Reporte de Inteligencia

Presunta filtración de datos corporativos caso Fibertel S.A



Fecha: 23/07/2026
Categoría: Reporte de presunta filtración de datos corporativos
Investigador: David Padron
Contacto: davidpadron.cyber@gmail.com

Índice

Alcance y Objetivos....4
Objetivo de la investigación:....4
Alcance de la investigación:....4
Se contemplan los siguientes aspectos de investigación:....5
Limites de la investigación:....5
Metodología....5
Técnicas y procedimientos:....5
Herramientas de la Investigación:....5
Resumen Ejecutivo....6
Hallazgos Claves:....7
1. Arquitectura de maquinas virtuales....8
1.1 Laboratorio Virtual para Research....8
1.2 Laboratorio Virtual para Análisis de Malware....9
2. Conexiones de Red....9
2.1 Arquitectura de Red:....9
2.2 Configuración DNS Remoto (Proxyxhains)....10
2.3 Tabla de rutas del tráfico TCP del sistema (ProtonVPN)....10
2.4 ProtonVPN y Tor sockets....10
3. Prueba de concepto tráfico TCP....11
4. Navegación foro Darkforums....12
4.1 Acceso al foro....13
4.2 Inicio de sesión (Login)....13
4.3 URL de filtración....14
4.4 URL descarga....15
4.5 Archivo descargado....15
5. Análisis de Malware Estático....16
5.1 Transferencia de archivos a VM....16
5.2 Metodología de Análisis Estático (RAR)....16
5.2.1 FASE 1 — Creación de directorios de trabajo....17
5.2.2 FASE 2 — Hashing....17
5.2.3 FASE 3 — Identificación Real del Archivo....18
5.2.4 FASE 4 — Magic Bytes....19
5.2.5 FASE 5 — Entropía....20
5.2.6 FASE 6 — Strings....21
5.2.7 Interpretación y Conclusión....23
5.3 Metodología de Análisis Estático (TXT)....23
5.3.1 FASE 1 — Creación de directorios de trabajo....23
5.3.2 FASE 2 — Hashing....23
5.3.3 FASE 3 — Identificación Real del Archivo....24
5.3.4 FASE 4 — Magic Bytes....25
5.3.5 FASE 5 — Entropía....26
5.3.6 FASE 6 — Strings....26
6. Visualización del archivo....27
6.1 FASE 7 — Inspección del Contenido....27
7. Validación de Identidad....28
8. Validación de Domicilio....28
8.1 Muestra del archivo extraído:....28
8.2 Domicilio Fiscal:....28
8.3 Ubicación Google Maps:....29

8.4 Interpretación.....29
8.5 Conclusión.....30
9. Validación Número de Teléfono.....31
9.1 Muestra del archivo extraído.....31
9.2 Número de teléfono.....31
9.3 Código de área telefónico.....31
9.4 Telefonía móvil Personal.....32
9.5 Verificación Whatsapp.....33
10. Validación Correo Electrónico.....33
10.1 Muestra del archivo extraído.....33
10.2 Microsoft Hotmail - Outlook.....34
11. Validación Redes sociales.....34
11.1 Facebook (Email).....34
11.2 Facebook (Teléfono).....35
11.3 Instagram (Email).....36
12. Validación Google.....37
13. Validación servicio energía.....37
13.1 Servicio energía eléctrica.....37
Validación de registro en plataforma web:.....37
Validación del correo electrónico:.....38
13.2 Servicio gas natural.....39
14. Conclusión del análisis de inteligencia.....40

Alcance y Objetivos

Objetivo de la investigación:

Se investigara la presunta filtración de datos de la empresa Fibertel S.A (actualmente absorbida por la corporación de servicios de internet y telefonía Telecom Argentina S.A) detectada en el foro de filtraciones denominado “DarkForums” publicada el 10/07/25.

Se iniciara un proceso de investigación privada con fines éticos mediante el uso de fuentes abiertas y cerradas para recolectar, analizar y correlacionar información que sirva para verificar si efectivamente los datos filtrados en el foro pertenecen a la empresa afectada o se trata de un falso positivo y en tal caso alertar a dicha empresa.

Alcance de la investigación:

El proceso de la investigación se llevara a cabo mediante el uso de fuentes de información tanto abiertas como cerradas, con el fin de poder recolectar datos que permitan verificar la veracidad y severidad de los hechos. La investigación se focaliza exclusivamente en la recolección y el análisis de datos publicados en el foro DarkForums sobre la empresa Fibertel S.A.

En ningún momento se pretende investigar al actor que vulnero la empresa afectada y realizo la publicaron de los datos filtrados en el foro.

Se contemplan los siguientes aspectos de investigación:

- Acceso y navegación por el foro Darkforums
- Búsqueda de filtración de datos relacionados a Fibertel S.A
- Ejecución de análisis estático de malware de los archivos descargados del foro antes de ser descomprimidos y visualizados
- Visualización de los datos contenidos en el archivo de filtración
- Validación de los datos filtrados con búsquedas de fuentes abiertas

Limites de la investigación:

- Investigación de los agentes que filtraron los datos corporativos
- Penetrar y vulnerar sistemas para la obtención de información
- Uso de tácticas y técnicas de ingeniería social para la obtención de información

Metodología

La intención de la investigación es mostrar un paso a paso de todas las fases del proceso investigativo contemplando medidas OPSEC, conexión a redes, acceso al foro, descarga del archivo filtrado, análisis de malware, visualización y validación de los datos.

- Securizar entorno OPSEC
- Recopilación de datos
- Análisis y procesamiento
- Validación y generación de hipotesis

Técnicas y procedimientos:

Para la siguiente investigación se utilizaron diferentes técnicas y procedimientos que incluyen laboratorio aislado con maquina virtual (VM), securización de conexiones de red como VPNs y proxys, navegación por el foro Darkforum, descarga de archivos de filtración de datos y análisis en busca de malware, visualización de los datos filtrados y navegación por Telegram al canal del agente de amenaza.

Herramientas de la Investigación:

- **Maquina Virtual (VM):** VirtualBox
- **Sistema Operativo:** Kali Linux
- **VPN:** ProtonVPN
- **Proxychains:** Tor Network
- **Análisis de Malware:** Detect It Easy (DIE), Malcat
- **Visualización de datos:** notepad.exe
- **Ofimática:** LibreOffice

Resumen Ejecutivo

Se identifico una posible filtración de datos personales de clientes relativos a la empresa de telecomunicaciones Fibertel S.A (Telecom Argentina S.A) publicada en la fecha 10/07/25 en el foro de ciberdelitos Darkforums. En objetivo del reporte es mostrar un pasos a paso de como se realizo la investigación y validación de los datos filtrados mediante el uso de investigación de fuentes abiertas (OSINT).

Dominio web:	darkforums.ru
Fecha de filtración:	10/07/25, 06:00pm
Actor:	injectioninferno2
Veracidad de la muestra (*sample*) filtrada:	Alto

Importante: el hallazgo de inteligencia relevante justifica una evaluación técnica adicional en colaboración con el equipo de seguridad de Fibertel S.A para validar la veracidad de los datos filtrados.

Hallazgos Claves:

Coincidencias entre el nombre consignado en la muestra con una persona física aparentemente existente.	Alto
Coincidencias entre el número de documento (DNI) analizado y referencias externas que lo vinculan con dicha identidad y con la localidad especificada en la filtración	Alto
Correspondencia entre el domicilio incluido en la muestra y referencias externas asociadas a la persona investigada.	Alto
Correspondencia de la dirección de correo electrónico en la muestra (h[redacted]@hotmail.com) con servicios personales asociadas a la persona	Medio

investigada.	
Correspondencia de la dirección de correo electrónico (h[redacted]@gmail.com) obtenida mediante OSINT con servicios personales asociadas a la persona investigada.	Alto
Correspondencia del número de telefono filtrado con la caracteristica de locación pertinente a la persona investigada.	Alto
Correspondencia del número de telefono filtrado con la persona investigada.	Bajo
Correspondencia del número de telefono filtrado vinculado con algún servicio de telecomunicaciones de la empresa Personal/Fibertel S.A.	Medio

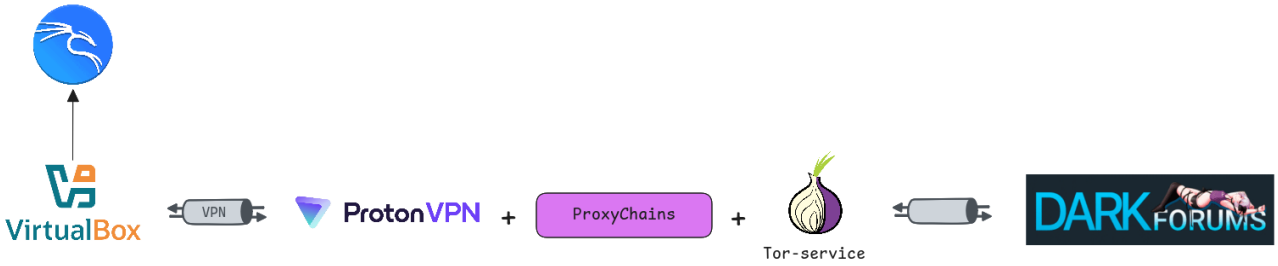
Conclusión: Tanto el número de teléfono como la dirección de correo electrónico Hotmail pueden estar descontinuados o abandonados. Sin embargo, todos los demás datos personales expuestos en el archivo de la muestra son verdaderos.

Configuración entorno OPSEC

1. Arquitectura de maquinas virtuales

Para esta investigación se han montado dos laboratorios virtuales para la etapa de recolección y descarga de archivos filtrados (máquina Linux) y en segunda instancia otro laboratorio aislado para analizar los archivos descargados del foro (máquina Windows) en busca de malware previamente a descomprimir y visualizar los datos filtrados.

1.1 Laboratorio Virtual para Research



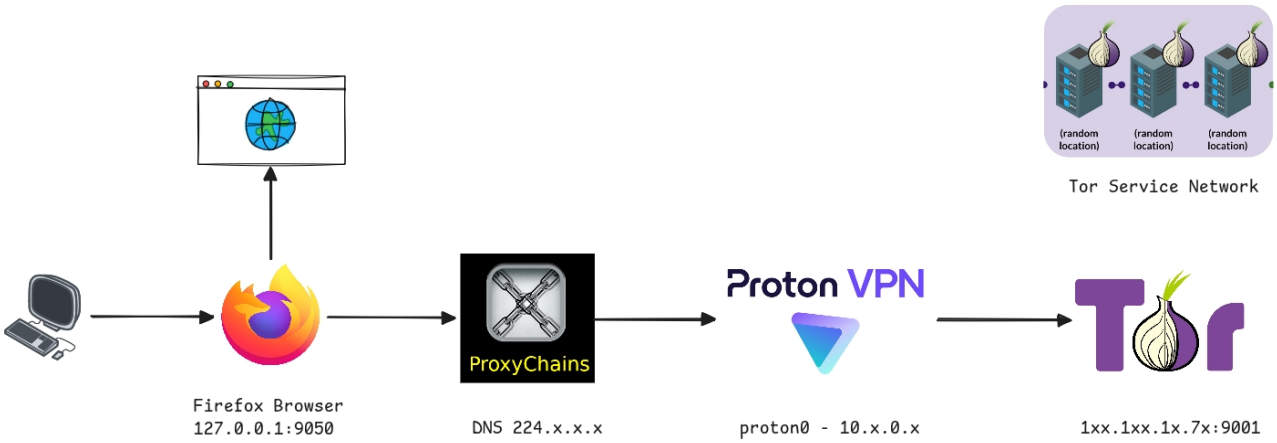
1.2 Laboratorio Virtual para Análisis de Malware



2. Conexiones de Red

Para nuestras conexiones de red utilizaremos la siguiente arquitectura combinando el servicio de `Proxychains` para resolución DNS, `ProtonVPN` para enmascarar nuestra IP real y cifrar nuestro tráfico para no ser visualizado por nuestro ISP ni tampoco revelar nuestra IP real ante Tor. Por último utilizaremos el servicio de la red de `Tor Service` para enrutar todo nuestro tráfico hasta llegar al sitio web solicitado.

2.1 Arquitectura de Red:



Machine → Firefox → Proxychains → ProtonVPN → Tor Service

2.2 Configuración DNS Remoto (Proxyxhains)

```
# set the class A subnet number to use for the internal remote DNS mapping
# we use the reserved 224.x.x.x range by default,
# if the proxified app does a DNS request, we will return an IP from that range.
# on further accesses to this ip we will send the saved DNS name to the proxy.
# in case some control-freak app checks the returned ip, and denies to
# connect, you can use another subnet, e.g. 10.x.x.x or 127.x.x.x.
# of course you should make sure that the proxified app does not need
# *real* access to this subnet.
# i.e. dont use the same subnet then in the localnet section
#remote_dns_subnet 127
#remote_dns_subnet 10
remote_dns_subnet 224
```

Habilitamos la configuración “`remote_dns_subnet 224`” del archivo “`/etc/proxychains4.conf`” para que Firefox ejecute consultas DNS por medio de Proxychains.

CLI: `sudo nano /etc/proxychains4.conf`

2.3 Tabla de rutas del tráfico TCP del sistema (ProtonVPN)



La configuración de la tabla de tráfico redirige todas la solicitudes del sistema a través de la interfaz de red de ProtonVPN (*proton0*).

CLI: `ip route get 1.1.1.1`

2.4 ProtonVPN y Tor sockets



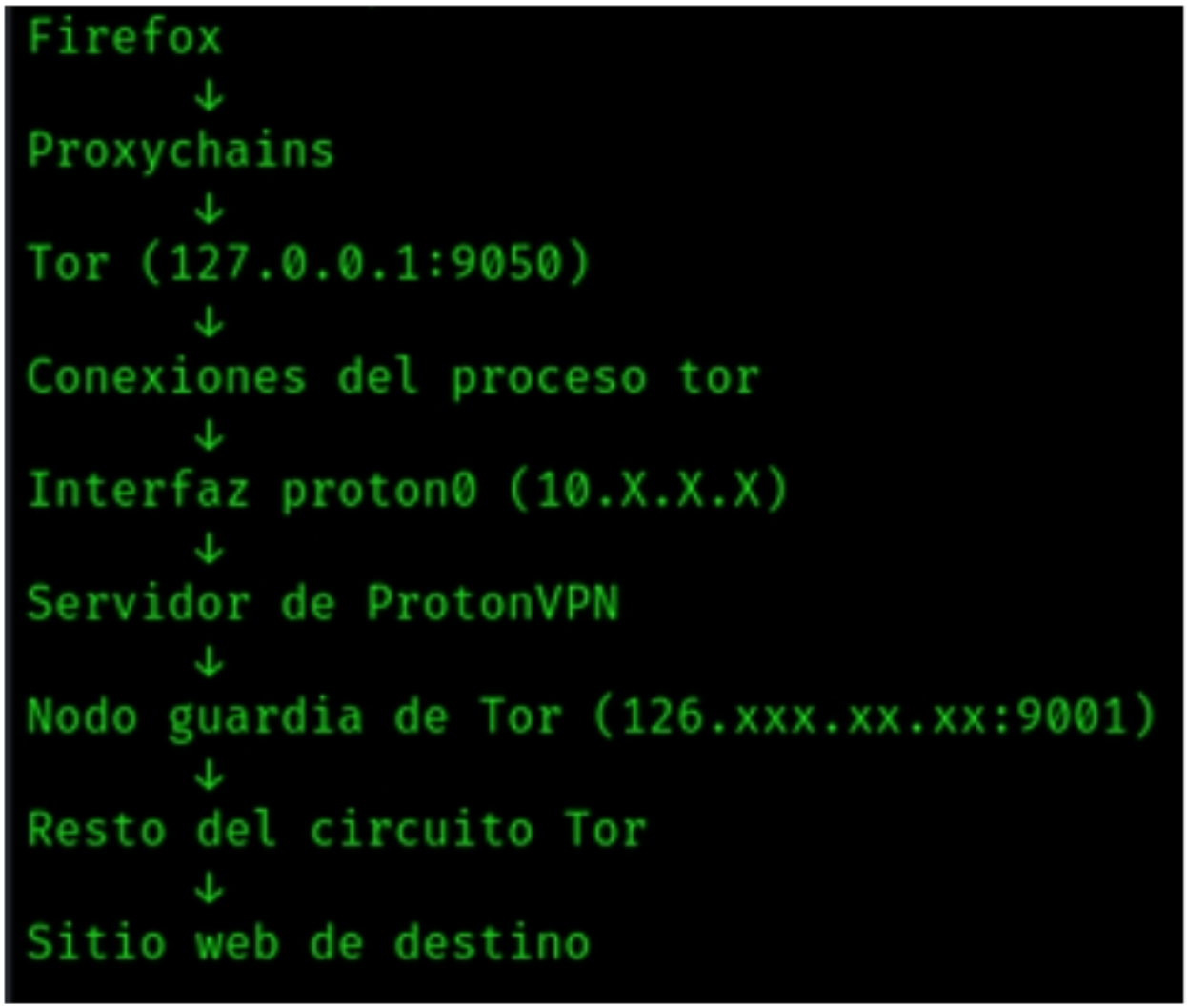
Tor service crea sus sockets de conexión a partir de la interfaz de red de la VPN de Proton.

