Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

ANÁLISIS Y DETECCIÓN DE VULNERABILIDADES

Departamento CIBERSEGURIDAD

División SEGURIDAD INFORMÁTICA

Centro de Operaciones de Seguridad (SOC)

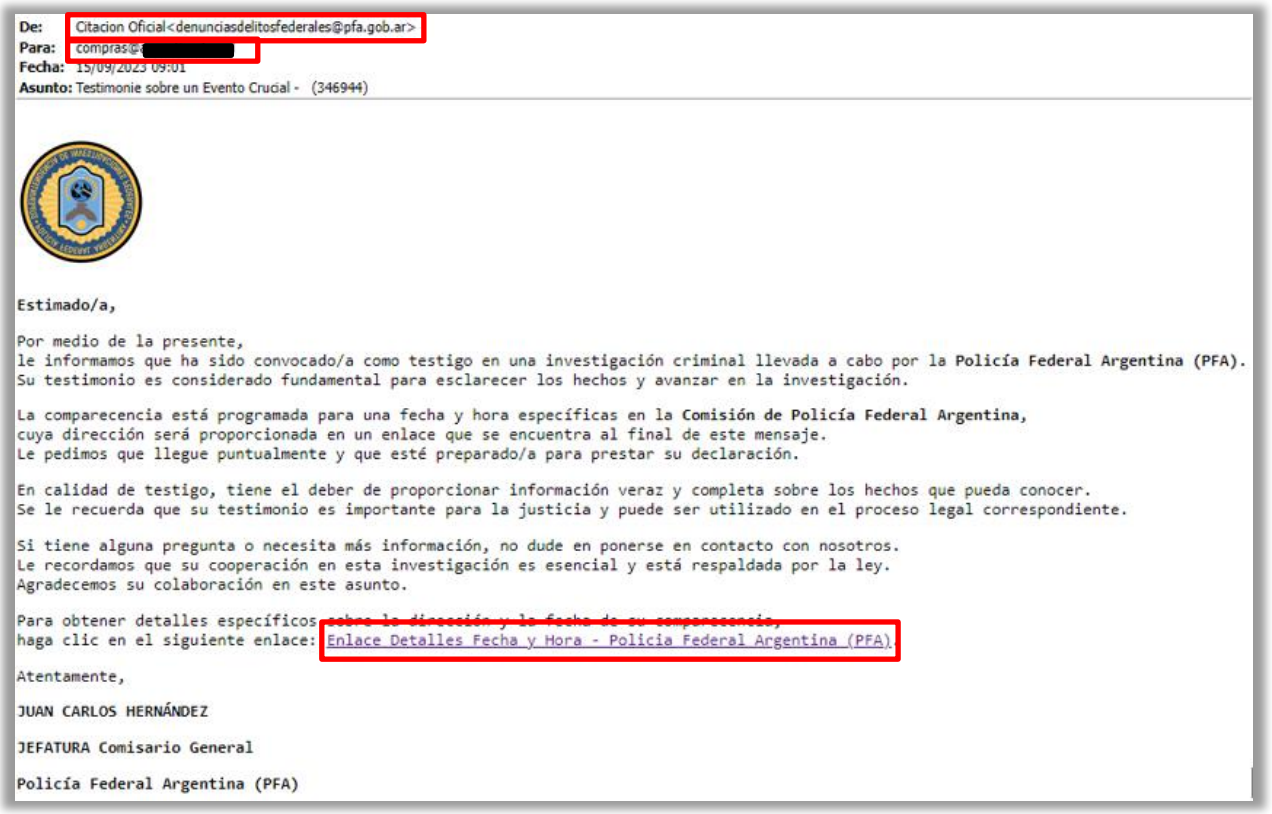
Campaña de Correos Maliciosos

Introducción

Este Centro de Operaciones de Seguridad (SOC) toma conocimiento de una campaña de Ingeniería Social en la cual se intenta suplantar la identidad de la Policía Federal Argentina por medio de correos electrónicos provenientes de la cuenta "denunciasdelitosfederales@pfa.gob.ar". Por tal motivo, se dio intervención al personal de Laboratorio de Malware a fin de verificar si el contenido presenta algún nivel de peligrosidad para los usuarios afectados.

