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)

Requerido por:

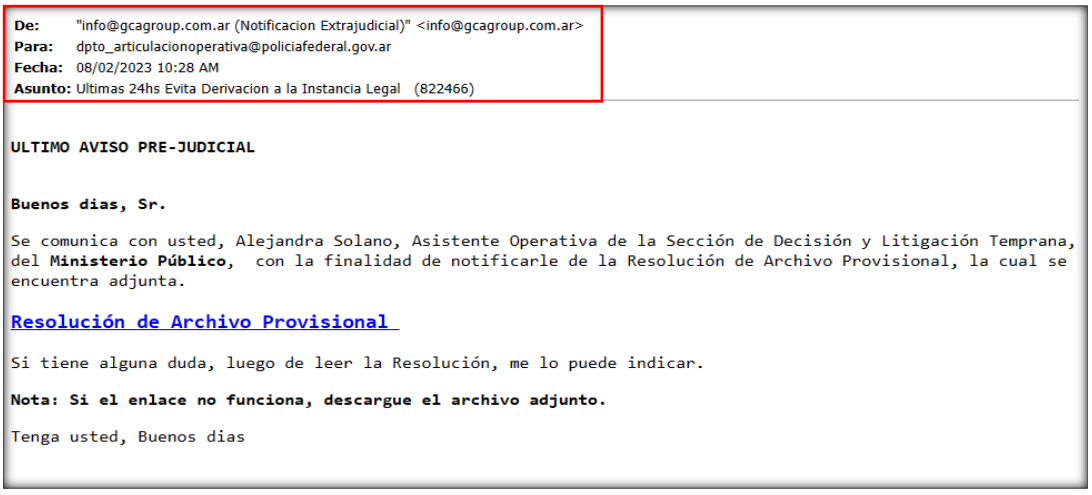
Departamento ARTICULACIÓN OPERATIVA.

Introducción

El día 9 de febrero del corriente año, se recepcionó en la cuenta csoc@policiafederal.gov.ar diferentes correos electrónicos provenientes de la cuenta dpto_articulacionoperativa@policiafederal.gov.ar, que serían de procedencia y contenido dudoso. Por tal motivo, se dio intervención al laboratorio de malware a fin de verificar si el contenido presenta algún nivel de peligrosidad.

Desarrollo

Una vez identificado el caso, se procedió al análisis de los correos provenientes de "info@gcagroup.com.ar" visualizándose en los mismos que, si bien el contenido podía diferir el fin terminaba siendo similar, la descarga de un archivo. También se expone como su remitente es ocultado a simple vista.



De: "info@gcagroup.com.ar (Notificacion Extrajudicial)" <info@gcagroup.com.ar>
Para: dpto_articulacionoperativa@policiafederal.gov.ar
Fecha: 08/02/2023 10:28 AM
Asunto: Ultimas 24hs Evita Derivacion a la Instancia Legal (822466)

ULTIMO AVISO PRE-JUDICIAL

Buenos dias, Sr.

Se comunica con usted, Alejandra Solano, Asistente Operativa de la Sección de Decisión y Litigación Temprana, del **Ministerio Público**, con la finalidad de notificarle de la Resolución de Archivo Provisional, la cual se encuentra adjunta.

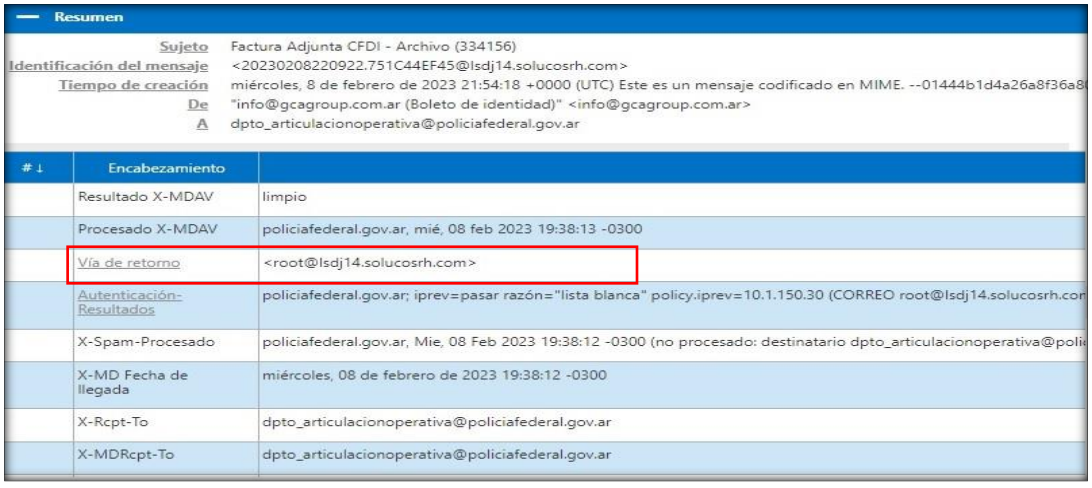
Resolución de Archivo Provisional

Si tiene alguna duda, luego de leer la Resolución, me lo puede indicar.

