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

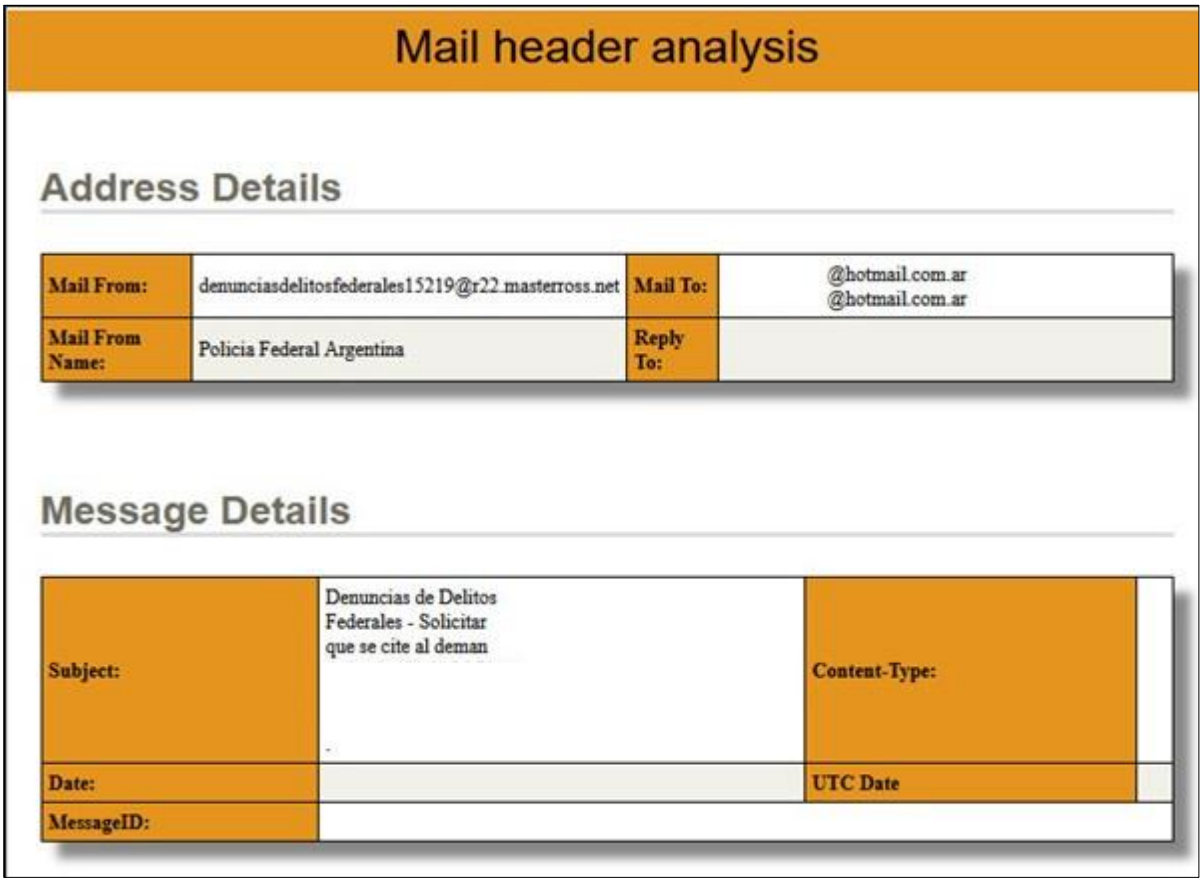
Este Centro de Operaciones de Seguridad (SOC) toma conocimiento de una campaña de Ingeniería Social en la cual se intenta suplantar la identidad de la Policía Federal Argentina por medio de correos electrónicos provenientes de la cuenta "denunciasdelitosfederales15219@r22.masterross.net". Por tal motivo, 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 "denunciasdelitosfederales15219@r22.masterross.net", observando que el mismo simula ser una comunicación policial de la Policía Federal Argentina, en la cual se hace uso de un escudo Institucional y el nombre de una Dependencia Policial, a través del cual informan sobre una supuesta citación en el Departamento Central de Policía. En el cuerpo del mensaje se encuentran además 2 links adjuntos:

Imagen 1: Cuerpo del correo electrónico.