Desarrollo

Una vez identificado el caso, se procede con las tareas de análisis del correo proveniente de "denunciasdelitosfederales@pfa.gob.ar", observando que el mismo simula ser una comunicación policial de la Policía Federal Argentina, en la cual se hace uso de un escudo perteneciente a la Superintendencia de Investigaciones Federales, a través del cual informan sobre una supuesta citación en la "Comisión de Policía Federal Argentina". Asimismo, en el cuerpo del mensaje se encuentran además un enlace adjunto el cual, según detalla, proporciona información sobre la fecha y hora de la citación:



De: Citacion Oficial<denunciasdelitosfederales@pfa.gob.ar>
Para: compras@[redacted]
Fecha: 15/09/2023 09:01
Asunto: Testimonie sobre un Evento Crucial - (346944)

Estimado/a,

Por medio de la presente,
le informamos que ha sido convocado/a como testigo en una investigación criminal llevada a cabo por la **Policía Federal Argentina (PFA)**.
Su testimonio es considerado fundamental para esclarecer los hechos y avanzar en la investigación.

La comparecencia está programada para una fecha y hora específicas en la **Comisión de Policía Federal Argentina**,
cuya dirección será proporcionada en un enlace que se encuentra al final de este mensaje.
Le pedimos que llegue puntualmente y que esté preparado/a para prestar su declaración.

En calidad de testigo, tiene el deber de proporcionar información veraz y completa sobre los hechos que pueda conocer.
Se le recuerda que su testimonio es importante para la justicia y puede ser utilizado en el proceso legal correspondiente.

Si tiene alguna pregunta o necesita más información, no dude en ponerse en contacto con nosotros.
Le recordamos que su cooperación en esta investigación es esencial y está respaldada por la ley.
Agradecemos su colaboración en este asunto.

Para obtener detalles específicos sobre la dirección y la fecha de su comparecencia,
haga clic en el siguiente enlace: Enlace Detalles Fecha y Hora - Policia Federal Argentina (PFA).