Nota: Si el enlace no funciona, descargue el archivo adjunto.

Tenga usted, Buenos dias

Imagen 1. Dirección del remitente y cuerpo de texto del mail



Resumen

Sujeto	Factura Adjunta CFDI - Archivo (334156)
Identificación del mensaje	<20230208220922.751C44EF45@lsdj14.solucosrh.com>
Tiempo de creación	miércoles, 8 de febrero de 2023 21:54:18 +0000 (UTC) Este es un mensaje codificado en MIME. --01444b1d4a26a8f36a8
De	"info@gcagroup.com.ar (Boleto de identidad)" <info@gcagroup.com.ar>
A	dpto_articulacionoperativa@policiafederal.gov.ar

#	Encabezamiento	
	Resultado X-MDAV	limpio
	Procesado X-MDAV	policiafederal.gov.ar, mié, 08 feb 2023 19:38:13 -0300
	Vía de retorno	<root@lsdj14.solucosrh.com>
	Autenticación-Resultados	policiafederal.gov.ar; iprev=pasar razón="lista blanca" policy.iprev=10.1.150.30 (CORREO root@lsdj14.solucosrh.com
	X-Spam-Procesado	policiafederal.gov.ar, Mie, 08 Feb 2023 19:38:12 -0300 (no procesado: destinatario dpto_articulacionoperativa@poli
	X-MD Fecha de llegada	miércoles, 08 de febrero de 2023 19:38:12 -0300
	X-Rcpt-To	dpto_articulacionoperativa@policiafederal.gov.ar
	X-MDRcpt-To	dpto_articulacionoperativa@policiafederal.gov.ar

Imagen 2. Muestra del encabezado y verdadero origen del mensaje

Al acceder en el enlace sugerido por el mensaje, se realiza la descarga automática de un archivo zip.

Continuando con el análisis del malware, se recurrió al uso de diferentes herramientas ejecutadas en entornos seguros donde se prosiguió con el análisis del archivo descargado: "**Arc_hivo_Doc_ume_ntMVEUANRKSNJUZZusxxj.zip**"

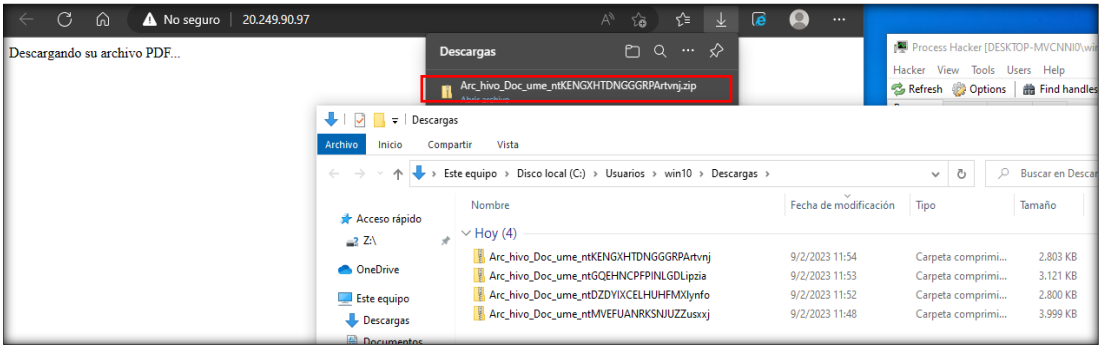


Imagen 3. IP a la cual somos derivados y descargas que se realizaron

El siguiente paso implica descomprimir dicho archivo, ejecutarlo y llevar a cabo su instalación (se remarca el hecho de que el mismo es percibido por el sistema de defensa del sistema operativo Windows defender el cual nos arroja la siguiente alerta).