CLI: `ss -tpn | grep tor`

3. Prueba de concepto tráfico TCP

```
~$ sudo tcpdump -i proton0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on proton0, link-type RAW (Raw IP), snapshot length 262144 bytes
10:24:52.415271 IP workstation.48369 > pim-routers.mcast.net.https: UDP, length 1357
10:24:52.480217 IP workstation.48217 > 10.[redacted].domain: 30841+ [1au] PTR? [redacted].224.in-addr.arpa. (52)
10:24:52.527921 IP workstation.58318 > [redacted]-126.ip.linodeusercontent.com.9001: Flags [P.], seq 1217921816:1217922352, ack 189
881982, win 286, options [nop,nop,TS val 2446220693 ecr 343119860], length 536
10:24:52.667297 IP [redacted]126.ip.linodeusercontent.com.9001 > workstation.58318: Flags [.], ack 536, win 293, options [nop,nop,
TS val 343125882 ecr 2446220693], length 0
10:24:52.704991 IP 10.[redacted].domain > workstation.48217: 30841 1/0/1 PTR pim-routers.mcast.net. (87)
10:24:52.886751 IP [redacted]-126.ip.linodeusercontent.com.9001 > workstation.58318: Flags [P.], seq 1:537, ack 536, win 293, optio
ns [nop,nop,TS val 343126101 ecr 2446220693], length 536
10:24:52.886782 IP workstation.58318 > [redacted]-126.ip.linodeusercontent.com.9001: Flags [.], ack 537, win 286, options [nop,nop,
TS val 2446221052 ecr 343126101], length 0
10:24:52.888152 IP workstation.58318 > [redacted]-126.ip.linodeusercontent.com.9001: Flags [P.], seq 536:1586, ack 537, win 286, op
tions [nop,nop,TS val 2446221054 ecr 343126101], length 1050
10:24:52.888176 IP workstation.48369 > pim-routers.mcast.net.https: UDP, length 1357
10:24:53.025634 IP [redacted]-126.ip.linodeusercontent.com.9001 > workstation.58318: Flags [.], ack 1586, win 289, options [nop,nop
,TS val 343126240 ecr 2446221054], length 0
```

Por medio de la siguiente captura de tráfico de red TCP verificamos que nuestras configuraciones de red sean las correctas y que todo nuestro tráfico utiliza la configuración de Proxychains para consultas DNS, ProtonVPN para enmascarar nuestra dirección IP y el servicio de Tor Network para enrutar nuestras peticiones de red.

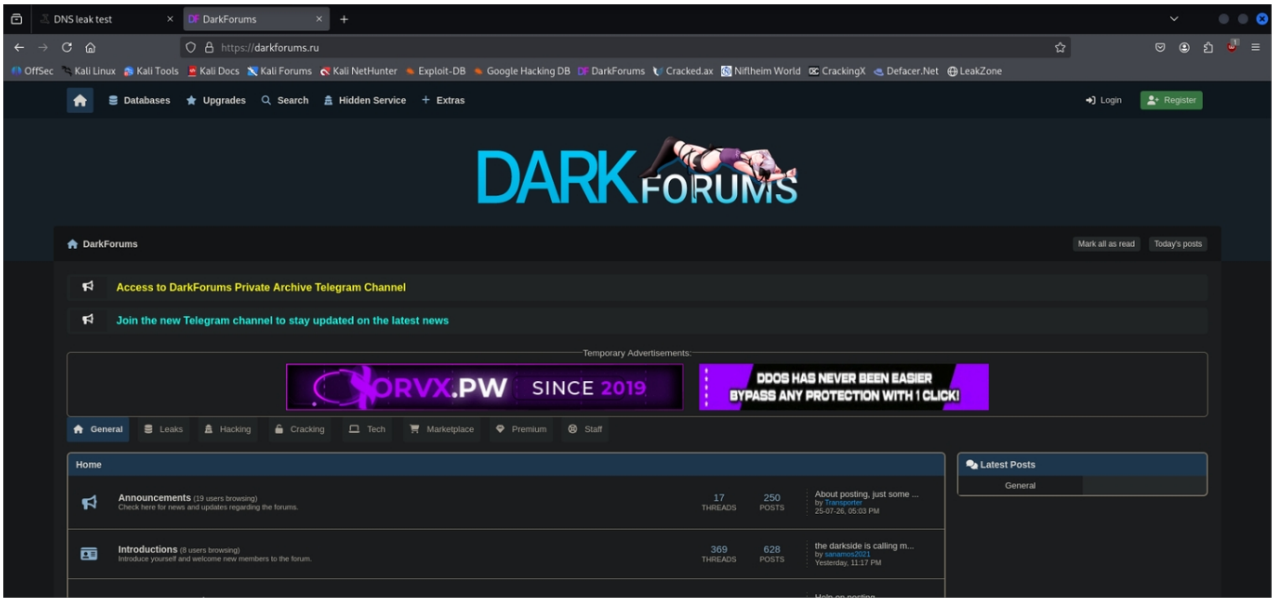


Investigación en foro web

4. Navegación foro Darkforums

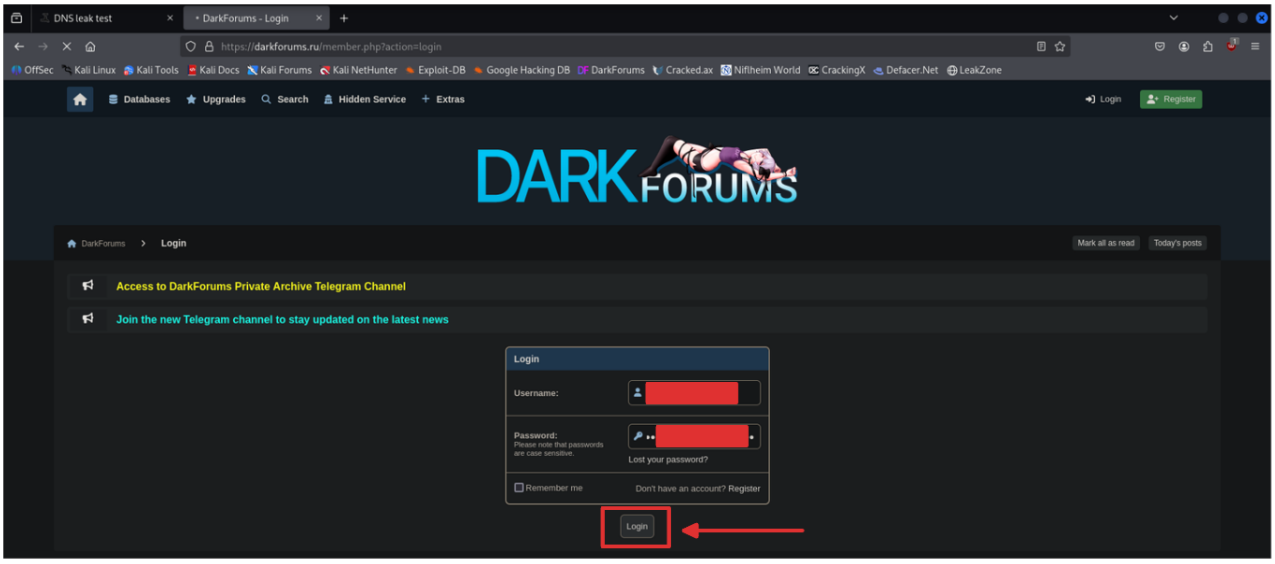
En esta sección del informe estaremos accediendo al foro de hacking denominado “Darkforums” en busca de la publicación de filtración de datos de la empresa Fibertel S.A.

4.1 Acceso al foro

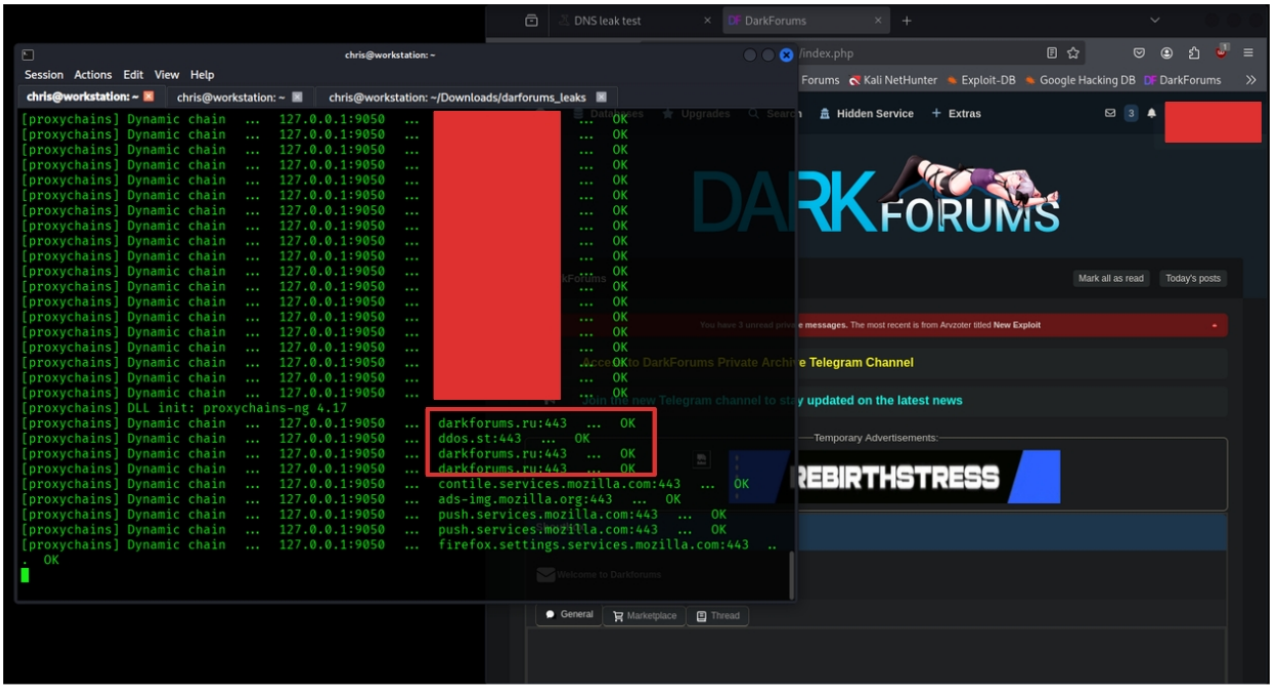


Dominio: darkforums.ru

4.2 Inicio de sesión (Login)

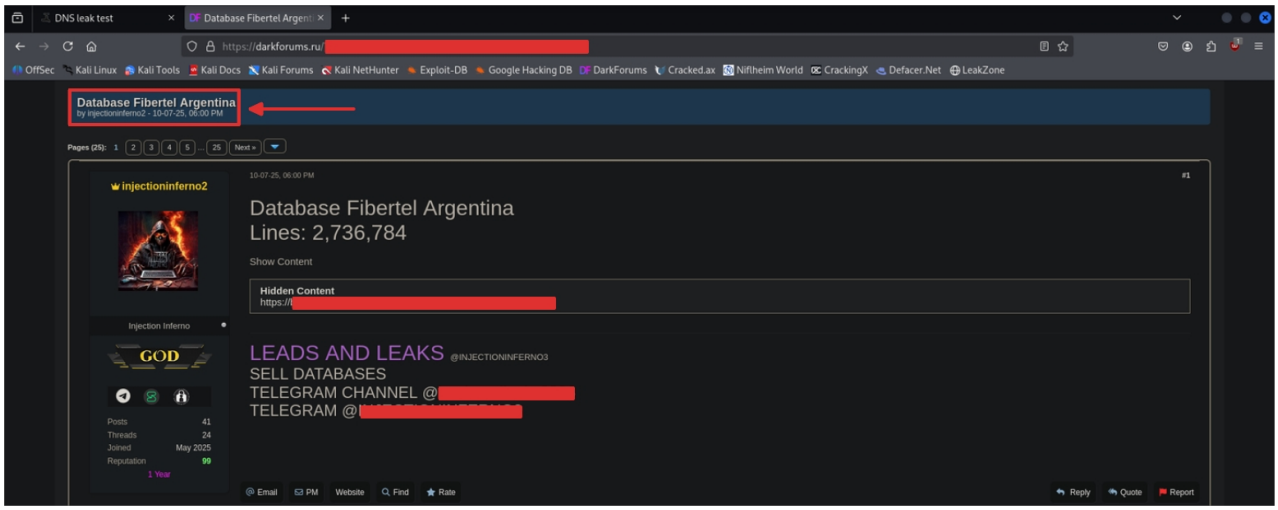


Es necesario estar registrado en la plataforma mediante usuario y contraseña para poder acceder y descargar el contenido publicado. De lo contrario simplemente podremos visualizar las publicaciones más no descargar los archivos.



Posterior al inicio de sesión (login), la plataforma nos solicitara realizar múltiples retos de “Captcha” para acceder efectivamente al sitio web.

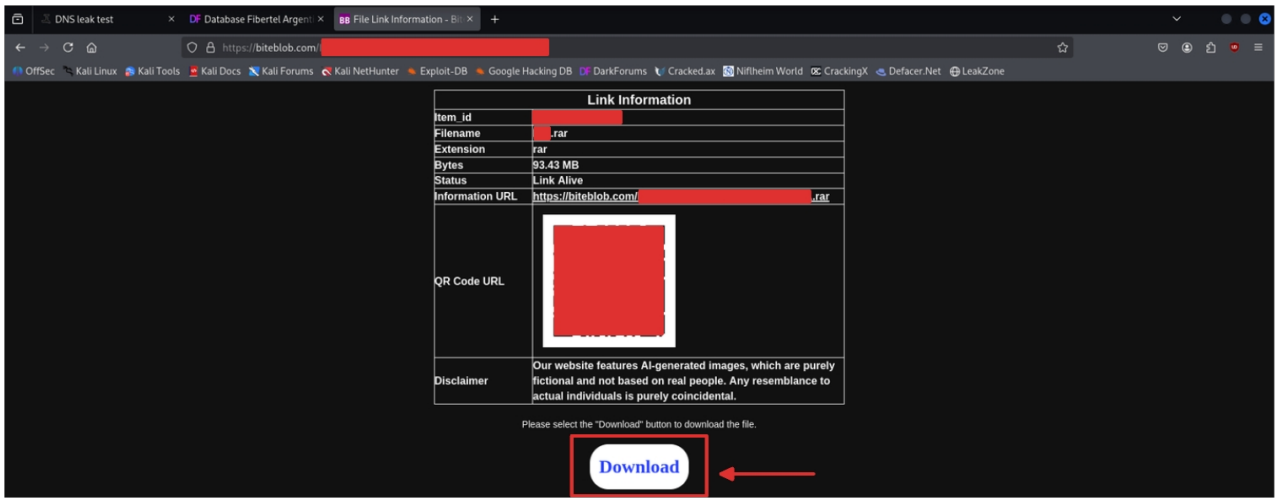
4.3 URL de filtración



Una ves autenticados dentro del foro, podremos navegar en busca de archivos de filtración. Lo podemos realizar desde la sección “*Databases* > *Leaks*” y filtrar por palabra clave de acuerdo a lo que buscamos.

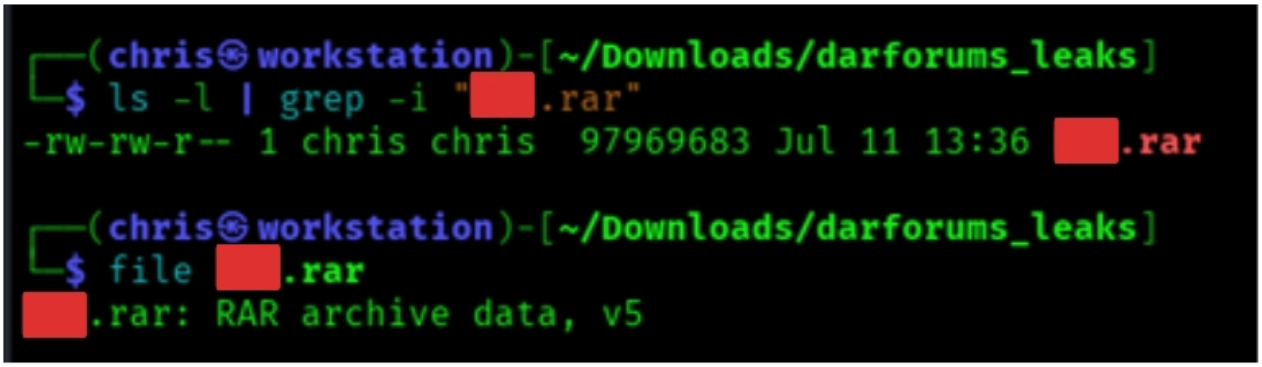
Para este caso especifico, ya se tenia previamente almacenada la URL de la publicación de filtración de los datos de Fibertel, por lo tanto se procedió a solicitar el recurso y descargarlo por medio de otra URL que redirecciono a un servicio de descarga de archivos privado.

4.4 URL descarga



BiteBlob (biteblob.com) es un servicio web de intercambio de archivos de forma anónima. Por medio de este servicio realice la descarga del archivo de filtración.

4.5 Archivo descargado



Finalizada la descarga, obtenemos como resultado un archivo con extensión .RAR.

Hasta aquí culmina la primer etapa de investigación y recolección de información del foro Darkforums. Continuamos con la siguiente fase para verificar si nuestro archivo descargado del foro posee algún tipo de malware.