Atentamente,

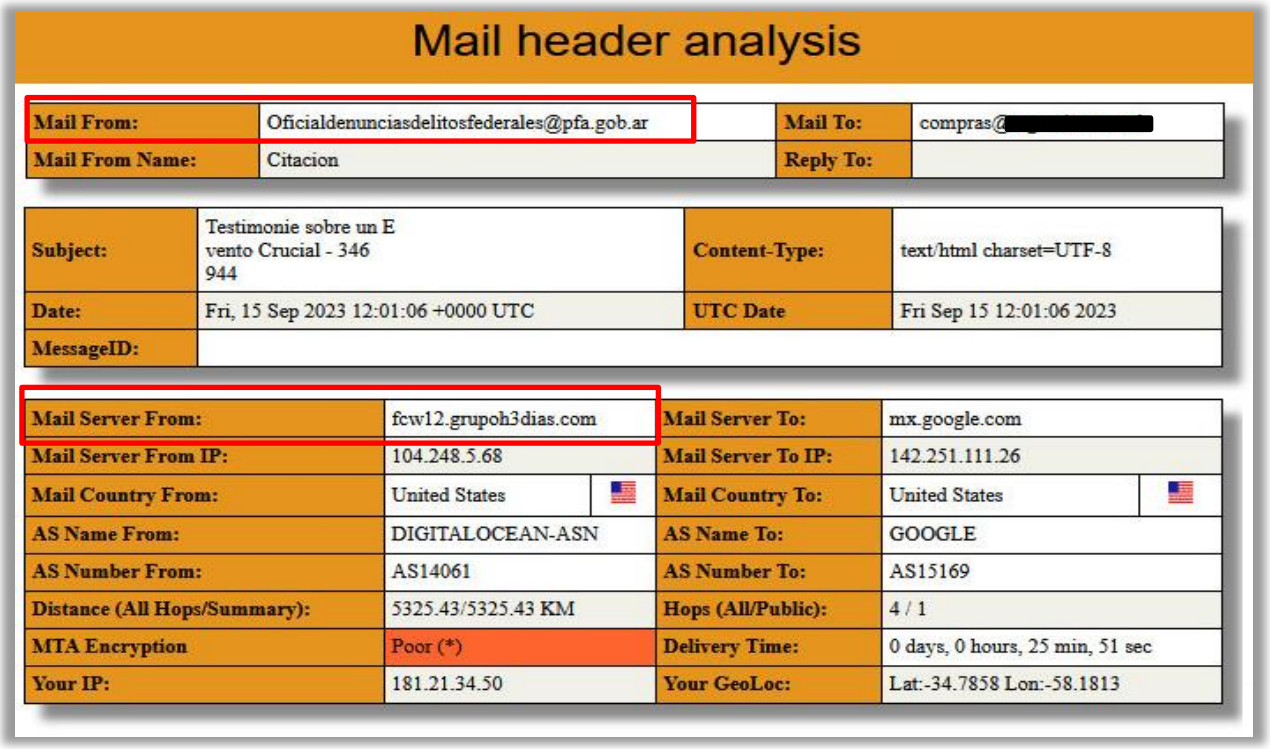
JUAN CARLOS HERNÁNDEZ

JEFATURA Comisario General

Policía Federal Argentina (PFA)

Imagen 1: Correo original, se detalla remitente, destinatario y enlace adjunto

Posteriormente, mediante la herramienta "Email Header Analizer", se analiza el encabezado del correo. De dicho análisis surge que el mismo se encuentra enmascarado, identificando que denunciasdelitosfederales@pfa.gob.ar procede realmente desde el servicio de mail fcw12.grupoh3dias.com.



Mail header analysis

Mail From:	Oficialdenunciasdelitosfederales@pfa.gob.ar	**Mail To:**	compras@[redacted]
Mail From Name:	Citacion	**Reply To:**	

Subject:	Testimonie sobre un E vento Crucial - 346 944	**Content-Type:**	text/html charset=UTF-8
Date:	Fri, 15 Sep 2023 12:01:06 +0000 UTC	**UTC Date**	Fri Sep 15 12:01:06 2023
MessageID:			

Mail Server From:	fcw12.grupoh3dias.com	**Mail Server To:**	mx.google.com
Mail Server From IP:	104.248.5.68	**Mail Server To IP:**	142.251.111.26
Mail Country From:	United States	**Mail Country To:**	United States
AS Name From:	DIGITALOCEAN-ASN	**AS Name To:**	GOOGLE
AS Number From:	AS14061	**AS Number To:**	AS15169
Distance (All Hops/Summary):	5325.43/5325.43 KM	**Hops (All/Public):**	4 / 1
MTA Encryption	Poor (*)	**Delivery Time:**	0 days, 0 hours, 25 min, 51 sec
Your IP:	181.21.34.50	**Your GeoLoc:**	Lat:-34.7858 Lon:-58.1813

Imagen 2: Análisis del encabezado del mensaje.

Al ingresar se observa que el enlace "Enlace Detalles Fecha y Hora – Policia Federal Argentina (PFA). se encuentra enmascarado[1] y nos re direcciona al sitio web "hxxps://soluttiondetallesfechargroup.westeurope.cloudapp.azure.com/", generando la descarga automática de un archivo (.zip), el cual, cuando se lo descomprime muestra el archivo ejecutable denominado "DCIX_Copia_de_LaMismaOXXUTPRBNKYD", tal como semuestra en las siguientes imágenes.

Imagen 3: URL derivada luego de interactuar con el enlace y la descarga del archivo.

[1] Dirección Web Enmascarada: es ocultar el verdadero destino de un enlace. Hacer ver a la víctima que está haciendo clic a algo que enrealidad no es.