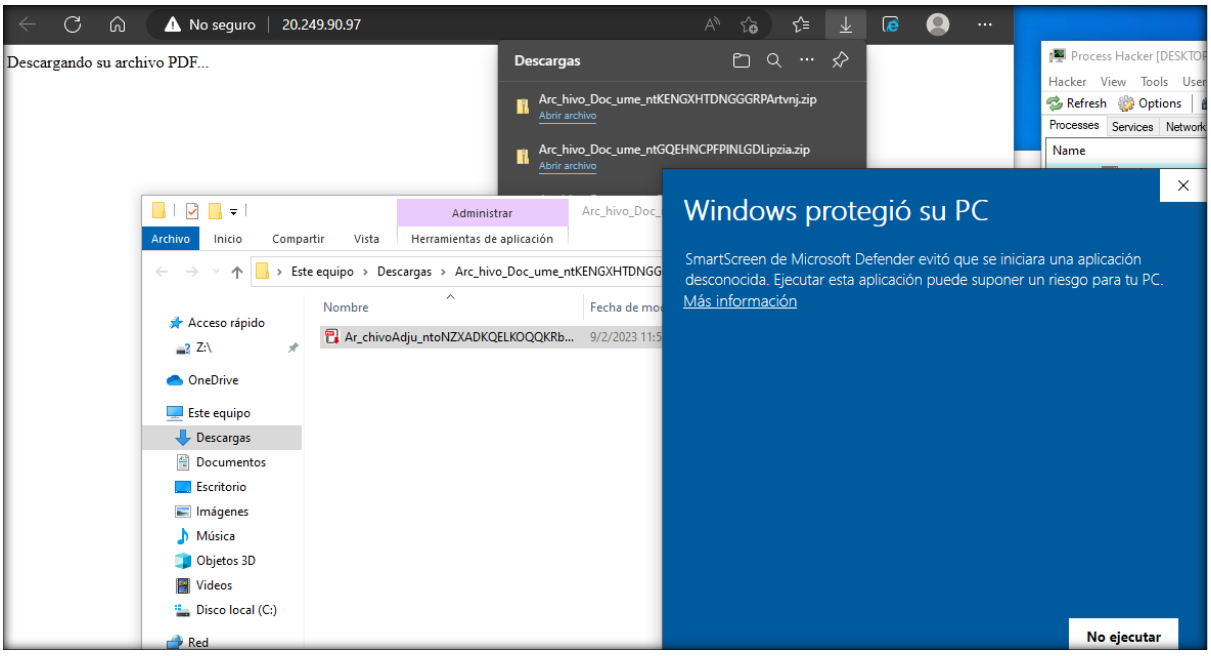


Imagen 4. Instalación y mensaje de seguridad emitido por Windows.

Al ejecutar el archivo descargado se observa como solo se solicita completar un campo de captcha, sin que se realicen más cambios a simple vista.

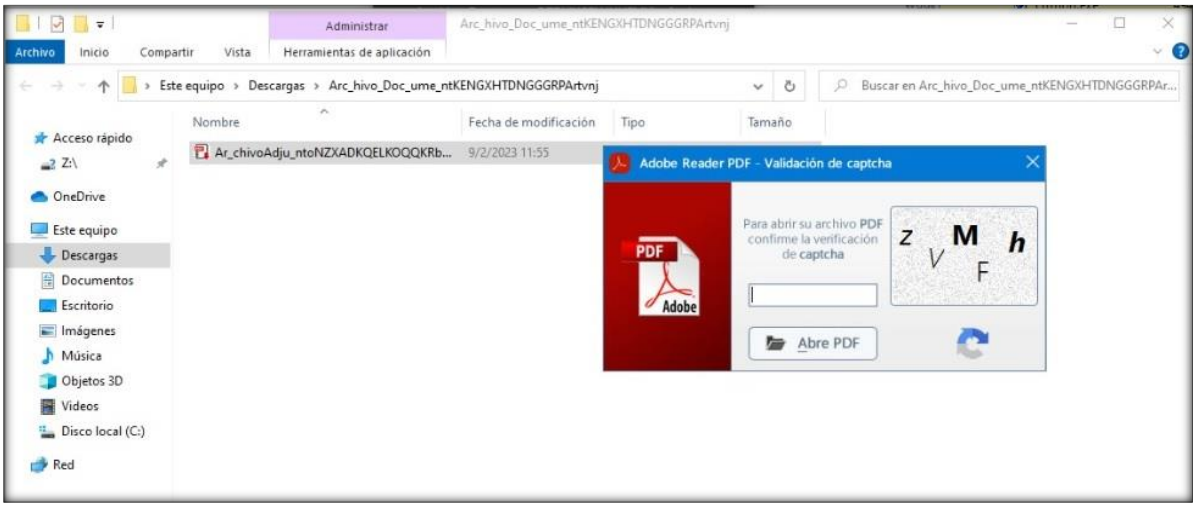


Imagen 5. Ventana emergente al seleccionar el archivo.

Analizando los procesos ejecutados al acceder al archivo descrito, se puede observar como se agregan rutas de accesos denominadas "HKU\S-1-5-21-…". Los mismos denotan el despliegue de código malicioso junto a otros procesos que podrían comprometer la seguridad de su información.