Análisis de Malware

5. Análisis de Malware Estático

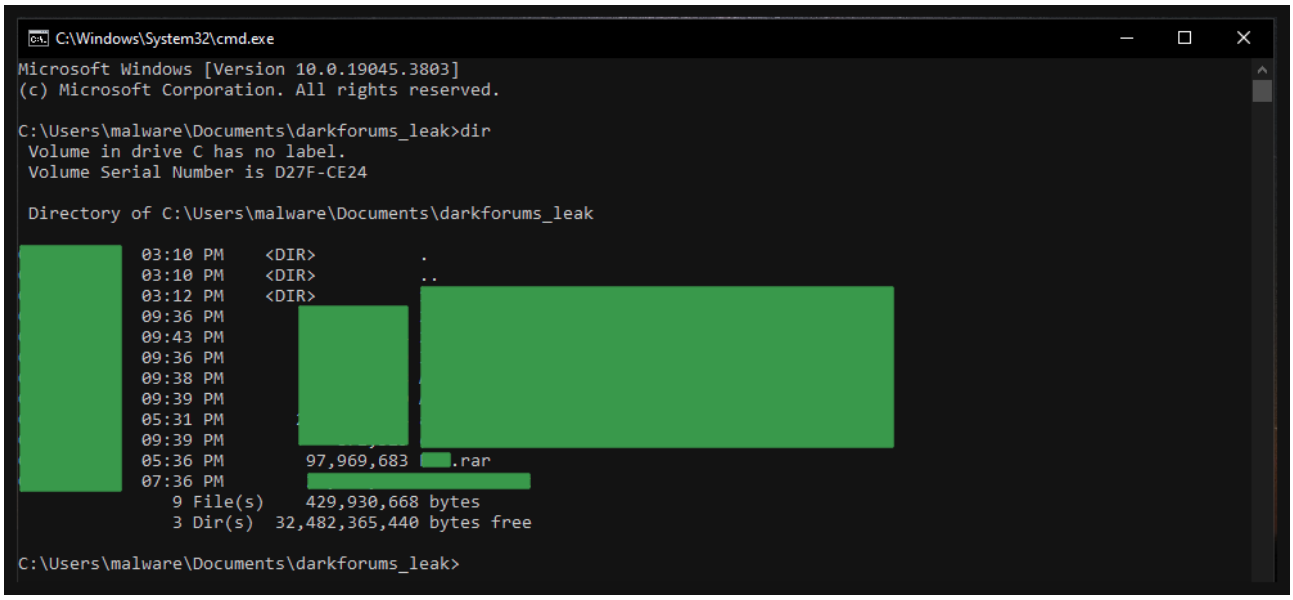
En esta sección del informe estaremos analizando y verificando si nuestra muestra del archivo descargado del foro de filtración de datos posee alguna indicio de malware previamente a descomprimirlo y visualizar los datos.

5.1 Transferencia de archivos a VM

El primer paso es transferir nuestro archivo de muestra .RAR a la maquina virtual de análisis de malware. En nuestro caso utilizaremos un pendrive para compartir la información.

Cabe destacar que el laboratorio de análisis de malware es una maquina virtual aislada y securizada específicamente para investigar archivos maliciosos. Pueden visualizar mi articulo publicado en mi blog donde explico como montar/instalar un laboratorio virtual para análisis de archivos desde cero.

Articulo: https://www.davidpadron.info/blog_articles/config_static_malware_lab.pdf



5.2 Metodología de Análisis Estático (RAR)

Como segundo paso utilizare mi propia metodología de análisis de malware que consta de las siguientes 7 fases (*Creación de directorios de trabajo, Hashing, Identificación Real del*

Archivo, Magic Bytes, Entropía, Strings e Inspección del Contenido). Pueden visualizar mi articulo publicado en mi blog para ver el paso a paso de mi metodología.

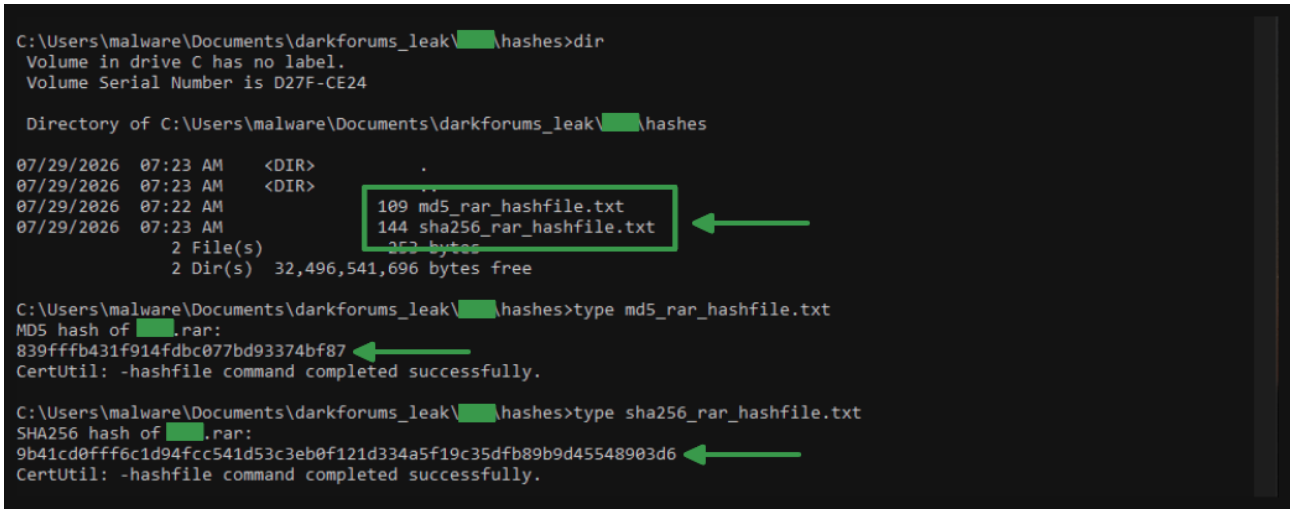
Articulo: https://www.davidpadron.info/blog_articles/static_analysis_deep_web_file.pdf

5.2.1 FASE 1 — Creación de directorios de trabajo



5.2.2 FASE 2 — Hashing

Calcular los hashes (MD5, SHA1, SHA256) de nuestro archivo .RAR y almacenarlo en el directorio “hashes”.



Hashes del archivo .RAR:

MD5: 839fffb431f914fdbc077bd93374bf87

SHA256: 9b41cd0fff6c1d94fcc541d53c3eb0f121d334a5f19c35dfb89b9d45548903d6

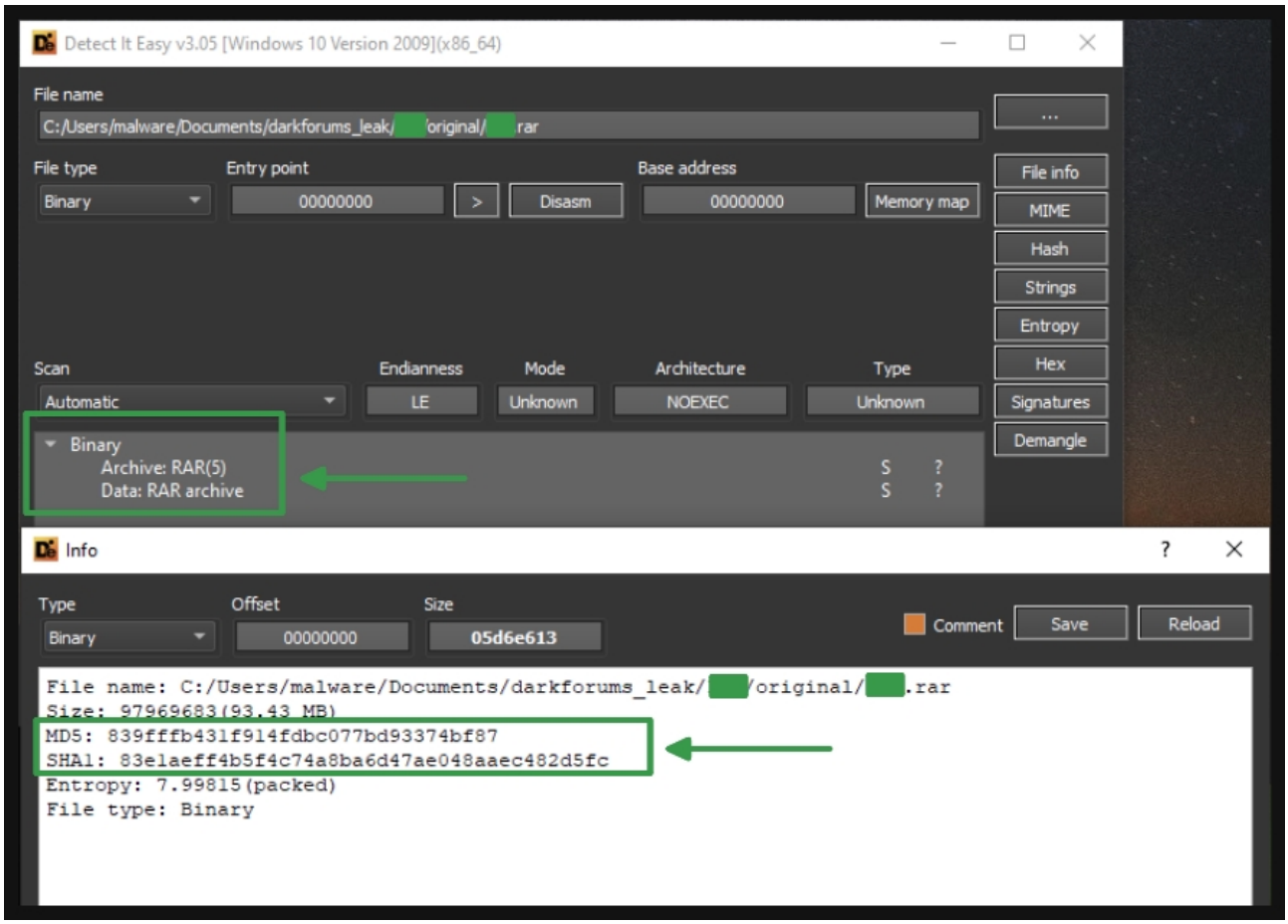
5.2.3 FASE 3 — Identificación Real del Archivo

Identificar el tipo de archivo real mediante la visualización del valor del encabezado

(PE32, ELF, Mach-O, Archive, Text, Binary).

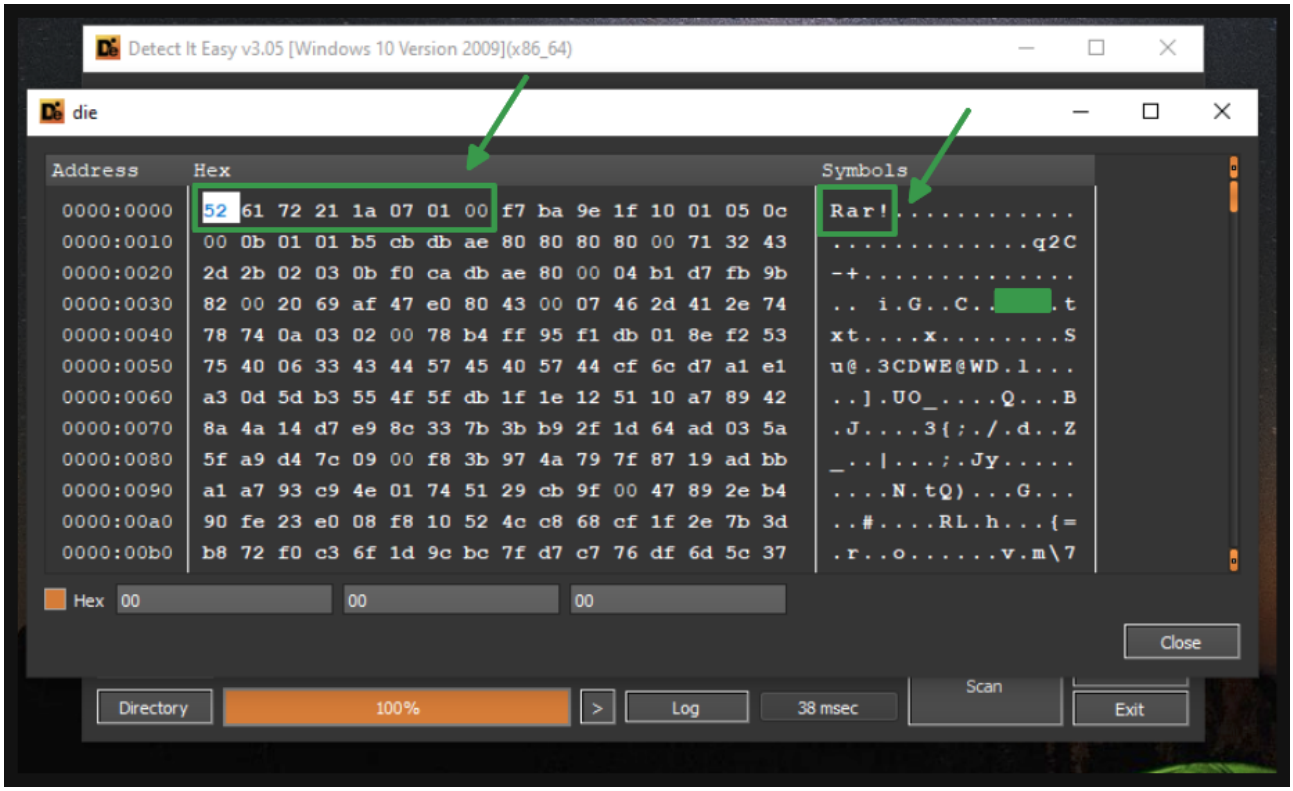
Para este caso particular la herramienta “Detect It Easy” identifica que nuestro archivo es un binario enpaquetado .RAR.

También podemos apreciar en el apartado “Info” que la herramienta nos proporciona los mismos hashes que almacenamos en nuestro directorio de trabajo `hashes/`.



5.2.4 FASE 4 — Magic Bytes

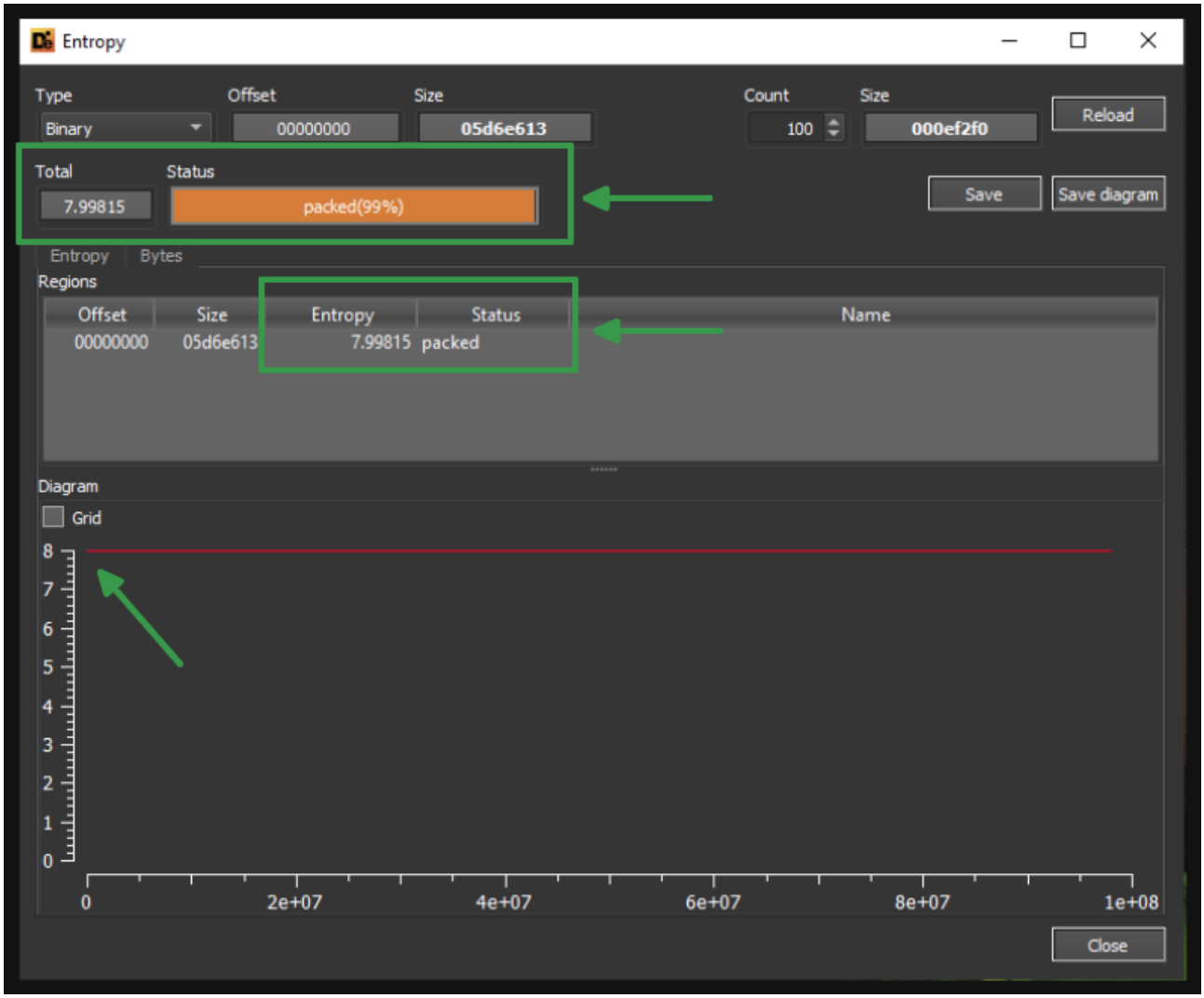
Verificar el valor de la cabecera de los “Magic Numbers” o “Magic Bytes”.