Posteriormente, mediante la herramienta "Email Header Analizer", se analiza el encabezado del correo, pero no sobre el mail original, sino sobre un correo reenviado por un usuario que lo recibió. De dicho análisis surge que no se encuentra enmascarado y efectivamente corresponde a denunicasdelitosfederales15219@r22.masterross.net.



Mail header analysis

Address Details

Mail From:	denunciasdelitosfederales15219@r22.masterross.net	Mail To:	@hotmail.com.ar @hotmail.com.ar
Mail From Name:	Policia Federal Argentina	Reply To:	

Message Details

Subject:	Denuncias de Delitos Federales - Solicitar que se cite al deman	Content-Type:	
Date:		UTC Date	
MessageID:			

Imagen 2: Análisis del encabezado del mensaje.

Al ingresar al primer enlace éste redirecciona al sitio web "http://transitonopagada.is-a-liberal.com/", observando que no se encuentra operativo al momento de realizar el análisis.

Continuando con el análisis del segundo enlace, se observa que la dirección web "https://www.argentina.gob.ar/policia-federal-argentina", se encuentra enmascarada[1] y nos redirecciona a un sitio web "https://dmhluxury.com/wp-content/gob/CITACIO610730BD4_DELITO_FEDERALE1373_5D3F_4B51_978E_379C65042752.php", generando la descarga del archivo (.zip), el cual, cuando se lo descomprime muestra el archivo ejecutable denominado "proceso0493f" con la extensión (.msi), tal como se muestra en las siguientes imágenes.

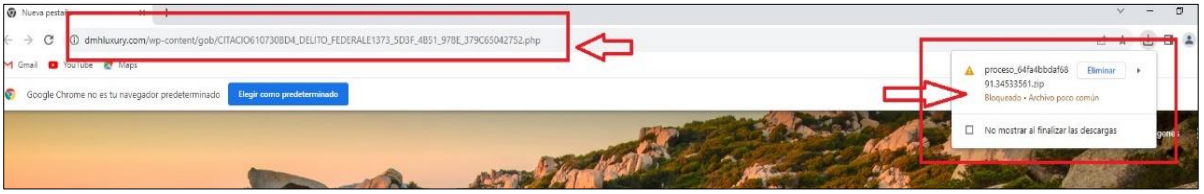


Imagen 3: URL derivada luego de interactuar con el enlace y la descarga del archivo.

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

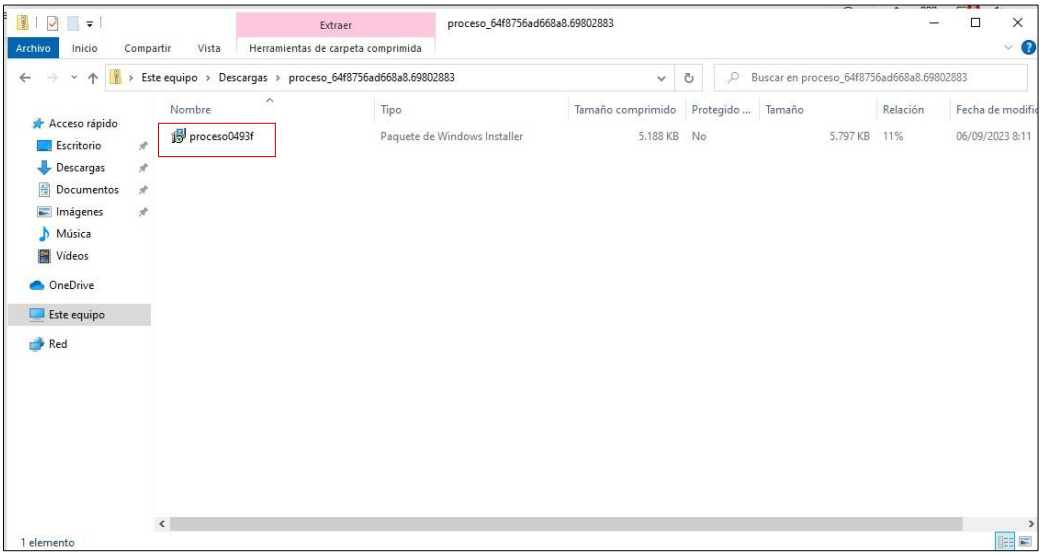


Imagen 4: Archivo descargado.