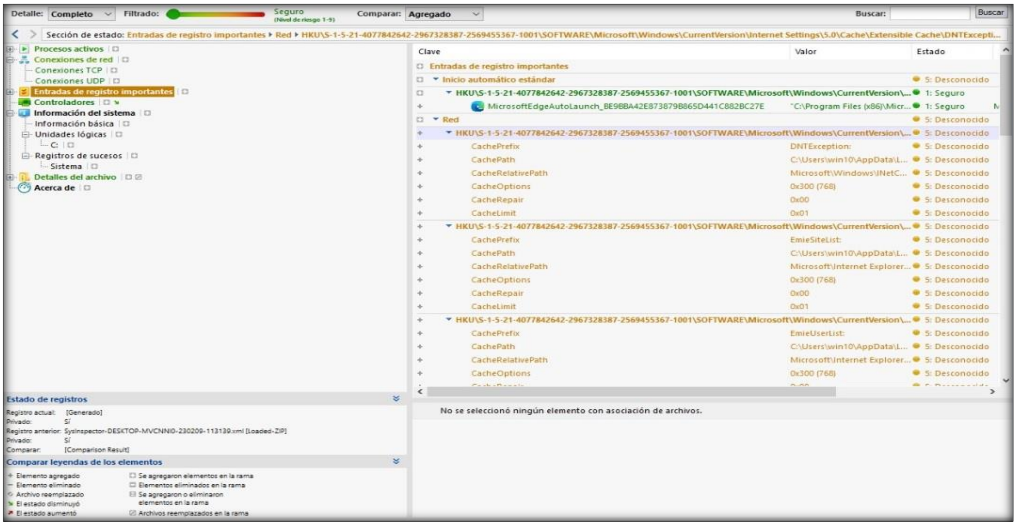


Imagen 6. Procesos ejecutados con el archivo malicioso.

Al comparar la reputación y el registro del archivo, se observa como efectivamente se lo reporta con la descripción de malware "troyano", siendo el mismo un programa ejecutado para disimular la funcionalidad de ataque que permite acceder a información privada.

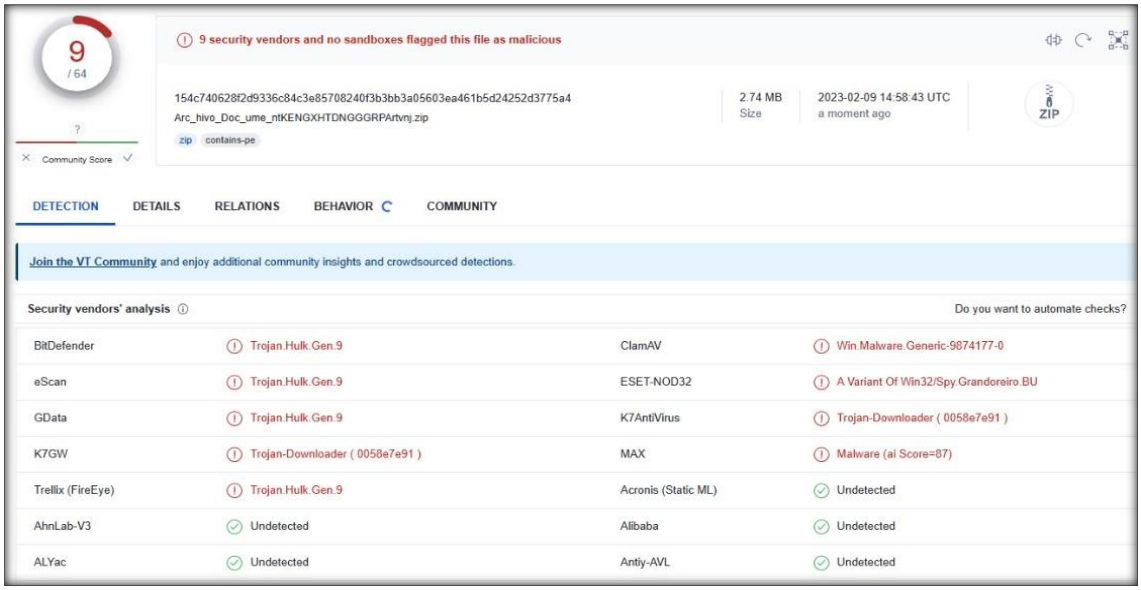


Imagen 7. Reporte del archivo descargado.

Conclusión

Se concluyó que el mismo corresponde a un ataque "troyano", en el que se realizan cambios en el equipo una vez descargado y ejecutado el archivo, camuflado o disimulado como otro tipo de programa, en este caso como un archivo ".pdf".

Para minimizar y mitigar cualquier riesgo ante esta situación, se recomienda realizar un backup (resguardo de la información) de su computadora, y formatearla, eliminando cualquier tipo de proceso o archivo malicioso en el mismo, junto a la instalación de un antivirus. Teniendo en cuenta esta recomendación como prioritaria en caso de haber ejecutado el archivo adjunto al correo recibido.

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