En nuestro caso el tipo de cabecera pertenece a el “Magic Number” de un archivo RAR5 (HEX `52 61 72 21 1A 07 01 00`, Roshal ARchive compressed archive v5.00 onwards) .

5.2.5 FASE 5 — Entropía

Analizar la entropía del archivo.

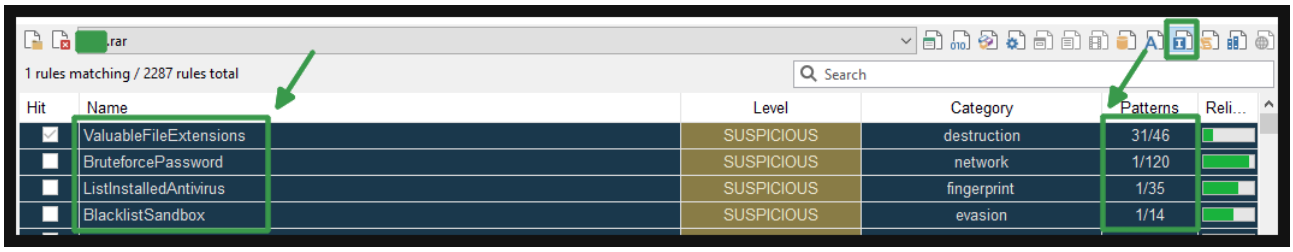


El archivo analizado posee un entropía extremadamente alta ya que es un archivo .RAR de compresión. Probablemente el sujeto utilizo la máxima compresión al momento de comprimir este archivo.

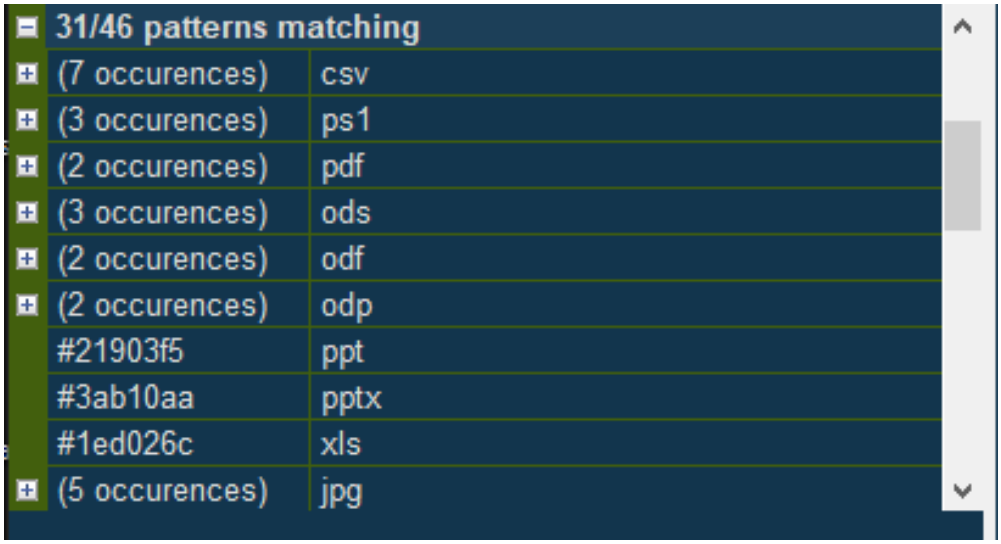
5.2.6 FASE 6 — Strings

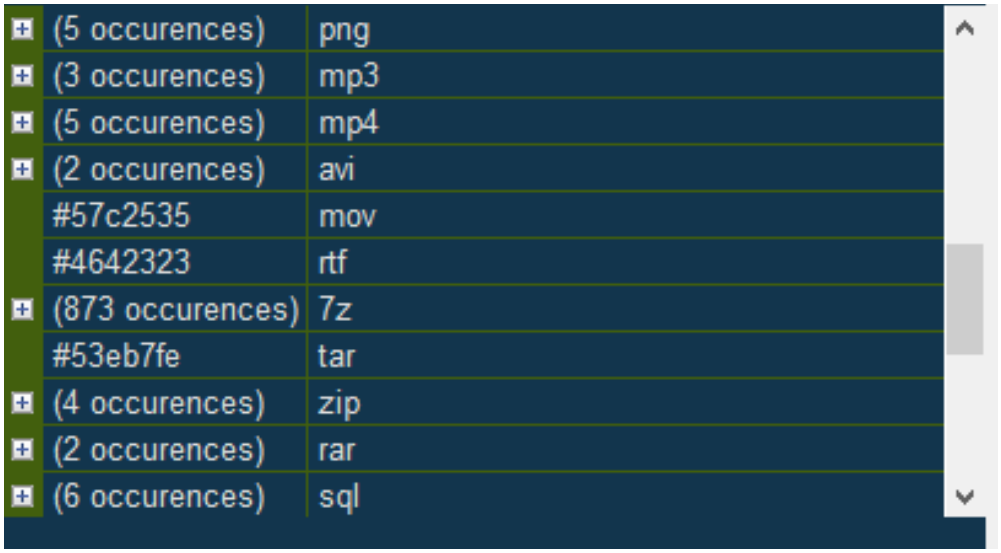
Analizar el archivo mediante un visualizador de strings para identificar cadenas de texto sospechosas.

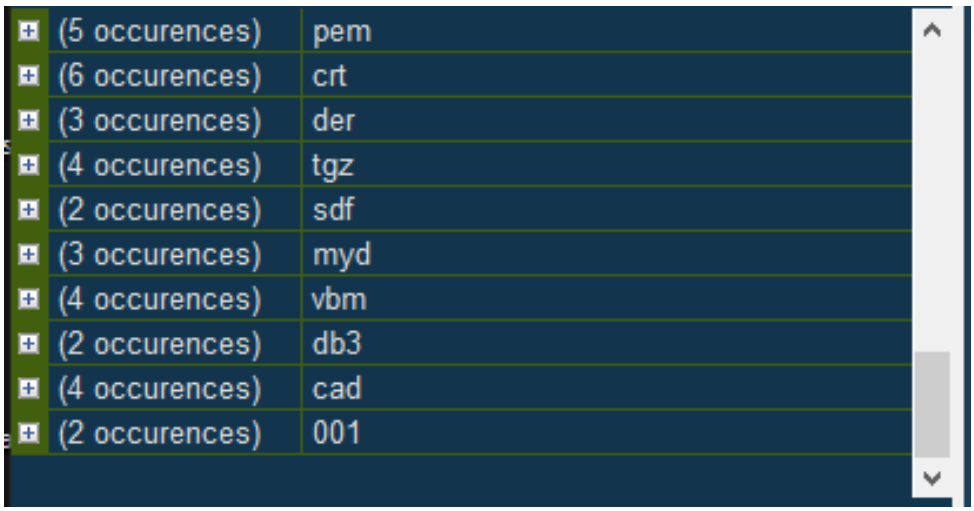
El análisis de “strings” del archivo .RAR mediante la herramienta “*Malcat*” detecto presencia de actividad sospechosa relacionada a múltiple enumeración de extensiones de archivos, un fingerprint de antivirus, contraseña de fuerza bruta y fingerprint de técnica de evasión de sandbox.



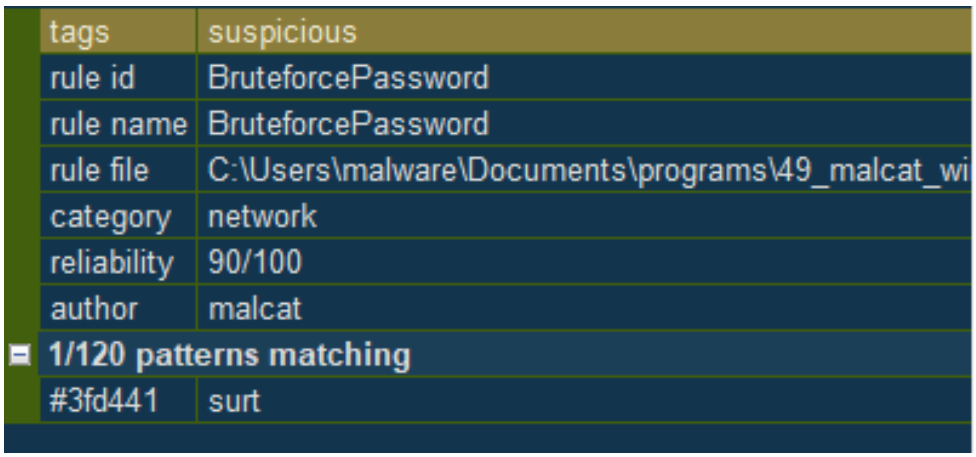
Enumeración de extensiones de archivos:



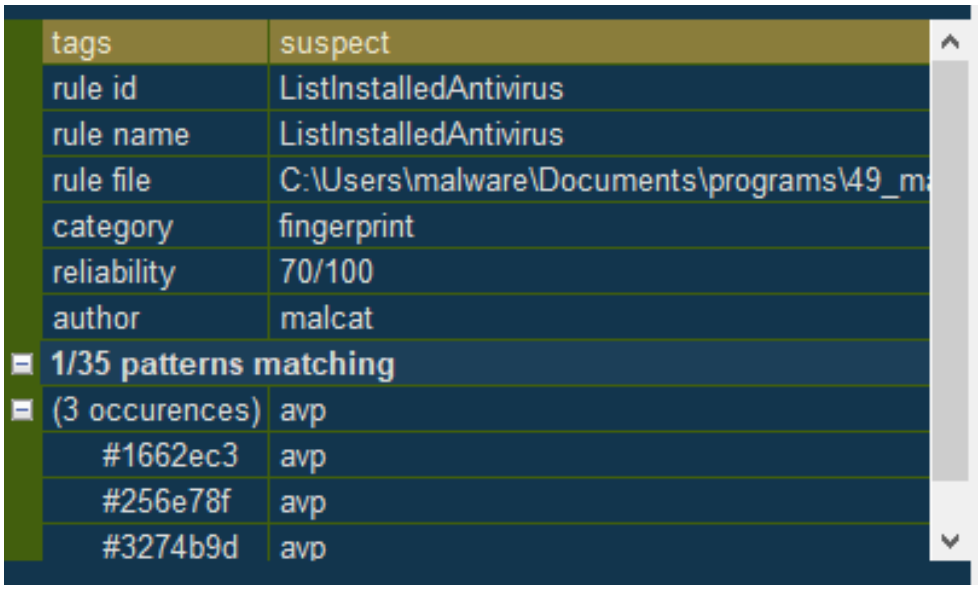




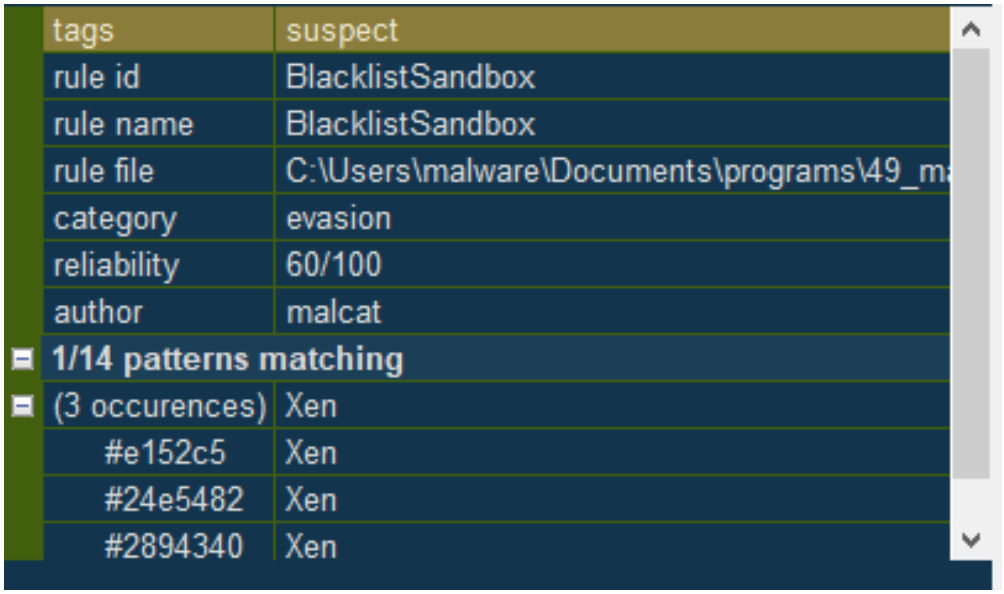
Contraseña de fuerza bruta:



Fingerprint de antivirus:



Técnica de evasión de sandbox:



5.2.7 Interpretación y Conclusión

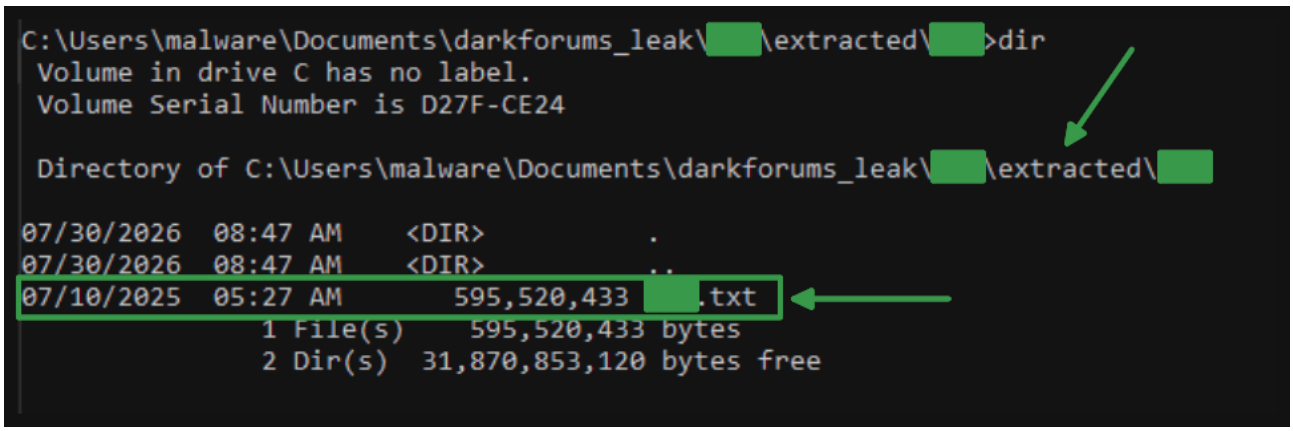
El análisis estático sobre el archivo .RAR demuestra que el archivo efectivamente es un binario no ejecutable tipo RAR5 con entropía extremadamente alta (7.99815) pero normal en archivos comprimidos. La interpretación sobre la presencia de enumeración de extensiones de archivos, fuerza bruta, fingerprint de antivirus y evasión de sandbox las podemos aludir a que el archivo .TXT que alberga el .RAR puede llegar a contener este tipo de cadenas y el software Malcat lo detecta como sospechoso y un posible falso positivo. Sin embargo con la evidencia disponible, no veo indicadores sólidos que permitan clasificar el RAR como malicioso ya que un archivo RAR no es un binario ejecutable.

El siguiente paso sera descomprimir el RAR y volver a realizar un análisis estático sobre el archivo TXT en busca de anomalías.

5.3 Metodología de Análisis Estático (TXT)

5.3.1 FASE 1 — Creación de directorios de trabajo

Este paso ya fue ejecutado en el análisis anterior. Ahora tenemos que descomprimir el archivo RAR y almacenar el TXT dentro de la carpeta “extracted”.



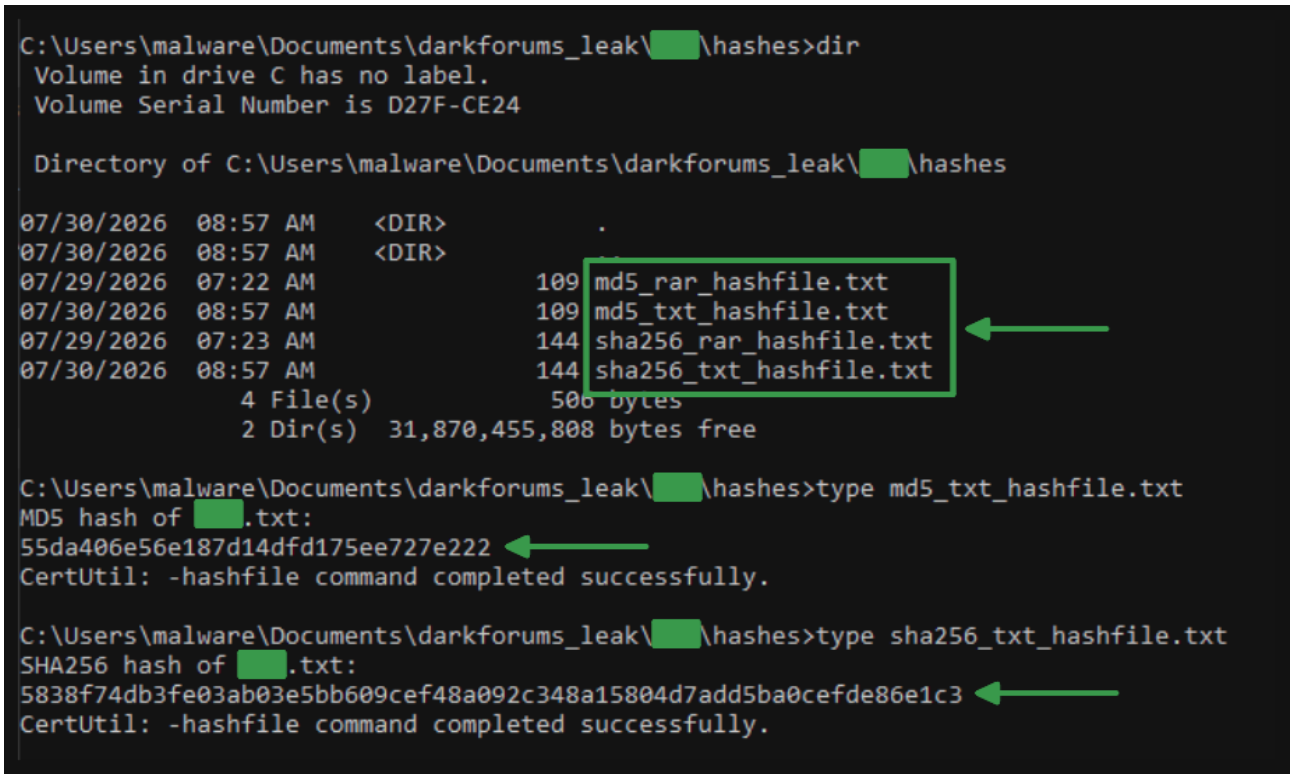
5.3.2 FASE 2 — Hashing

Calcular los hashes (MD5, SHA1, SHA256) de nuestro archivo .TXT y almacenarlo en el directorio “hashes”.