Al ejecutar el archivo no se observaron cambios a simple vista. Una vez realizado el análisis con herramientas específicas se logró comparar los registros que modificaba el malware determinando varios procesos maliciosos en ejecución.

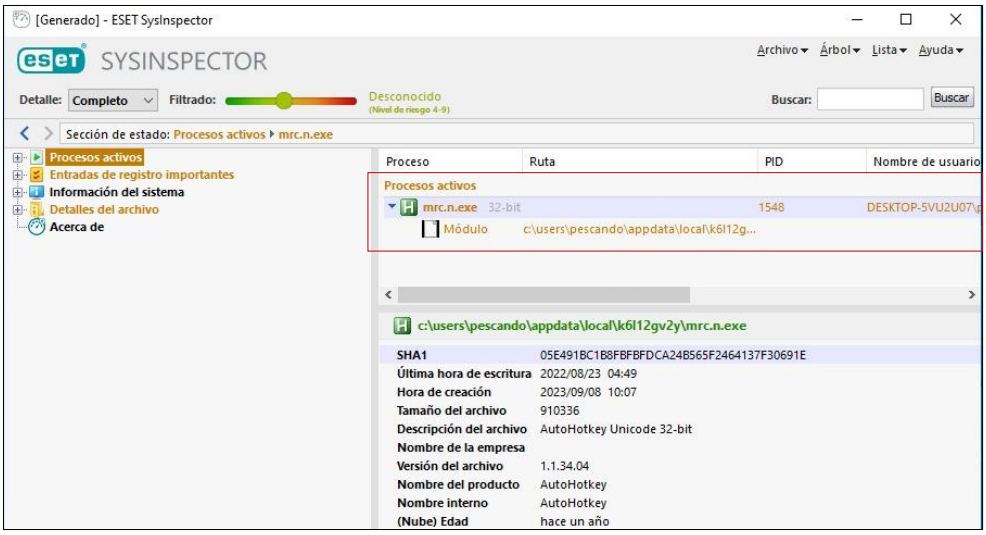


Imagen 5: Procesos maliciosos detectados.

Asimismo, se procedió a analizar mediante diferentes soluciones de seguridad, las URL´s relacionadas a los links adjuntos al mail, los cuales reportan que dichos sitios poseen indicadores de compromiso del tipo malware "Software malicioso".

