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:

Depto. Cuerpo Guardia de Infanteria .

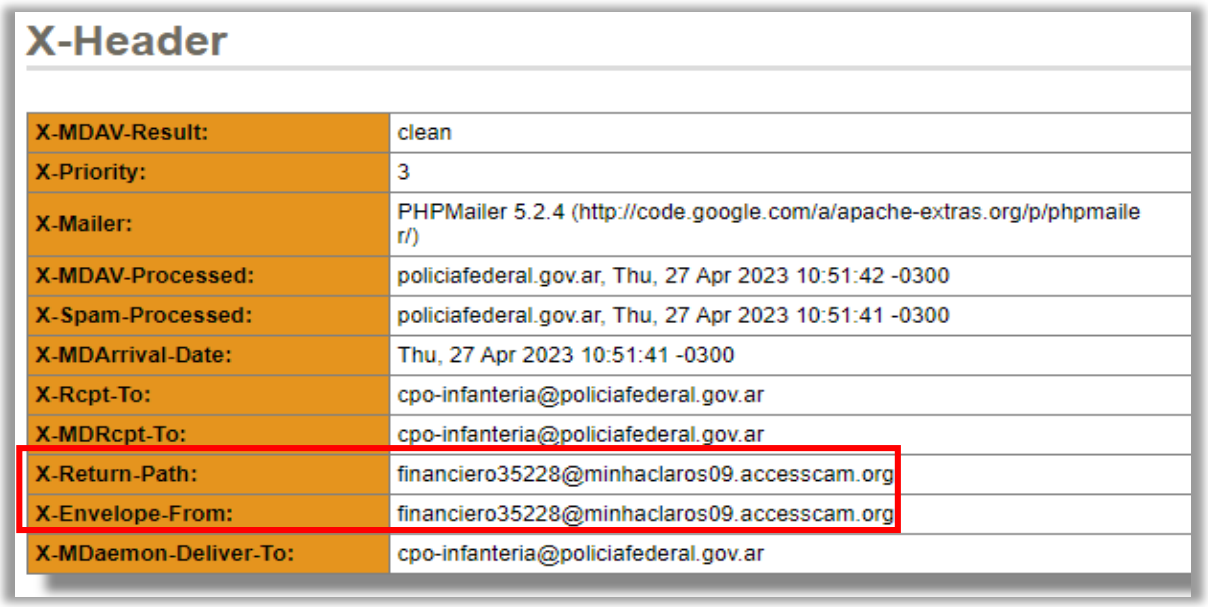
Introducción

En el día 27 de abril del corriente año, se recibe en la casilla "**csoc@policiafederal.gov.ar**", un mail proveniente de Depto. Cuerpo Guardia de Infantería, informando que en su casilla "**cpo-infanteria@policiafederal.gov.ar**" habrían recibido un correo electrónico de procedencia sospechosa por lo cual se procede a su análisis en un entorno seguro.

Imagen 1: muestra Cuerpo del Mensaje.

Desarrollo

Ante este reporte, como primera aproximación, se identificó que el mensaje proviene de la dirección de correo **"financiero35228@minhaclaros09.accesscam.org".** Mediante la herramienta "Email Header Analizer", se procedió a examinar el encabezado, determinando que el remitente no se encuentra enmascarado.



X-Header

X-MDAV-Result:	clean
X-Priority:	3
X-Mailer:	PHPMailer 5.2.4 (http://code.google.com/a/apache-extras.org/p/phpmailer/)
X-MDAV-Processed:	policiafederal.gov.ar, Thu, 27 Apr 2023 10:51:42 -0300
X-Spam-Processed:	policiafederal.gov.ar, Thu, 27 Apr 2023 10:51:41 -0300
X-MDArrival-Date:	Thu, 27 Apr 2023 10:51:41 -0300
X-Rcpt-To:	cpo-infanteria@policiafederal.gov.ar
X-MDRcpt-To:	cpo-infanteria@policiafederal.gov.ar
X-Return-Path:	financiero35228@minhaclaros09.accesscam.org
X-Envelope-From:	financiero35228@minhaclaros09.accesscam.org
X-MDaemon-Deliver-To:	cpo-infanteria@policiafederal.gov.ar