Hashes archivos TXT:

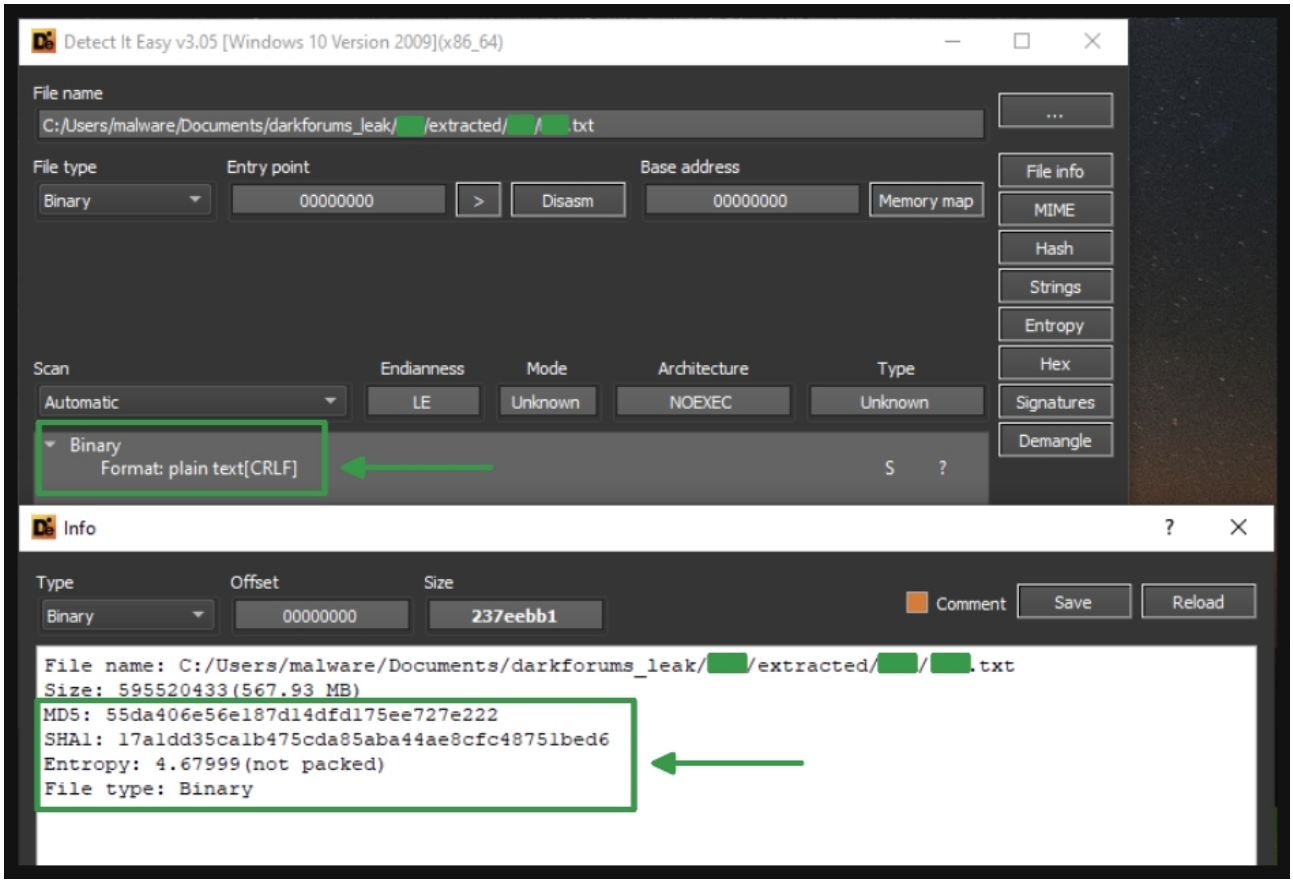
MD5: 55da406e56e187d14dfd175ee727e222

SHA256: 5838f74db3fe03ab03e5bb609cef48a092c348a15804d7add5ba0cefde86e1c3



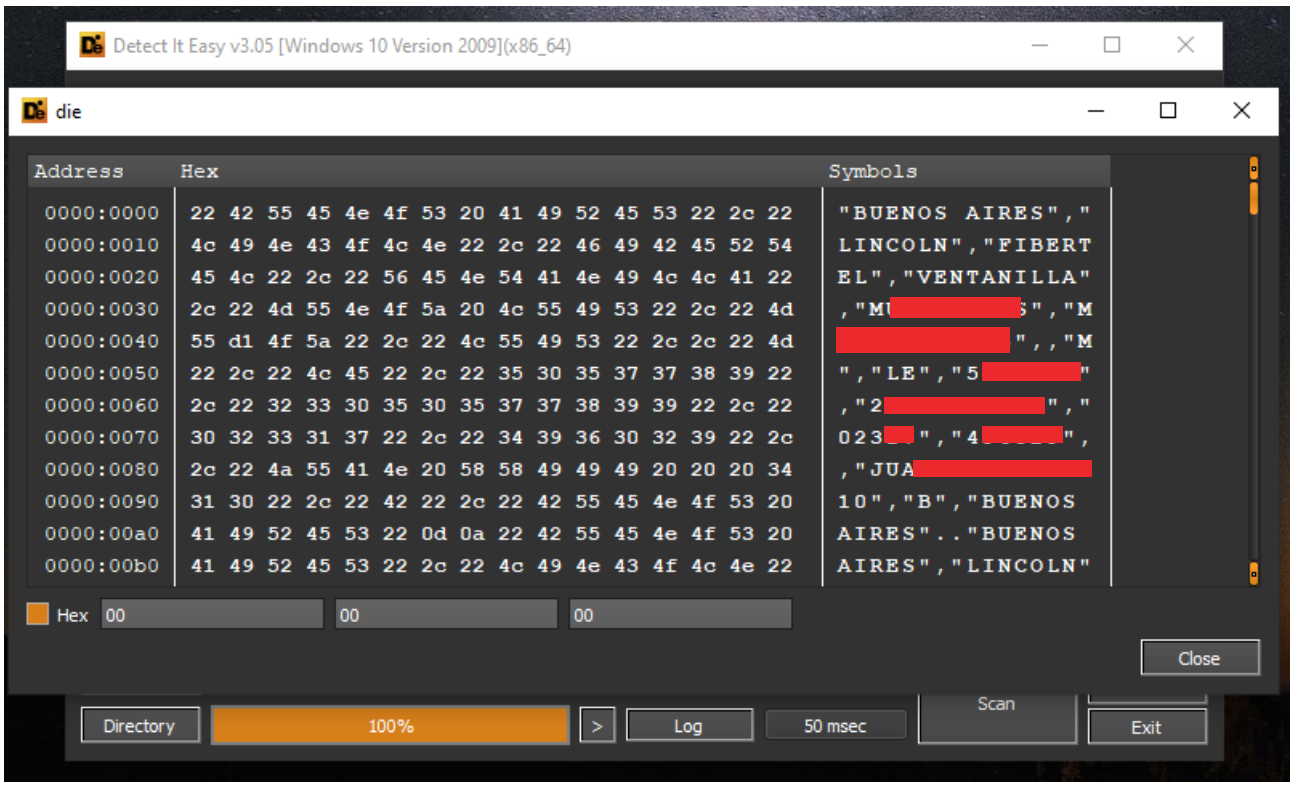
5.3.3 FASE 3 — Identificación Real del Archivo

El tipo de archivo identificado es un archivo de formato texto plano (TXT).



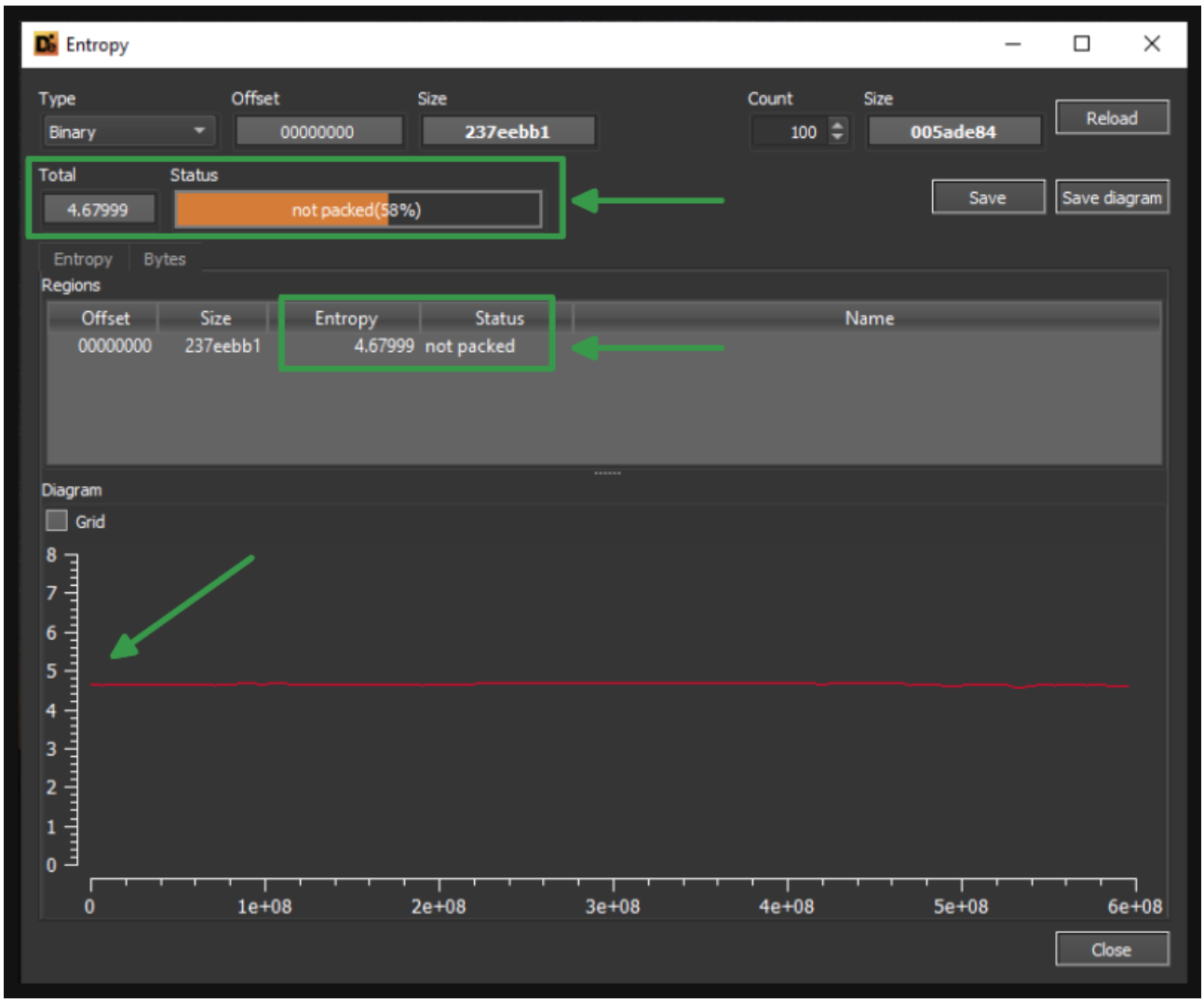
5.3.4 FASE 4 — Magic Bytes

Los archivos de texto plano (TXT) no tienen un número mágico (Magic Number). Dado que estos consisten únicamente en datos de caracteres sin procesar (como ASCII o UTF-8).



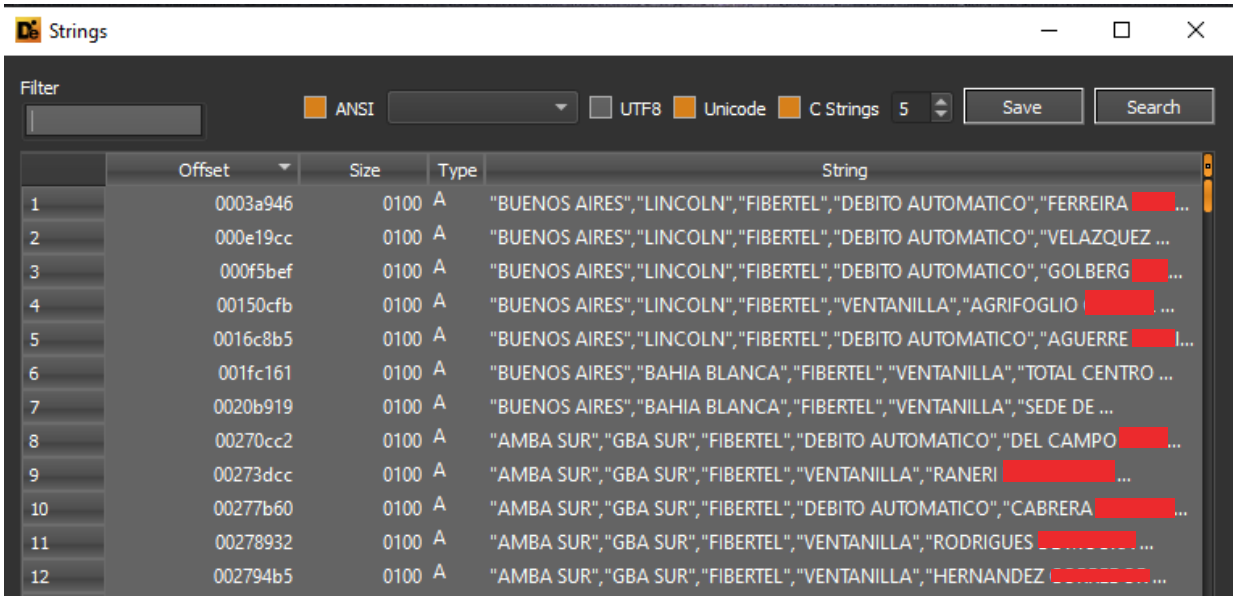
5.3.5 FASE 5 — Entropía

Nuestro archivo de texto plano (TXT) posee baja entropía (4.67999) y está catalogado sin compresión (Not packed).



5.3.6 FASE 6 — Strings

No se identificaron cadenas sospechosas o maliciosas.

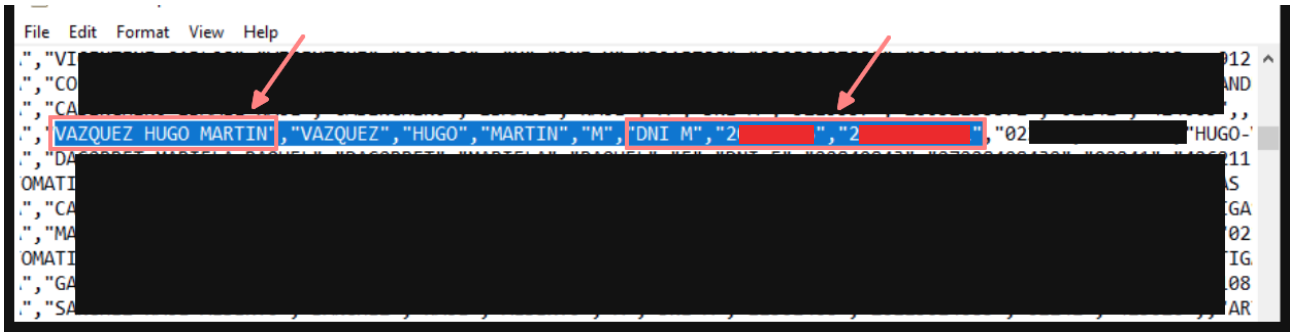


Análisis de la filtración

6. Visualización del archivo

6.1 FASE 7 — Inspección del Contenido

Finalizada la etapa de análisis de malware sobre el archivo descargado del foro darkforums, se concluye que el archivo es apto para ser visualizado mediante un visor de datos en texto plano y analizar los datos que se encuentran dentro.



Como resultado extraeremos una muestra de un registro del archivo TXT para verificar si los datos personales expuestos son verdaderos o falsos mediante técnicas de Investigación de fuentes abiertas (OSINT).