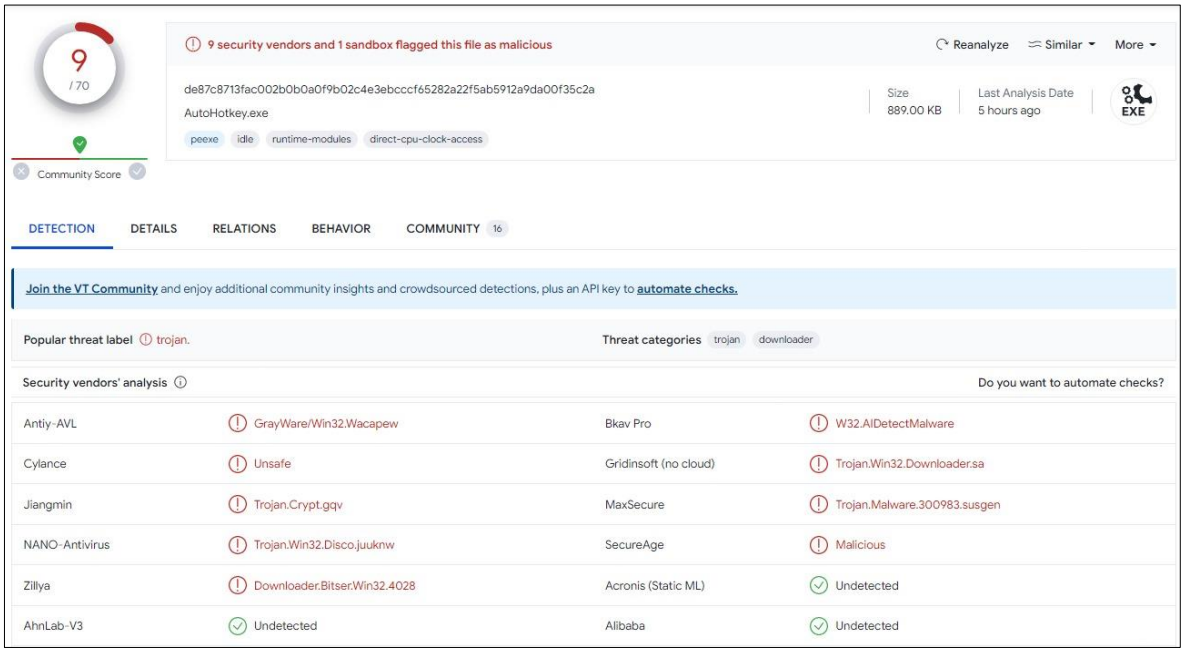


Imagen 6: Análisis del archivo.

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

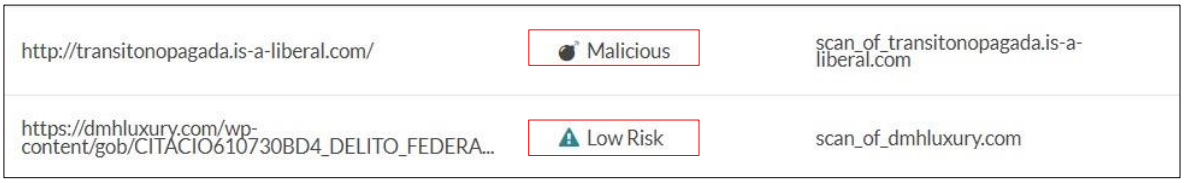


Imagen 7: Resultado de los enlaces.

