)”

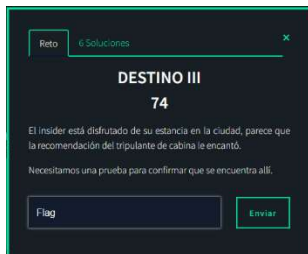
Una pequeña búsqueda nos indica que Pyra labs se ha convertido en blogger por lo que vamos a buscar un perfil de blogger utilizando el número encontrado previamente:

<https://www.blogger.com/profile/04936018196757075735> y efectivamente nos sale el usuario d.storm y un blog Tormentaydesierto además del nombre en ruso del autor: Анатолий Андрусенко que al pasarlo por el traductor de google nos lleva al nombre real: Anatoly Andrusenko y por tanto a la flag: INT{Anatoly\_Andrusenko}

RETO DESTINO I: Aquí nos piden averiguar la ciudad donde se encuentra el aeropuerto y nos proporcionan una imagen, haciendo una búsqueda con google lens en el arco de las maletas nos apunta al aeropuerto de Naxos en Grecia. Por lo que ya tenemos la flag: INT{NAXOS}

RETO DESTINO II: Aquí nos piden el nombre del tripulante de cabina que le recomendó el hotel, sin más datos no había manera de encontrarlo así que me decidí por buscarlo a fuerza bruta utilizando un diccionario de nombres comunes y una frecuencia adecuada para no dañar la plataforma. No obstante al no quedarme tranquilo, más tarde se me ocurrió que al describir un puesto de trabajo podría intentar buscar en linkedin un perfil profesional que se ajustase a los pocos datos disponibles y al investigar sobre vuelos desde Naxos solo había un destino sin escalas posible, de esta manera construimos una búsqueda con el vuelo Naxos atenas (JNX-ATH) y la profesión traducida al griego πλήρωμα καμπίνας con lo

que google nos lleva a un perfil falso de linkedin llamado losif García donde recomienda un hotel en atenas. Esto nos permite insertar la siguiente flag: INT{IOSIF}



RETO DESTINO III: Aquí debemos encontrar una prueba de que el agente está en el lugar indicado, para ello usamos la foto de la recomendación de linkedin y google lens, lo que nos lleva a la plaza Monastirakiou de atenas, y a través de google maps buscamos el hotel que proporciona las vistas, que por ubicación solo puede ser el A for Athens.

Tenemos localizado el hotel y hay que encontrar evidencias de que nuestro Anatoly está en la ciudad por lo que vamos a tripadvisor como web de referencia y buscamos el hotel, ordenando las reseñas por más recientes y todos los idiomas, confirmamos que tenemos un comentario de anatoly con una referencia a losif:



Con lo que conseguimos la última flag: INT{p0SMzGL1oAMhWin}