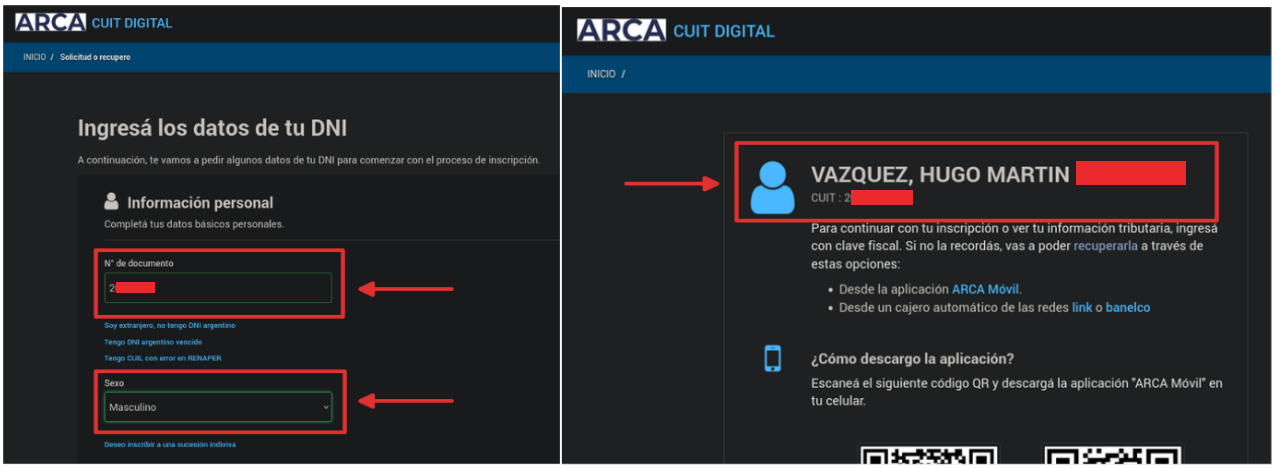
Muestra de filtración de datos:

"AMBA SUR", "LA PLATA", "FIBERTEL", "VENTANILLA", "VAZQUEZ HUGO MARTIN", "VAZQUEZ", "HUGO", "MARTIN", "M", "DNI M", "2[redacted]", "2[redacted]", "02241", "5[redacted]", "H[redacted]@HOTMAIL.COM", "A[redacted]4", "B", "BUENOS AIRES"

Validación mediante OSINT

7. Validación de Identidad

Validamos que la identidad del sujeto expuesta en el *sample* “*Vazquez Hugo Martin*” de genero masculino con DNI “*2[redacted]*” es un registro valido dentro de la base de datos del servicio gubernamental ARCA.

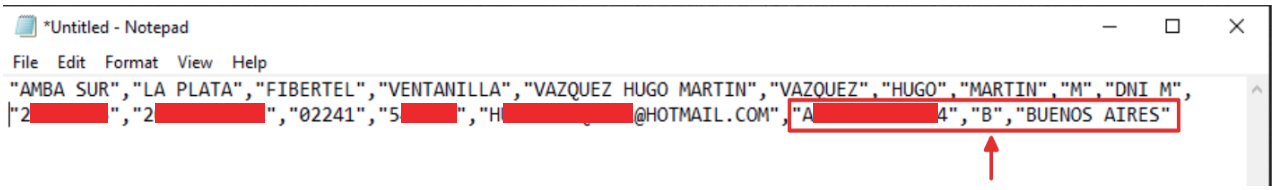


Nombre	**CUIT**	**Edad**	**Provincia**	**Ciudad**
Vazquez Hugo Martin [redacted]	2[redacted]	[redacted]	Buenos Aires (Pcia)	Chacomús

8. Validación de Domicilio

8.1 Muestra del archivo extraído:

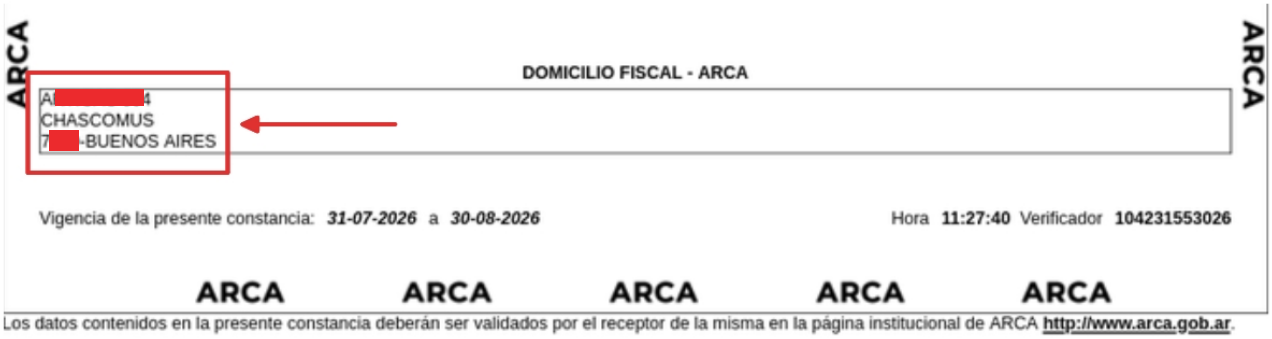
Dirección: A[redacted]4, Buenos Aires, Argentina



8.2 Domicilio Fiscal:

Obtención del domicilio fiscal por medio del servicio web de ARCA.

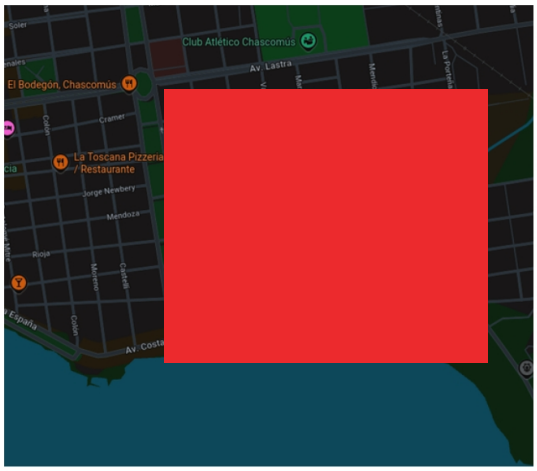
Dirección: A[redacted]4, Chascomus B7[redacted], Buenos Aires, Argentina



8.3 Ubicación Google Maps:

Dirección: A[redacted]4, B7[redacted] Chascomús, Provincia de Buenos Aires, Argentina

Coordenada: -3[redacted], -5[redacted]

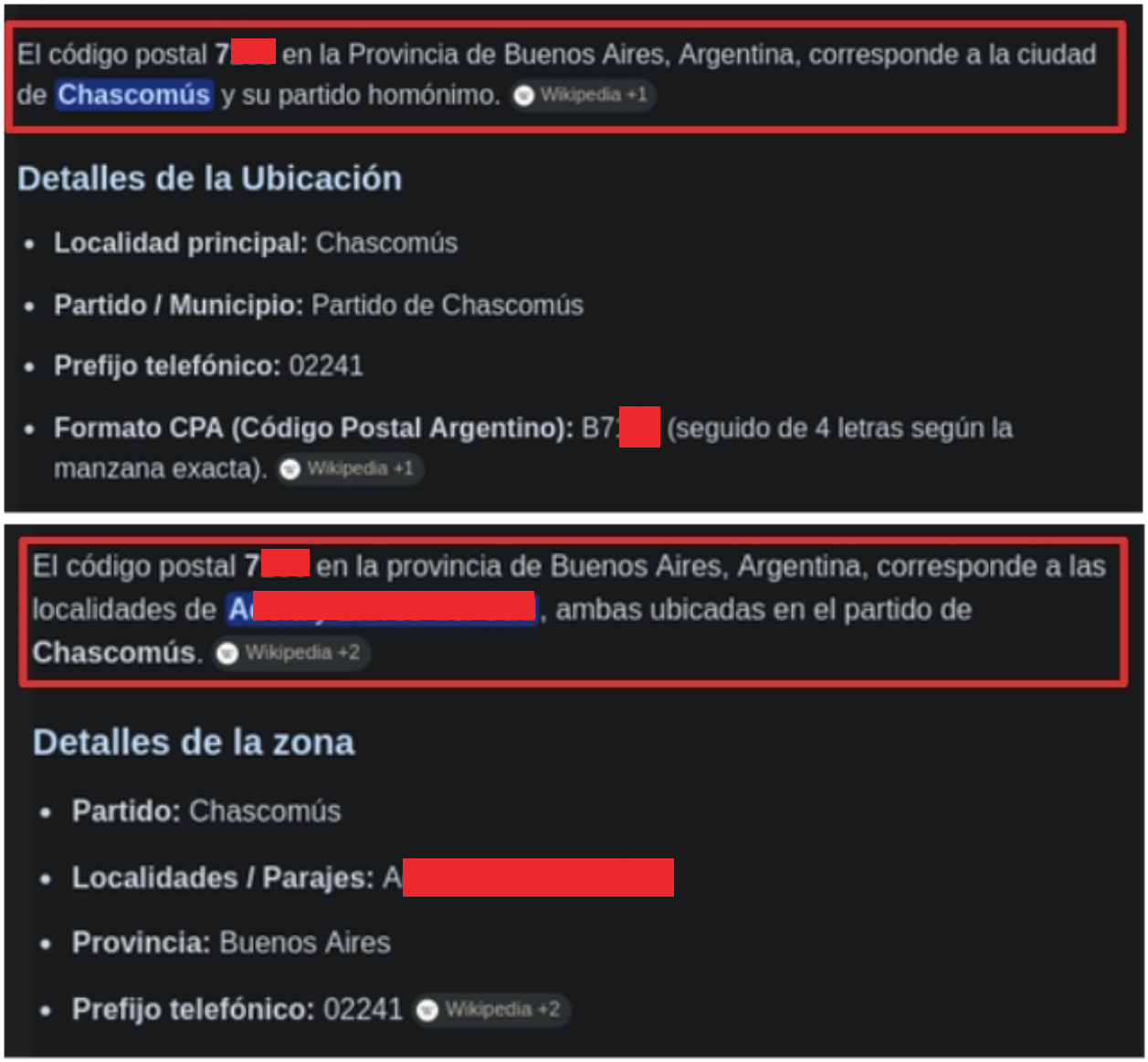




8.4 Interpretación

La dirección extraída del archivo de filtración coincide con la dirección obtenida por medio de la consulta del domicilio fiscal en ARCA y la búsqueda en Google Maps.

Se aprecia una diferencia con respecto a los códigos postales proporcionados por el servicio de ARCA y Google Maps pero ambos códigos postales pertenecen a zonas del partido de Chascomús, Buenos Aires, Argentina.



8.5 Conclusión

En primera instancia se verifica que la dirección del domicilio (A 4, Buenos Aires, Argentina) del sujeto “*Vazquez Hugo Martin*” expuesta en el archivo de filtración es verdadera.

9. Validación Número de Teléfono

9.1 Muestra del archivo extraído

Teléfono: 02241-5[redacted]



9.2 Número de teléfono

Número de teléfono: 022415[redacted]

Internacional: +5422415[redacted]

País: Argentina (+54)

Localidad: Chascomús, Pcia de Bs As, Argentina

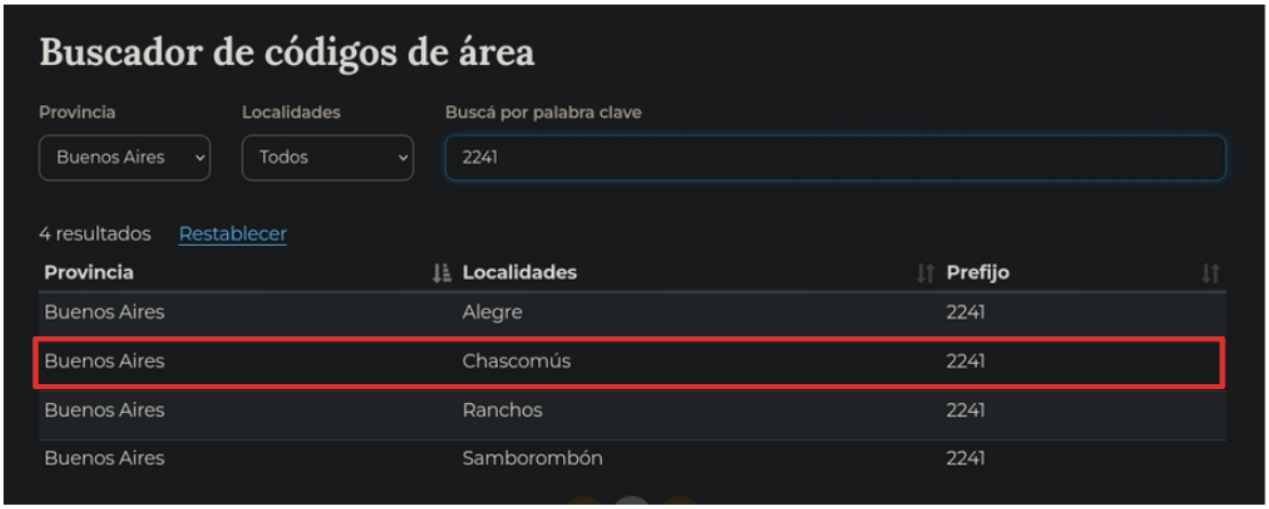
Servicio: Servicio móvil celular

Servicio de telefonía: Personal (probabilidad media)

Whatsapp: Si

9.3 Código de área telefónico

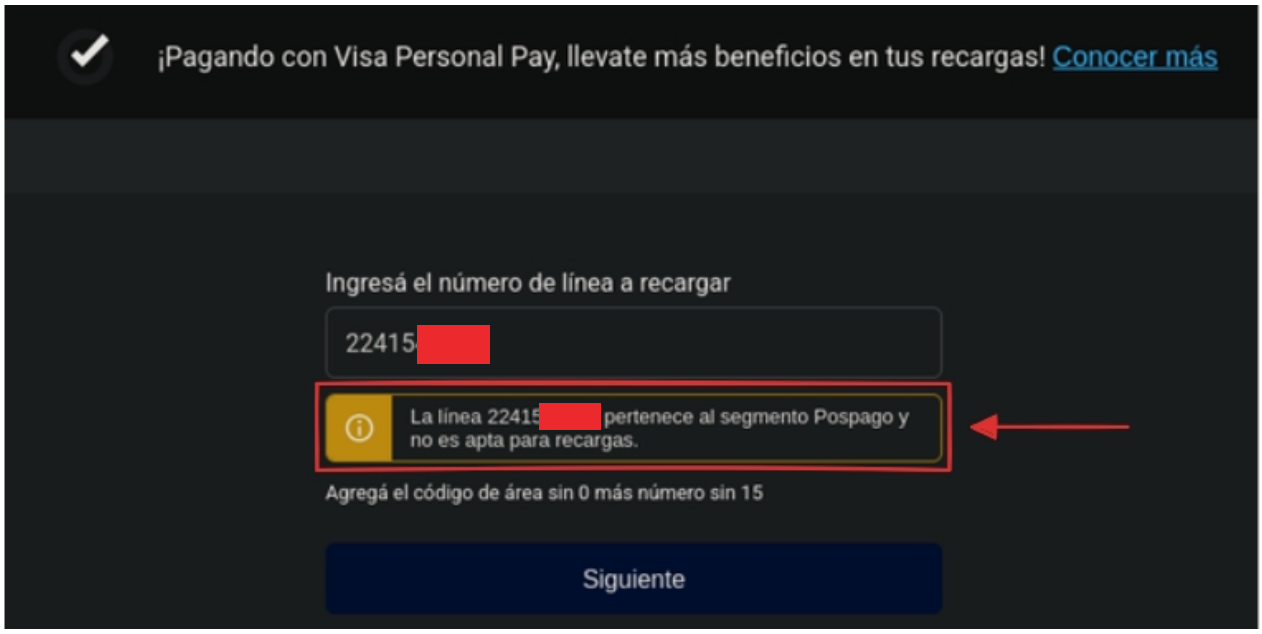
Código de área: 2241



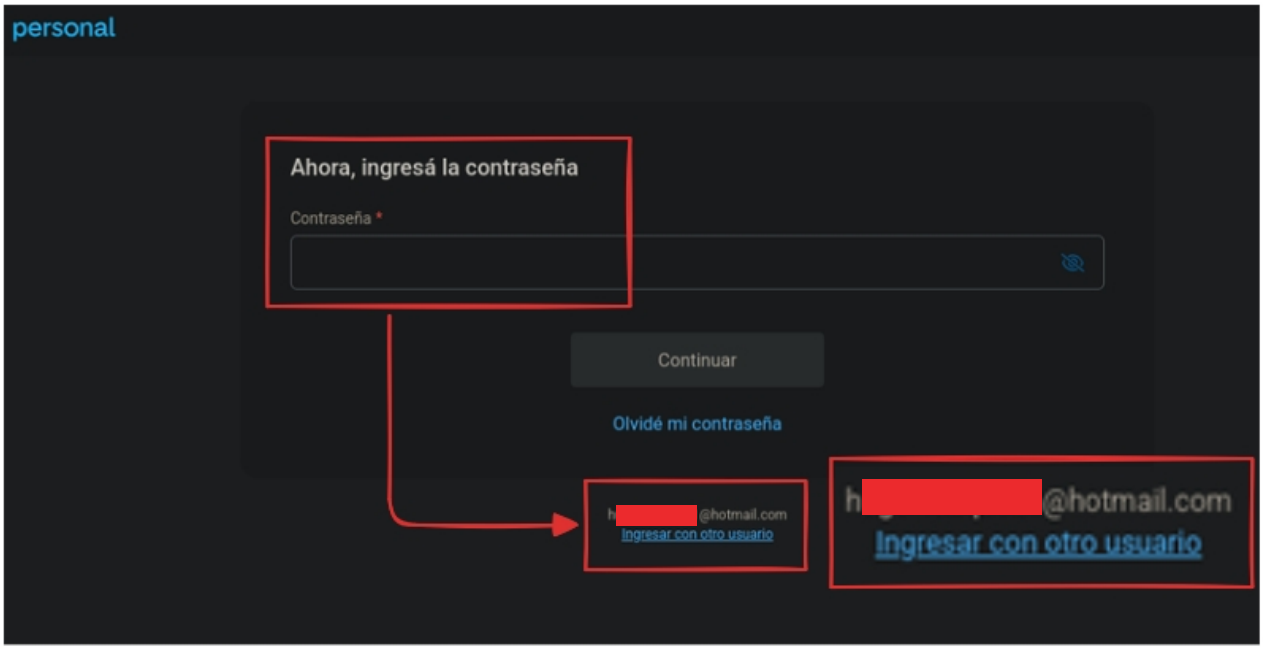
Fuente: https://www.argentina.gob.ar/pais/codigo-telefonia

9.4 Telefonía móvil Personal

La línea de teléfono (*22415*[redacted]) se encuentra aparentemente registrada en la categoría de Postpago (Plan de abono) del portal de Personal Argentina.