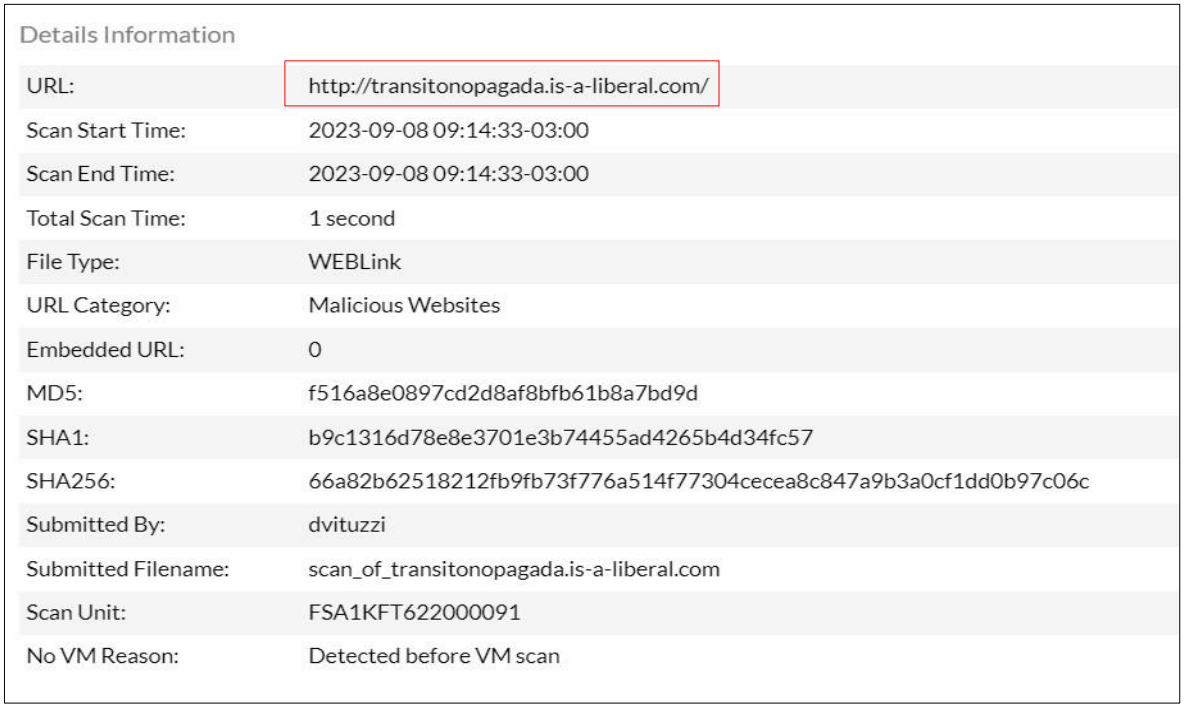


Imagen 8: Detalle del enlace "malicioso".

Details Information

URL:	https://dmhluxury.com/wp-content/gob/CITACIO610730BD4_DELITO_FEDERALE1373_5D3F_4B51_978E_379C65042752.php
Scan Start Time:	2023-09-08 09:11:55-03:00
Scan End Time:	2023-09-08 09:11:55-03:00
Total Scan Time:	1 second
File Type:	WEBLink
Redirect URL:	http://20.82.183.33/mode/
URL Category:	Phishing
Embedded URL:	0
MD5:	ab9aab089a8b9073aa3ee6efcb8e1b0b
SHA1:	b4a6f09b6baa97d0e421635e44a20fd7ec993672
SHA256:	f95510b66d4ff42bf053da15a488bf72a064537c664b73a7acad52739b5ae764
Submitted By:	dvituzzi
Submitted Filename:	scan_of_dmhluxury.com
Scan Unit:	FSA1KFT622000091
No VM Reason:	sandboxing prefilter on URL

Imagen 9: Detalle del enlace "Low Risk".

Cabe aclarar que pasado los días se observó que la url mencionada anteriormente paso a ser esta IP Pública "http://20.82.183.33/mode/", la que se encuentra hosteada en un servidor "Cloud Azure" de la empresa Microsoft.

IP Information for 20.82.183.33

− Quick Stats

IP Location	Ireland Dublin Microsoft Corporation
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
Whois Server	whois.arin.net
IP Address	20.82.183.33

```
NetRange:       20.33.0.0 - 20.128.255.255
CIDR:           20.48.0.0/12, 20.128.0.0/16, 20.34.0.0/15, 20.40.0.0/13, 20.33.0.0/16,
20.64.0.0/10, 20.36.0.0/14
NetName:        MSFT
NetHandle:      NET-20-33-0-0-1
Parent:         NET20 (NET-20-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Microsoft Corporation (MSFT)
RegDate:        2017-10-18
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/20.33.0.0
```

Imagen 10: Detalle del host del Servidor "Cloud Azure".

Conclusión

En base a lo expuesto en el presente informe, se logró determinar que el correo electrónico remitido desde "denunciasdelitosfederales15219@r22.masterross.net" posee enlaces enmascarados, alojados en los servicios "Cloud Azure" de la empresa Microsoft, y que al ingresar, realizan la descarga de un archivo comprimido en formato ".zip", conteniendo un archivo malicioso ejecutable, el cual con el paso de los días va variando su nombre con el fin de no ser detectado fácilmente por los antivirus, escrito en un lenguaje de programación de scripts de código abierto denominado "AutoHotkey o AHK", utilizado para la automatización de software en los dispositivos con sistemas operativos Windows.

Este malware del tipo troyano en lugar de recibir comandos directamente del servidor C&C, descarga y ejecuta scripts AHK para realizar diferentes tareas, de esta manera evita ser detectado y permite a los atacantes robar información sensible como por ejemplo credenciales de 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.