Imagen 2: análisis del encabezado del mensaje

Al acceder en el enlace sugerido por el mensaje, se realiza la descarga automática de un archivo zip. Seguidamente se recurrió al uso de diferentes herramientas ejecutadas en entornos seguros donde se prosiguió con el análisis del archivo descargado: "ID-FACT.644ab7b711425.zip"

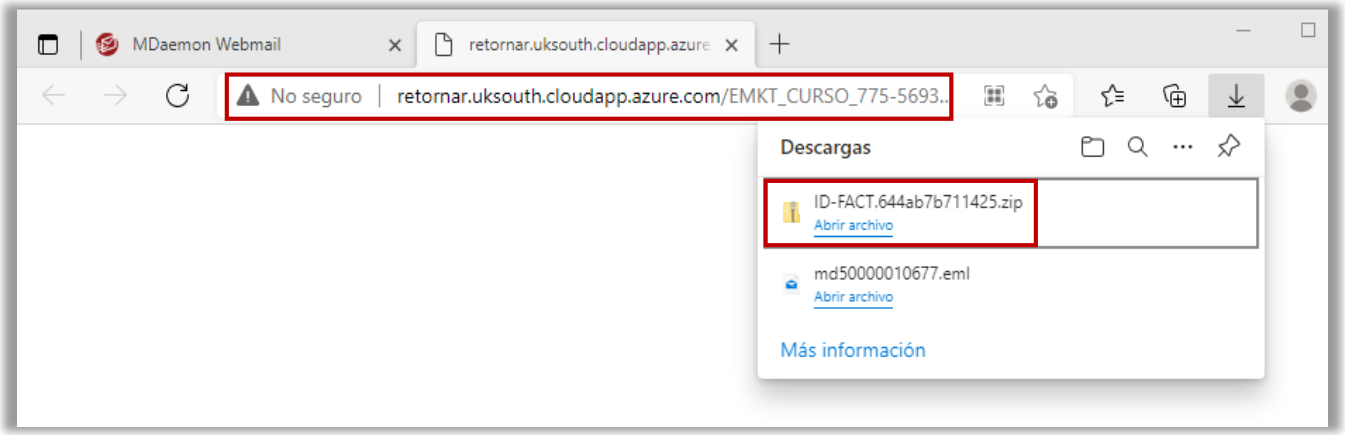


Imagen 3: IP a la cual somos derivados y descargas que se realizaron

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).