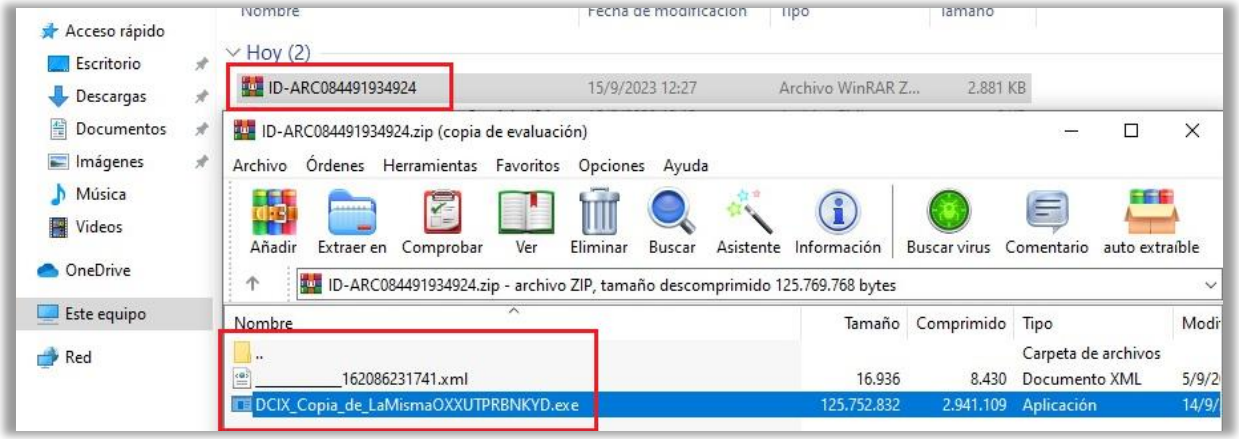


Imagen 4: Archivo descomprimido.

Al ejecutar el archivo se observó una ventana indicando la actualización de la aplicación Adobe Reader, y posteriormente el reinicio del ordenador. Luego del reinicio y una vez realizado el análisis mediante la herramienta FortiSandbox, se logró comparar los registros del sistema que modificaba el malware determinando varios procesos maliciosos en ejecución.

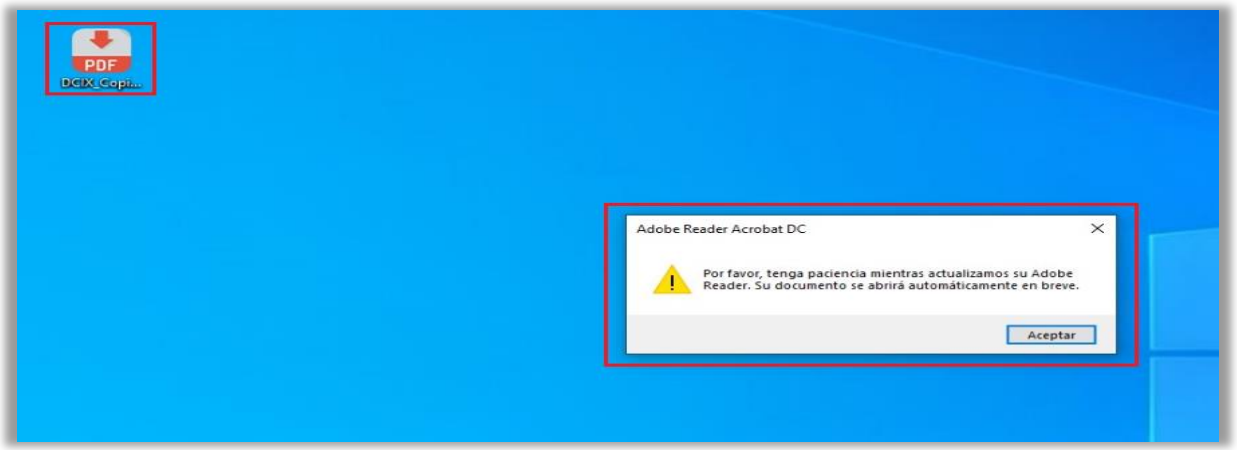


Imagen 5: Mensaje antes del reinicio del ordenador.