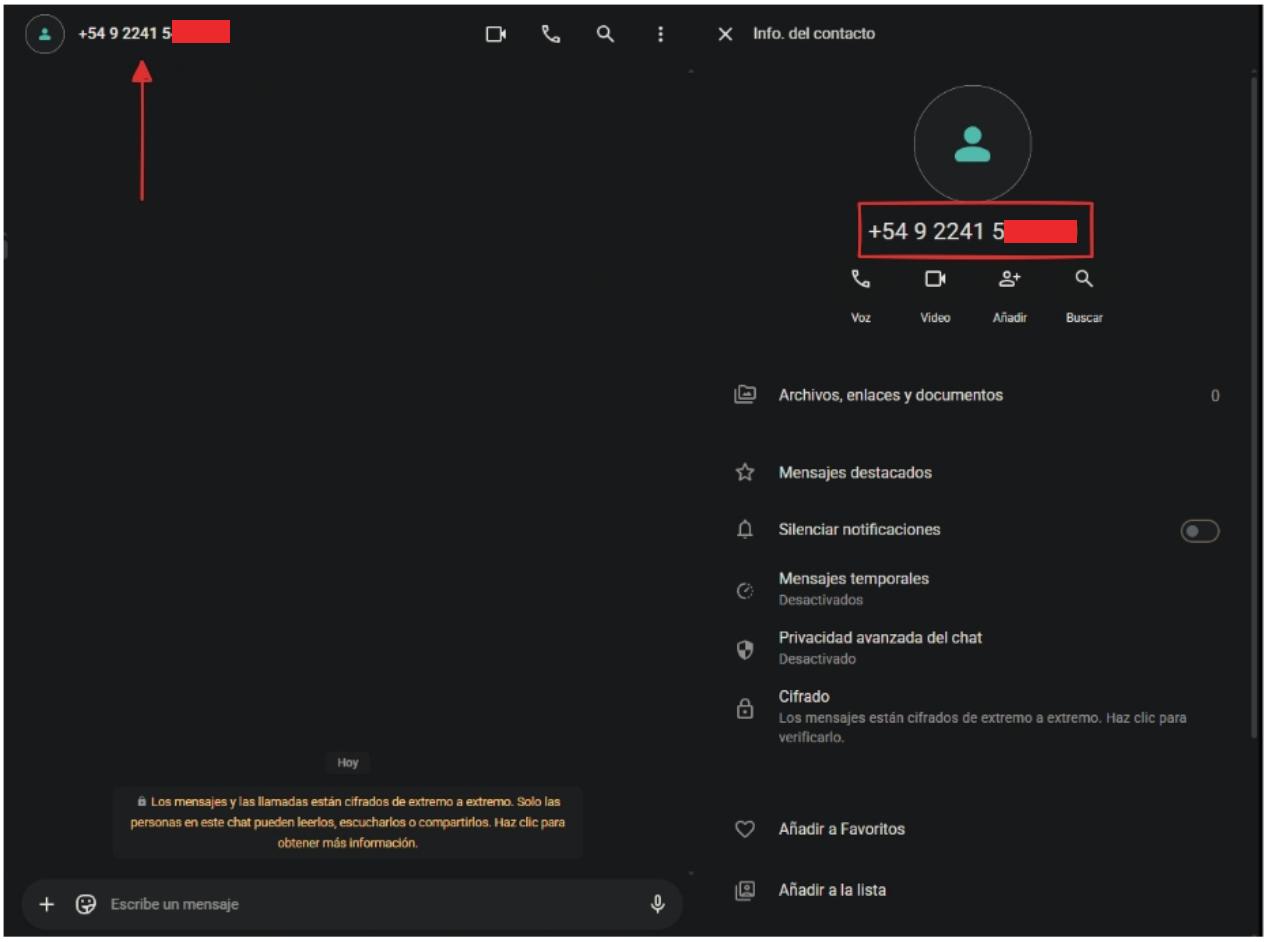


La dirección de correo electrónico (*h*[redacted]*@hotmail.com*) se encuentra aparentemente registrada dentro de la base de datos del portal de Personal Argentina.



9.5 Verificación Whatsapp

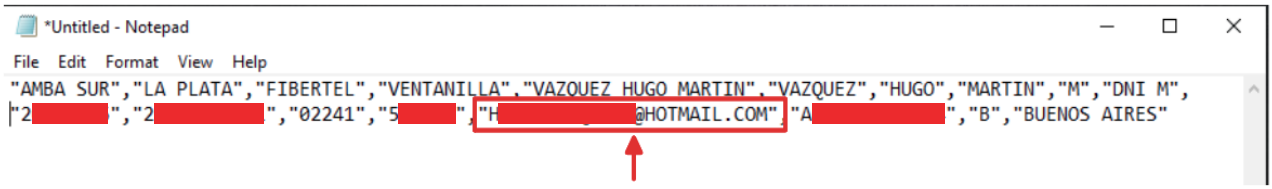
El número de teléfono (*22415*[redacted]) posee registro activo en el servicio de mensajería Whatsapp. Sin embargo no podemos aseverar que el número de teléfono siga perteneciendo a la misma persona.



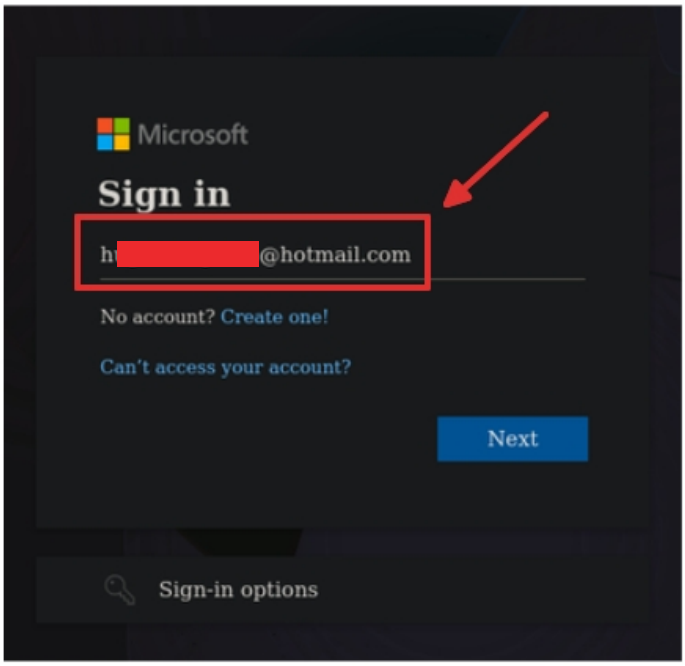
10. Validación Correo Electrónico

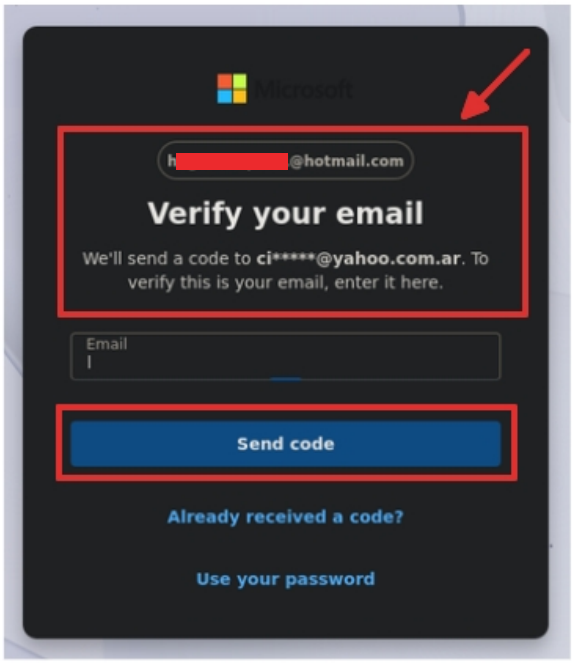
10.1 Muestra del archivo extraído

Email: h[redacted]@hotmail.com



10.2 Microsoft Hotmail - Outlook





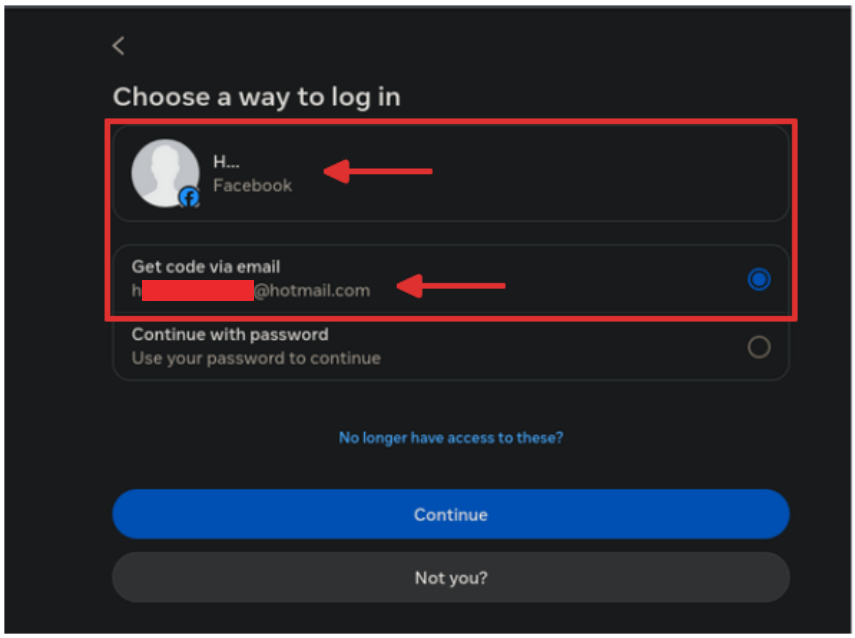
Se valido que la dirección de correo electrónico (*h[redacted]@hotmail.com*) es un registro activo para el servicio de login de Microsoft y acceso a Hotmail/Outlook.

En este caso en particular cuando se intenta acceder con el correo solicita una verificación adicional a la siguiente dirección (ci*****@yahoo.com.ar).

11. Validación Redes sociales

11.1 Facebook (Email)

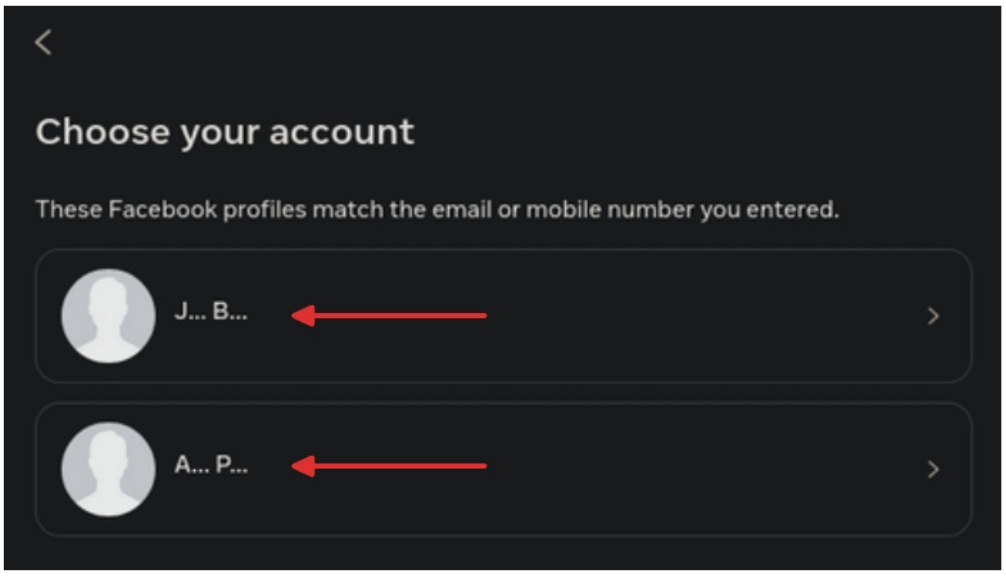
Email: h[redacted]@hotmail.com



Se valido que la dirección de correo electrónico (*h[redacted]@hotmail.com*) es un registro activo para el servicio de login de la red social Facebook.

11.2 Facebook (Teléfono)

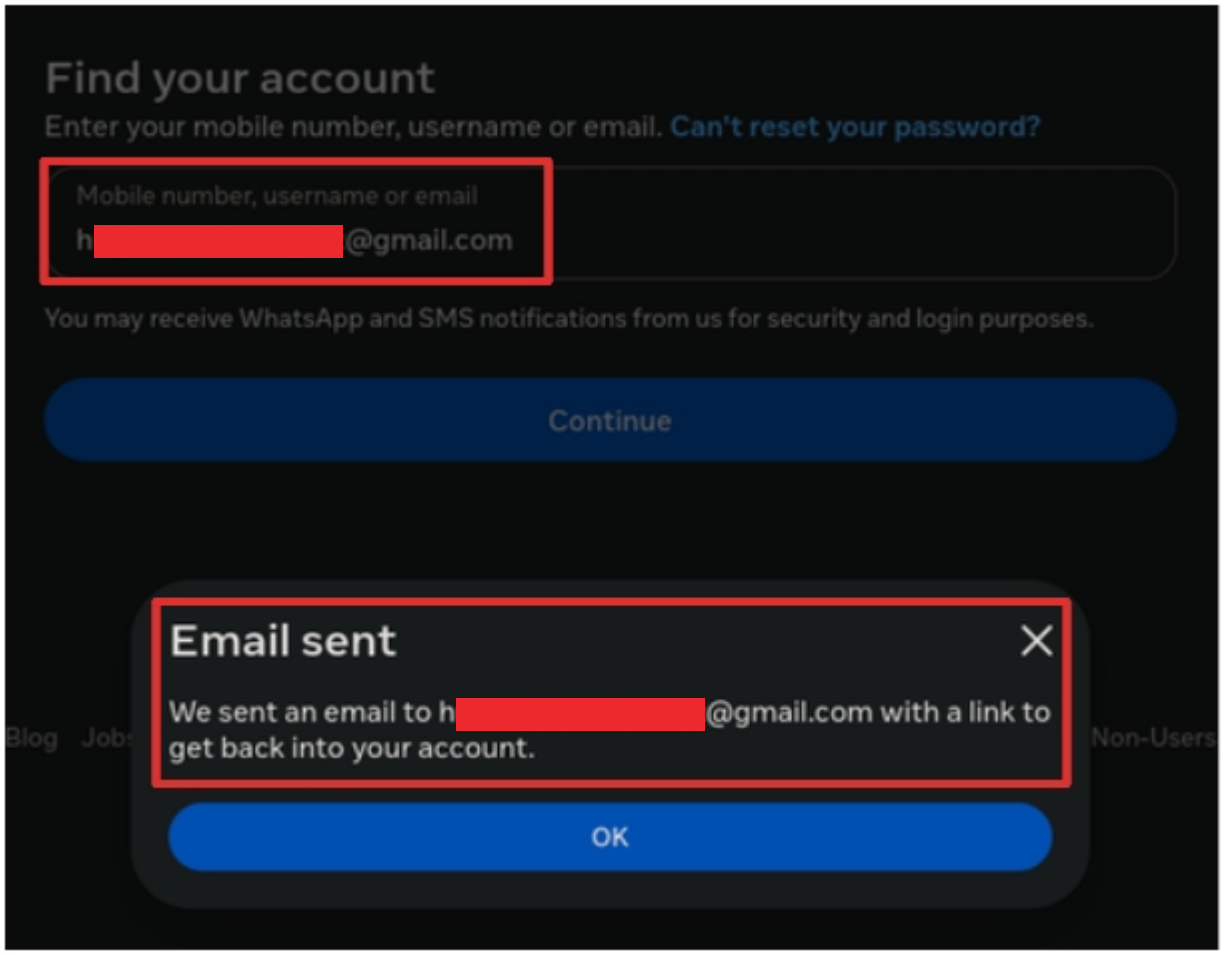
Teléfono: 22415[redacted]



Se valido que el número de teléfono (*22415[redacted]*) esta asociado a el registro de 2 cuentas de Facebook para realizar login.