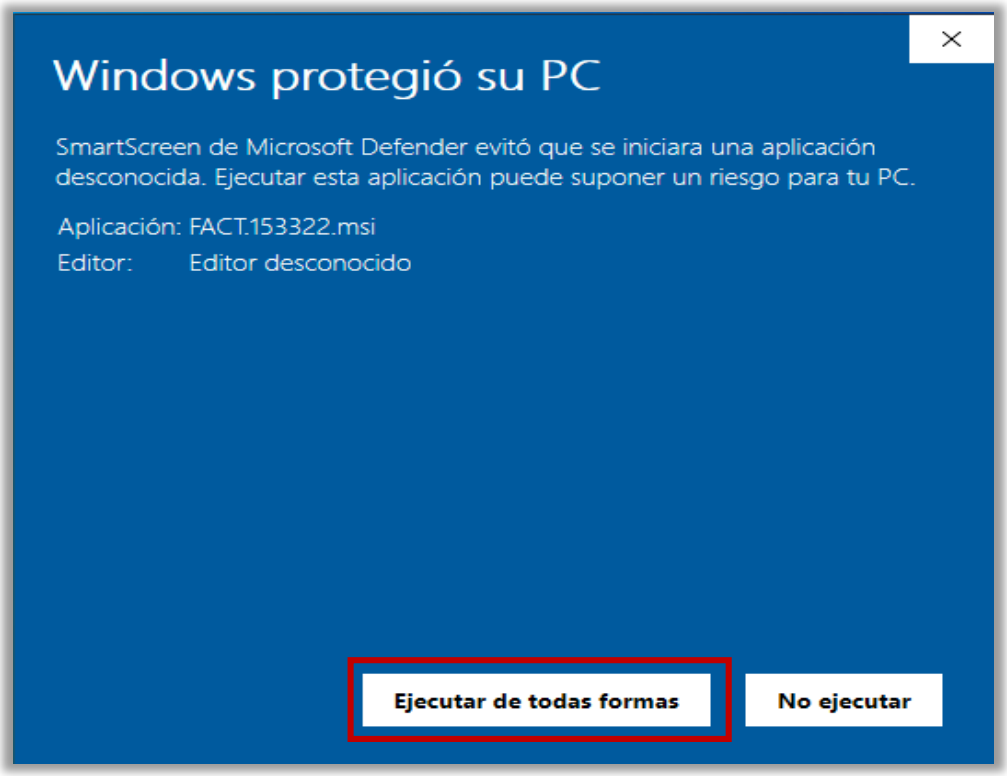


Imagen 4. Instalación y mensaje de seguridad emitido por Windows.

Si hacemos clic en "Ejecutar de todas formas" se produce la instalación de un ejecutable, "**FACT.153322.msi**" el mismo al finalizar muestra un resultado de "eRR0r".

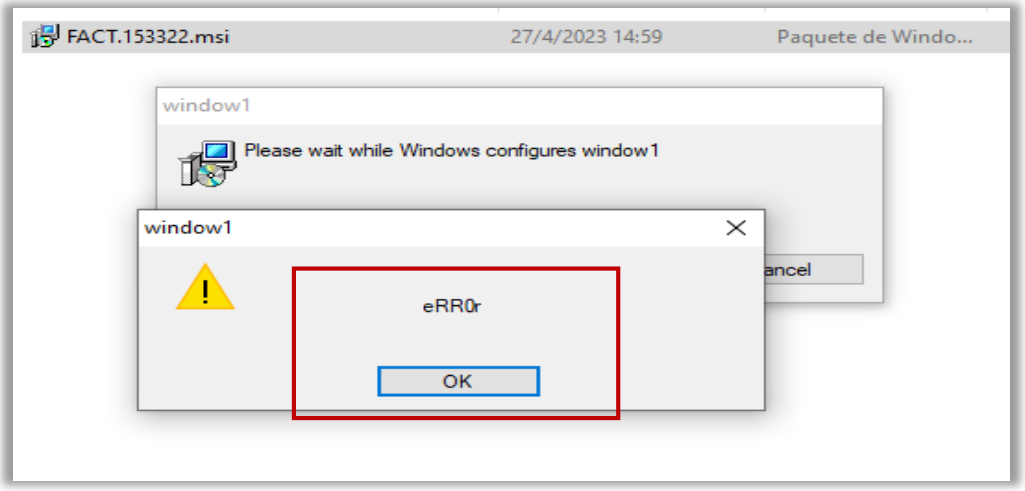


Imagen 5. Ventana emergente al seleccionar el archivo.

Se procede a analizar los cambios que surgieron en el sistema operativo a partir de la ejecución del archivo descargado a través de la herramienta "**ESET SysInspector**", se puede observar un nuevo proceso con el nombre "g4l.m.exe", mismos denotan el despliegue de código malicioso junto a otros procesos que podrían comprometer la seguridad de su información.