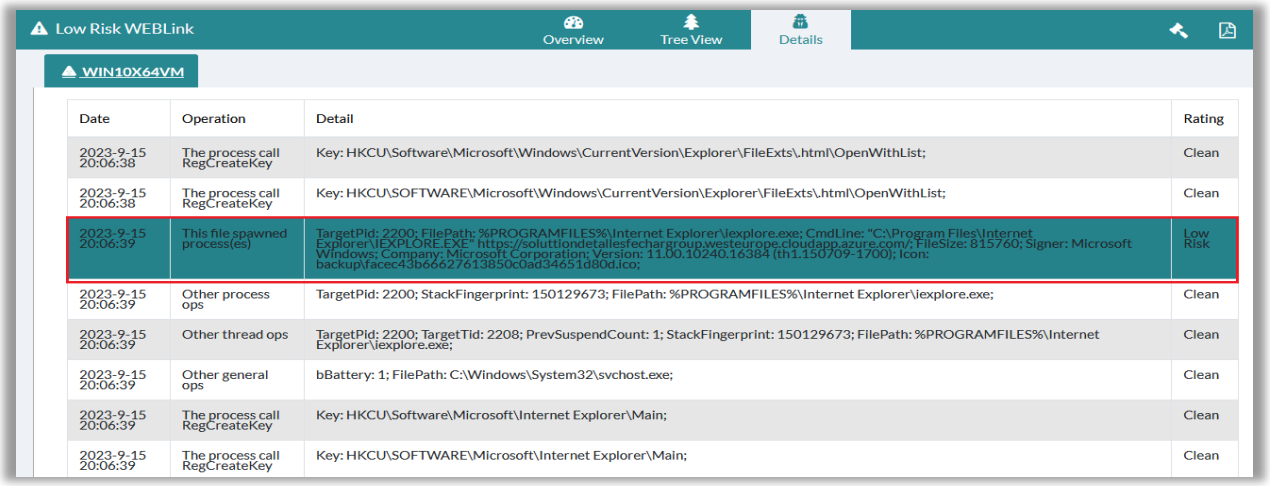


Imagen 6: Procesos maliciosos detectados mediante la herramienta FortiSandbox.

Se procedió a analizar mediante diferentes soluciones de seguridad, la URL relacionada al link adjunto al mail, la cual reporta que dicho sitio posee indicadores de compromiso del tipo "Phishing" y el archivo descargado es identificado como un "Trojan o (Troyano)"

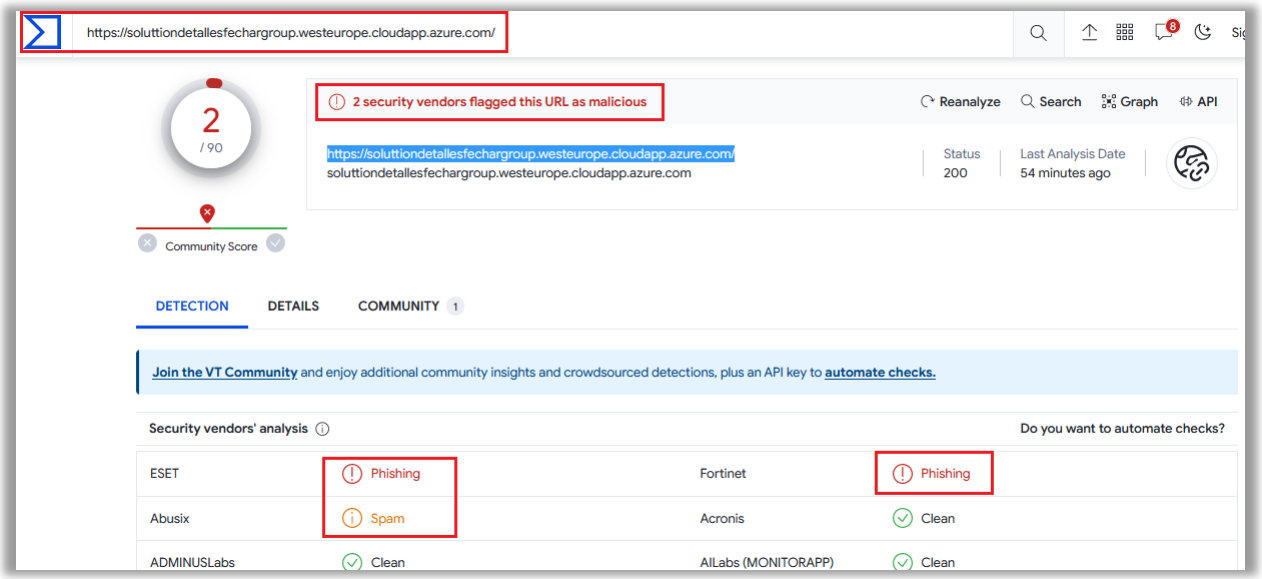


Imagen 7: Análisis de la URL a la cual somos re-direccionados.