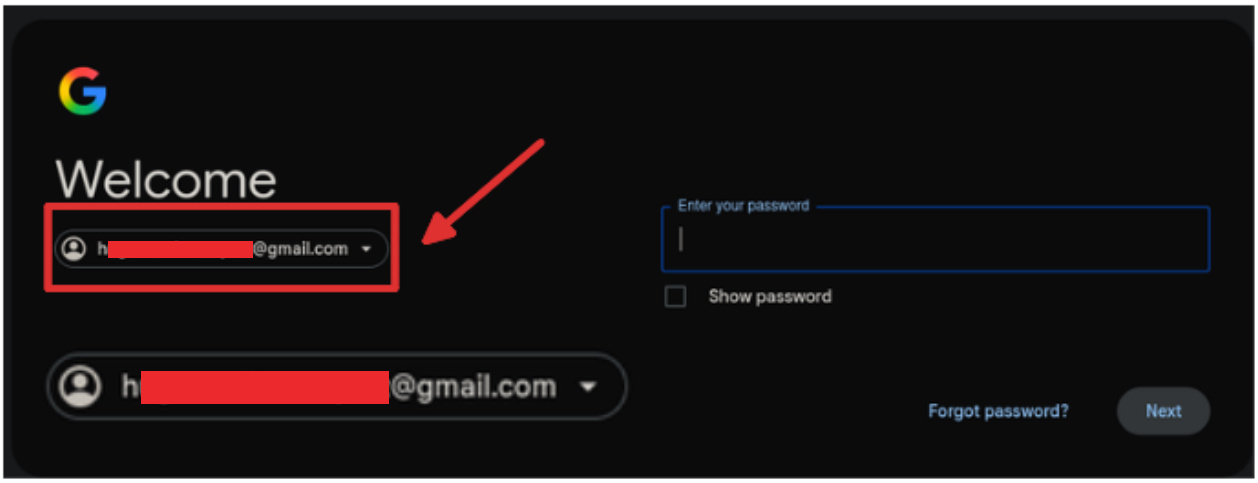
11.3 Instagram (Email)

Email: h[redacted]@gmail.com



12. Validación Google

Email: h[redacted]@gmail.com



Se valido que la siguiente dirección de correo electrónico (*h[redacted]@gmail.com*) esta asociado al registro del servicio de Google.

13. Validación servicio energía

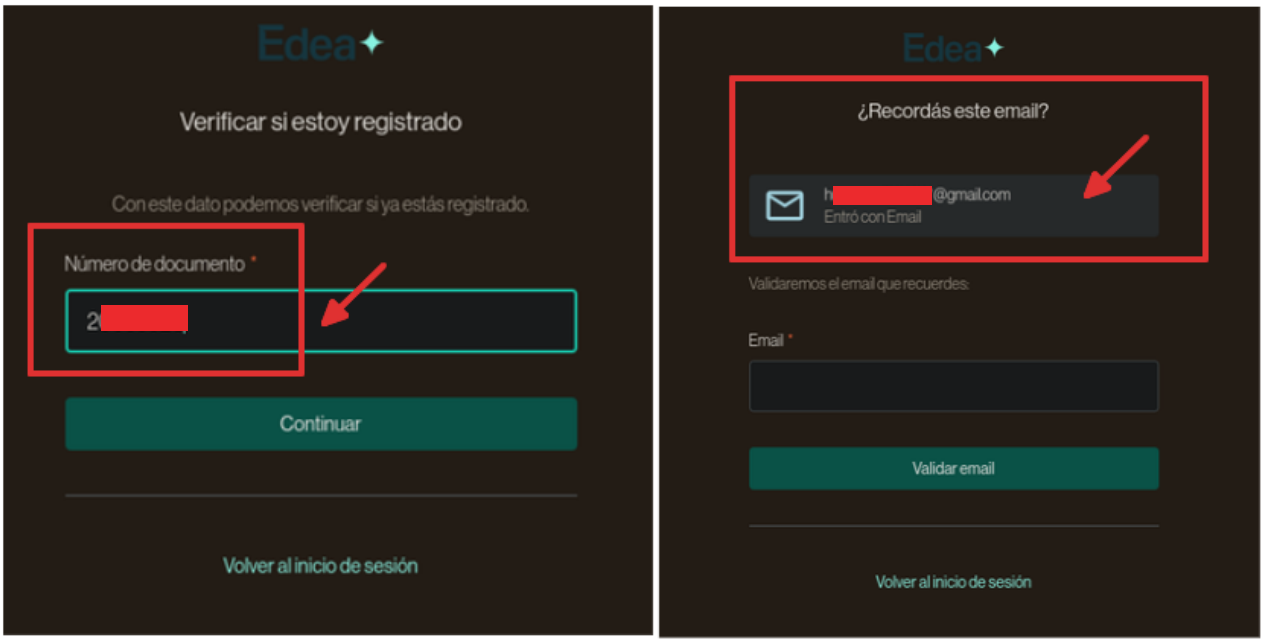
13.1 Servicio energía eléctrica

El proveedor de energía eléctrica para la ciudad de Chascomús, Pcia de Buenos Aires, Argentina es la empresa EDEA S.A.

Validación de registro en plataforma web:

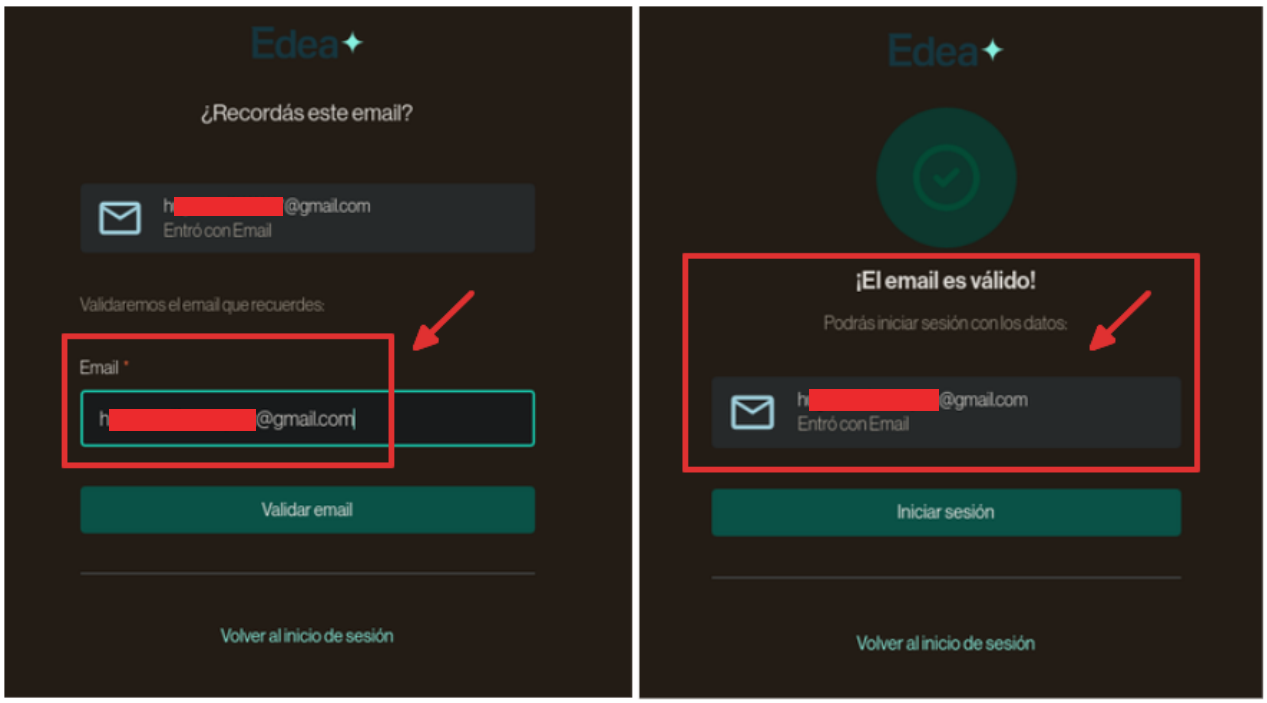
Validamos el registro del sujeto (*Vazquez Hugo Martin* [redacted]) mediante su DNI (*2*[redacted]).

URL: https://oficinavirtual.edeaweb.com.ar/ingreso



Validación del correo electrónico:

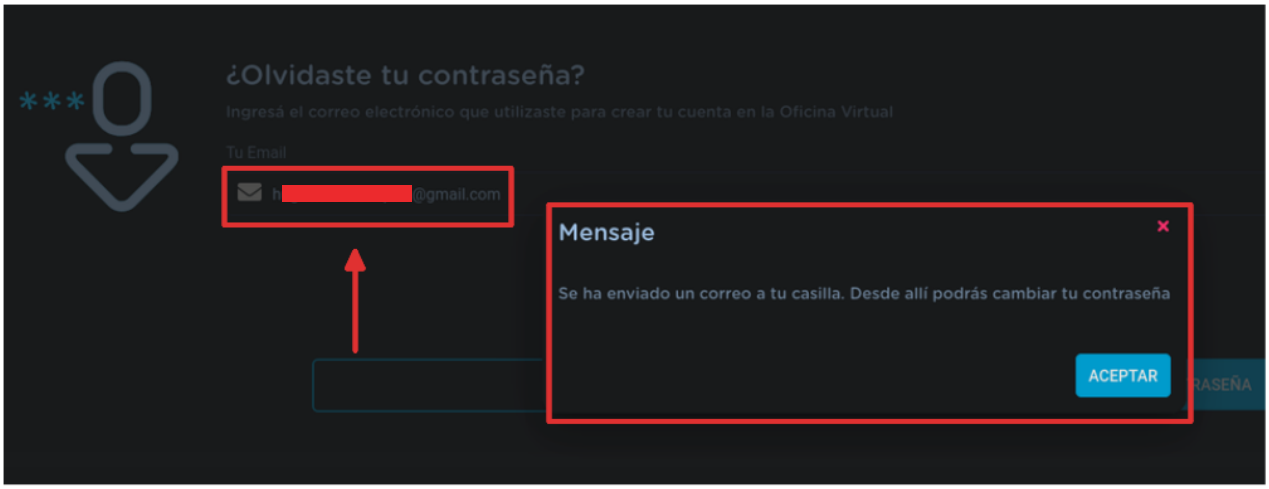
Se valido que la dirección de correo electrónico provista parcialmente por EDEA S.A del sujeto con DNI (*2*[redacted]) es: h[redacted]@gmail.com.



13.2 Servicio gas natural

El proveedor de gas natural para la ciudad de Chascomús, Pcia de Buenos Aires, Argentina es la empresa Camuzzi Gas Pampeana.

Se valido que el sujeto (*Vazquez Hugo Martin* [redacted]) posee una cuenta registrada en el portal web de la empresa de gas natural Camuzzi Gas Pampeana con la dirección de correo electrónico h[redacted]@gmail.com.



Conclusión

14. Conclusión del análisis de inteligencia

A partir del proceso de investigación, recopilación, correlación y validación de información de fuentes abiertas (OSINT), se concluye que la muestra de datos identificada en el foro de la clearnet **DarkForums**, asociado al dominio *darksforums.ru*, presenta indicios relevantes de contener información personal correspondiente a ciudadanos argentinos reales. Asimismo, las características estructurales de los registros analizados permiten plantear la hipótesis de que la información podría proceder de una base de datos vinculada a un servicio comercial de telecomunicaciones, con una posible relación con los servicios prestados por **Fibertel S.A.**

No obstante, desde una perspectiva estrictamente investigativa, **no es posible atribuir de manera concluyente la titularidad de la base de datos filtrada a Fibertel S.A. únicamente a partir de la muestra examinada**. Si bien determinados campos, como la identificación de la marca, la información geográfica y los datos asociados a un supuesto registro de cliente, resultan compatibles con esta hipótesis, la confirmación de su procedencia requiere una instancia de análisis conjunto con los responsables técnicos de la organización. En particular, sería necesario correlacionar los registros obtenidos con las bases de datos, los sistemas de información y los registros históricos de la infraestructura corporativa, a fin de determinar su correspondencia, procedencia y posible alcance.

El análisis preliminar de la muestra permite observar una estructura de datos compatible con registros individuales de clientes, incluyendo campos relativos a la región geográfica, localidad, marca comercial, modalidad de atención, nombre y apellido, número de documento, identificadores adicionales, información de contacto y domicilio. Esta composición constituye un indicador de interés para la investigación, dado que podría corresponder a información almacenada en una base de datos operativa o comercial. Sin embargo, la estructura de los registros, por sí sola, no permite determinar el sistema de origen ni establecer si los datos fueron obtenidos directamente de la infraestructura de Fibertel S.A. o a través de una fuente intermedia.

En relación con la posible finalidad de la publicación, el contexto de exposición observado resulta compatible con la utilización de una muestra (*sample*) como mecanismo de demostración de la información que un actor afirma poseer. Este tipo de publicación puede tener como objetivo acreditar, ante potenciales compradores, la existencia y las características de un conjunto de datos ofrecido posteriormente mediante canales privados de comunicación, entre ellos Telegram. En consecuencia, el hallazgo podría representar una etapa preliminar de comercialización de información presuntamente obtenida de manera no autorizada. No obstante, con los elementos disponibles no es posible confirmar que la venta se haya concretado, que la totalidad de los registros anunciados exista o que el actor disponga efectivamente de una base de datos completa.

Como parte del proceso de validación, se realizó un análisis de correlación sobre un registro representativo de la muestra, correspondiente a una persona identificada como **VAZQUEZ HUGO MARTIN**. Las consultas efectuadas en distintas fuentes digitales permitieron identificar coincidencias entre los datos personales del registro y referencias externas asociadas a la identidad, la localización geográfica y los posibles servicios utilizados por dicha persona.

En primer lugar, las consultas realizadas mediante servicios de información y verificación disponibles en línea permitieron encontrar correspondencias entre el nombre consignado en la muestra y una persona física aparentemente existente. Asimismo, se identificaron coincidencias entre el número de documento analizado y referencias externas que lo vinculan con dicha identidad y con la localidad de Chascomús, provincia de Buenos Aires. Estas coincidencias aportan elementos de corroboración respecto de la verosimilitud del registro, aunque su alcance depende de la actualidad, exactitud e independencia de las fuentes consultadas.

En segundo lugar, se identificó una correspondencia entre el domicilio incluido en la muestra y referencias externas asociadas a la persona investigada. La ubicación geográfica resultante presenta, además, consistencia con la característica telefónica consignada en el registro, correspondiente al área de Chascomús. Esta correlación geográfica refuerza la coherencia interna de los datos analizados, sin constituir por sí misma una prueba concluyente sobre la titularidad actual de la línea telefónica ni sobre la procedencia corporativa de la información.

En tercer lugar, se efectuaron verificaciones sobre el número telefónico y las direcciones de correo electrónico incluidos u obtenidos durante la investigación. Los resultados permitieron identificar indicios de actividad o asociación con diferentes servicios digitales y plataformas comerciales. Entre ellos, se observaron referencias compatibles con el uso de servicios de mensajería, correo electrónico, redes sociales y servicios de telecomunicaciones. Adicionalmente, algunas consultas permitieron obtener indicios parciales de registros vinculados a servicios de telefonía móvil, electricidad residencial y gas natural en la localidad analizada.

La correlación de estos elementos permitió ampliar el contexto del registro original y detectar relaciones entre distintos identificadores digitales y referencias geográficas. Sin embargo, es necesario distinguir entre la existencia de una cuenta, la asociación de un identificador con una plataforma y la confirmación de que una persona determinada mantiene actualmente su titularidad o control. En particular, las validaciones efectuadas mediante mecanismos de recuperación de contraseña o formularios de acceso deben interpretarse como indicios de asociación con un servicio, y no necesariamente como una confirmación definitiva de identidad, titularidad o actividad reciente.

En términos generales, **el conjunto de coincidencias observadas incrementa la plausibilidad de que la muestra contenga datos personales correspondientes a una persona real y que dichos datos presenten un grado significativo de consistencia entre distintas fuentes**. Asimismo, la estructura de los registros y la presencia del identificador comercial «FIBERTEL» justifican profundizar el análisis sobre una posible

relación con información de clientes de la organización. No obstante, la autenticidad del registro individual y su coherencia con fuentes externas no deben interpretarse como prueba suficiente de que la base de datos haya sido extraída de los sistemas de Fibertel S.A.

En consecuencia, el principal hallazgo de esta investigación consiste en la identificación de una muestra de datos presuntamente expuesta en un entorno asociado a la comercialización de información, cuya composición presenta indicios de contener información personal real y potencialmente vinculada a servicios de telecomunicaciones. La hipótesis de una posible afectación a Fibertel S.A. permanece abierta y requiere validación técnica y corporativa para establecer su procedencia con un nivel de confianza concluyente.

A efectos de avanzar en la investigación y determinar la eventual materialización de un incidente de seguridad, se considera prioritario establecer un canal de colaboración con los responsables de ciberseguridad, infraestructura y protección de datos de la organización. Este trabajo conjunto debería contemplar la comparación controlada de los registros de la muestra con las fuentes de información corporativas pertinentes, la identificación de posibles coincidencias con sistemas históricos o actuales, la determinación del período al que corresponderían los datos y la evaluación del posible alcance de la exposición. Asimismo, se recomienda preservar las evidencias digitales disponibles, documentar las fuentes y fechas de consulta y mantener la trazabilidad de las validaciones efectuadas, a fin de facilitar futuras instancias de análisis técnico y respuesta ante incidentes.

Finalmente, se destaca que la investigación realizada constituye un **hallazgo de inteligencia relevante que justifica una evaluación técnica adicional**, pero no permite, en su estado actual, confirmar de manera definitiva una filtración originada en la infraestructura de Fibertel S.A. La colaboración entre las partes permitirá determinar con mayor precisión la procedencia de los registros, evaluar el riesgo potencial para la organización y las personas involucradas, y definir las medidas de mitigación que correspondan en función de los resultados obtenidos.