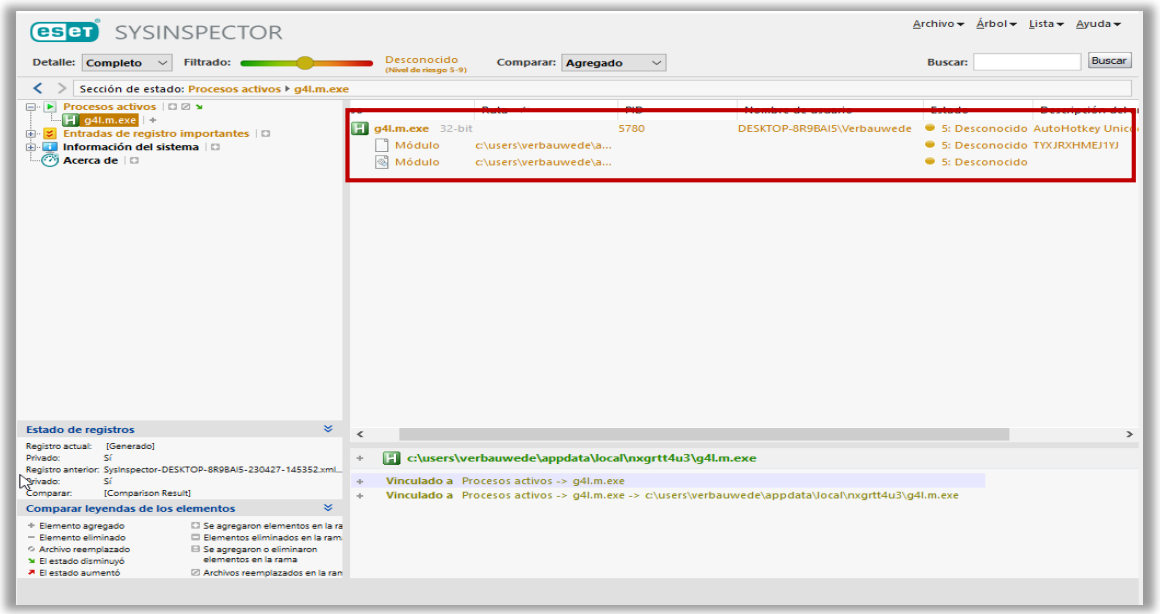


Imagen 6: Herramienta ESET SysInspector

Se procedió a analizar con diferentes vendors, observando como efectivamente se lo reporta con la descripción de malware "trojan", siendo el mismo un programa ejecutado para disimular la funcionalidad de ataque que permite acceder a información privada.

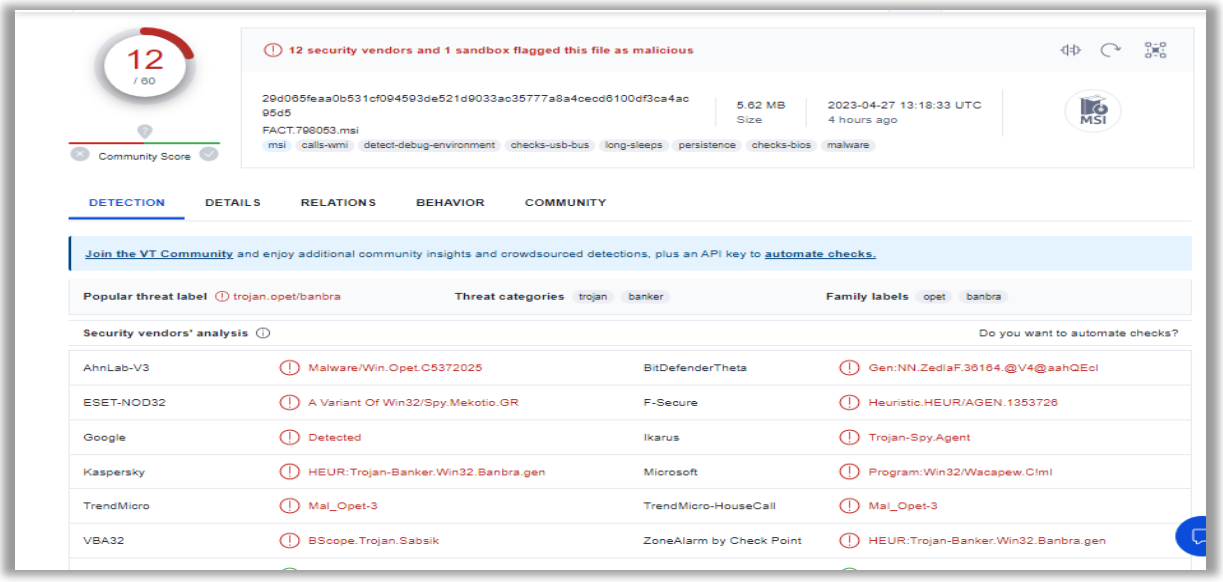


Imagen 7: Reporte del archivo descargado

Conclusión

En base a lo expuesto en el presente informe, se afirma que el correo electrónico remitido desde "**financiero35228@minhaclaros09.accesscam.org**" hacia la casilla de Policía Federal "**cpo-infanteria@policiafederal.gov.ar"**, se trata de un malware de tipo "trojan", en el que se realizan cambios en el equipo una vez descargado y ejecutado el archivo, camuflado o disimulado como otro tipo de programa.

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.

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 sigan siendo víctimas de este tipo de engaño.