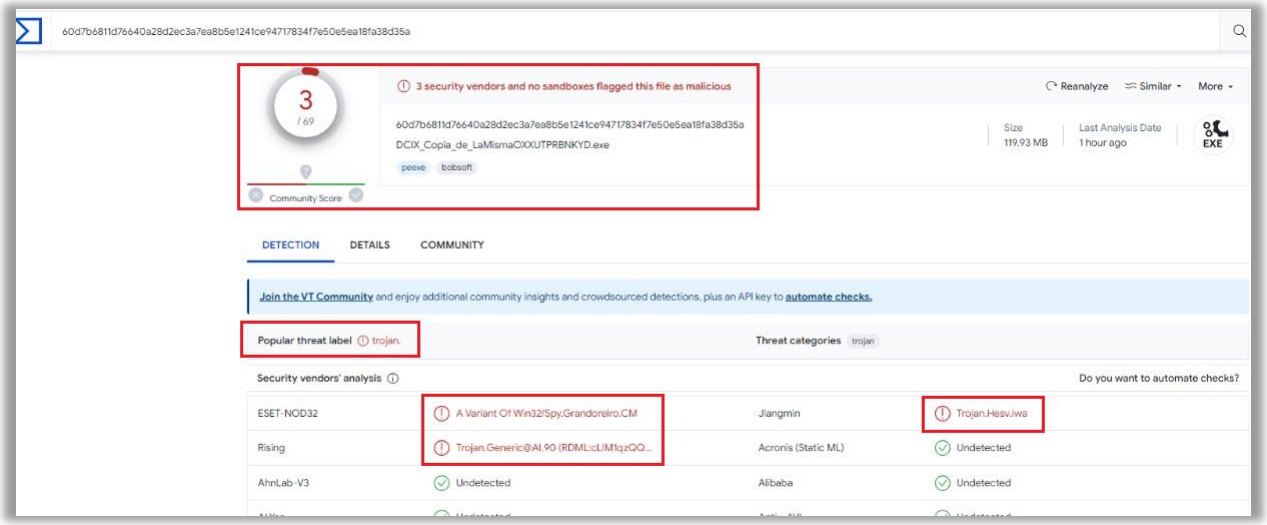
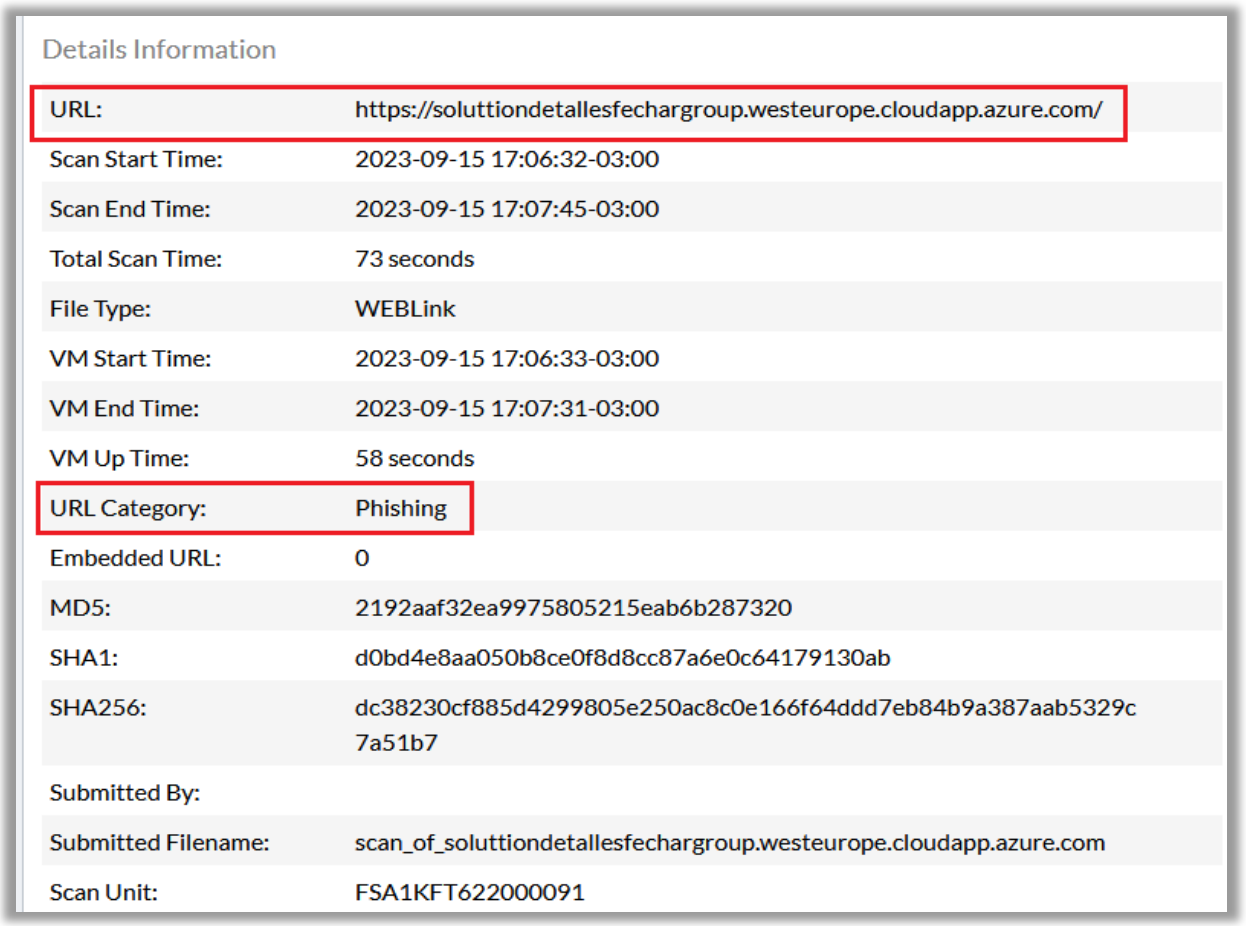


Imagen 8: Análisis del archivo.

Por otro lado, se analizó los enlaces en un entorno controlado mediante una "FortiSandbox", determinando que dicho enlaces se encuentran etiquetados como malicioso.



Details Information

URL:	https://soluttiondetallesfechargroup.westeurope.cloudapp.azure.com/
Scan Start Time:	2023-09-15 17:06:32-03:00
Scan End Time:	2023-09-15 17:07:45-03:00
Total Scan Time:	73 seconds
File Type:	WEBLink
VM Start Time:	2023-09-15 17:06:33-03:00
VM End Time:	2023-09-15 17:07:31-03:00
VM Up Time:	58 seconds
URL Category:	Phishing
Embedded URL:	0
MD5:	2192aaf32ea9975805215eab6b287320
SHA1:	d0bd4e8aa050b8ce0f8d8cc87a6e0c64179130ab
SHA256:	dc38230cf885d4299805e250ac8c0e166f64ddd7eb84b9a387aab5329c7a51b7
Submitted By:	
Submitted Filename:	scan_of_soluttiondetallesfechargroup.westeurope.cloudapp.azure.com
Scan Unit:	FSA1KFT622000091

Imagen 9: Detalle del enlace "malicioso".

Conclusión

En base a lo expuesto en el presente informe, se logró determinar que el correo electrónico remitido desde denunciasdelitosfederales@pfa.gob.ar, se trata de un mensaje con la dirección del remitente enmascarada, proviniendo realmente desde fcw12.grupoh3dias.com, el cual posee un enlace a un sitio web malicioso, alojado en "Azure" servicios cloud de la empresa Microsoft, y que al momento de ingresar, se realiza la descarga de manera automática sin intervención del usuario, de un archivo comprimido en formato ".zip" de nombre "ID-ARC084491934924" encontrándose dentro de este un archivo malicioso ejecutable, de nombre "DCIX_Copia_de_LaMismaOXXUTPRBNKYD" (ver imagen 4).

Al abrir el archivo ".exe" se ejecuta una aplicación la cual simula ser un archivo PDF y en consecuencia surge una ventana falsa de "Adobe Reader Acrobat DC" indicando al usuario que se están llevando a cabo actualizaciones y que el archivo se abrirá automáticamente cuando esta finalice, instante en donde se inyecta software malicioso en el equipo (ver imagen 5). En esta instancia por medio de diferentes soluciones de seguridad se determina que se están llevando a cabo cambios en el sistema (ver imagen 6)

Este malware, descarga y ejecuta un script (comandos para realizar instalaciones de forma automática dentro de un sistema) para realizar diferentes tareas, de esta manera evita ser detectado y permite a los atacantes robar información sensible como por ejemplo credencialesde acceso (usuarios y contraseñas), tarjetas de créditos entre otras.

Se recomienda, al recibir correos de dudosa procedencia**,** no ingresar a los enlaces o archivos adjuntos y en ninguna circunstancia completar los datos solicitados en los mismos, a su vez, reportarlo cuanto antes a nuestra División a través de la casilla de correo electrónico csoc@policiafederal.gov.ar.

Al respecto, se requirió a la División CENTRO FEDERAL DE DATOS el bloqueo preventivo de la cuenta maliciosa como también a la División SEGURIDAD EN REDES DE DATOS para el bloqueo de las conexiones maliciosas, con el fin de evitar que los usuarios de nuestra Institución sean víctimas de este tipo de engaño.