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:

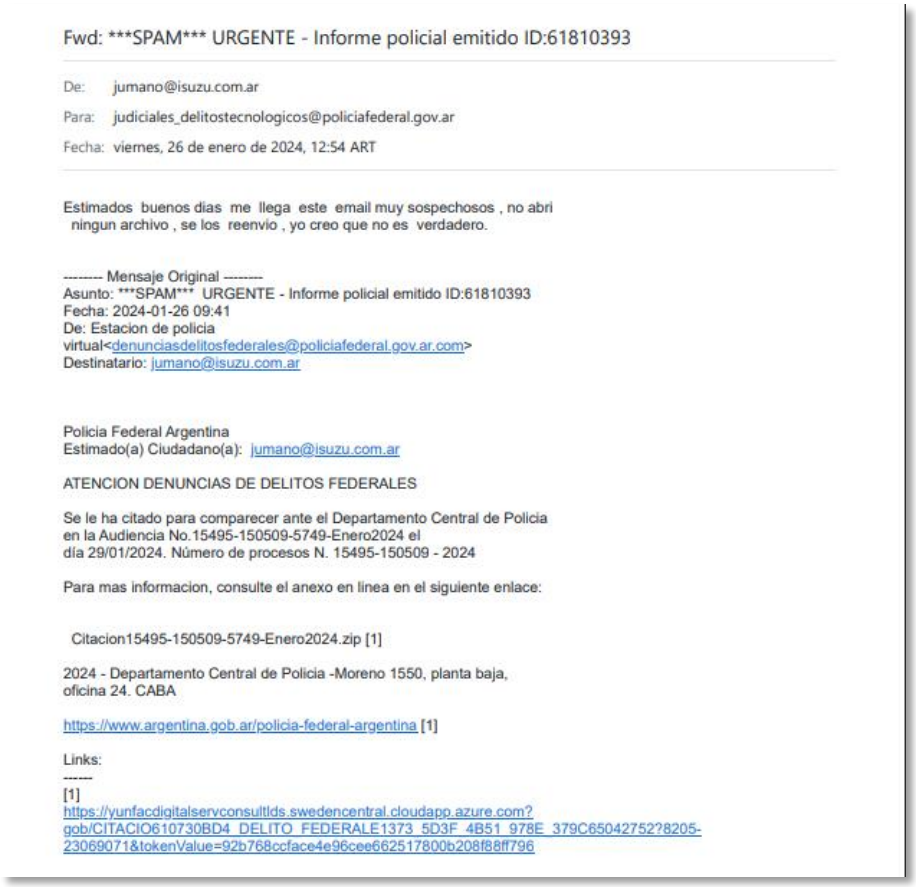
División DELITOS TECNOLOGICOS

Introducción

El día 06 de marzo del corriente año, se recepciono un correo electrónico proveniente de la cuenta judiciales_delitostecnologicos@policiafederal.gov.ar perteneciente a la División DELITOS TECNOLOGICOS, donde adjunta un archivo PDF solicitando colaboración de esta Dependencia para realizar el análisis de un link presuntamente malicioso.

Desarrollo

Una vez identificado el caso, se procedió al análisis del correo proveniente de "**denunciasdelitosfederales@policiafederal.gov.ar.com".** El mismo simula ser una comunicación oficial donde se cita al usuario para que se presente ante el "*Departamento Central de Policía*" aludiendo al Departamento Central de la Policia Federal Argentina, mencionando un número de audiencia y número de procesos.



Fwd: ***SPAM*** URGENTE - Informe policial emitido ID:61810393

De: jumano@isuzu.com.ar

Para: judiciales_delitostecnologicos@policiafederal.gov.ar

Fecha: viernes, 26 de enero de 2024, 12:54 ART

Estimados buenos dias me llega este email muy sospechosos , no abri ningun archivo , se los reenvio , yo creo que no es verdadero.

-------- Mensaje Original --------
Asunto: ***SPAM*** URGENTE - Informe policial emitido ID:61810393
Fecha: 2024-01-26 09:41
De: Estacion de policia virtual<denunciasdelitosfederales@policiafederal.gov.ar.com>
Destinatario: jumano@isuzu.com.ar

Policia Federal Argentina
Estimado(a) Ciudadano(a): jumano@isuzu.com.ar

ATENCION DENUNCIAS DE DELITOS FEDERALES

Se le ha citado para comparecer ante el Departamento Central de Policia en la Audiencia No.15495-150509-5749-Enero2024 el día 29/01/2024. Número de procesos N. 15495-150509 - 2024

Para mas informacion, consulte el anexo en linea en el siguiente enlace:

Citacion15495-150509-5749-Enero2024.zip [1]

2024 - Departamento Central de Policia -Moreno 1550, planta baja, oficina 24. CABA

https://www.argentina.gob.ar/policia-federal-argentina [1]

Links:
------
[1]
https://yunfacdigitalservconsultlds.swedencentral.cloudapp.azure.com?gob/CITACIO610730BD4_DELITO_FEDERALE1373_5D3F_4B51_978E_379C650427528205-23069071&tokenValue=92b768ccface4e96cee662517800b208f88ff796

Imagen 1. Cuerpo del mail.

Continuando con el análisis, dentro del cuerpo del mensaje, se pueden observar dos enlaces, en el primero https://www.argentina.gob.ar/policia-federal-argentina, redirecciona al usuario al sitio oficial de Policía Federal ARGENTINA descartando así que este se trate de un enlace malintencionado.

Mediante la herramienta FortiSANDBOX se analizó el segundo enlace hxxps://yunfacdigitalservconsultlds[.]swedencentral[.]cloudapp[.]azure[.]com?gob/CITACIO610730BD4_DELITO_FEDERALE1373_5D3F_4B51_978E_379C65042752?8205-23069071&tokenValue=92b768ccface4e96cee662517800b208f88ff796. Al ingresar al mismo, se observa una advertencia propia de la página, aludiendo inconvenientes con el certificado de seguridad.

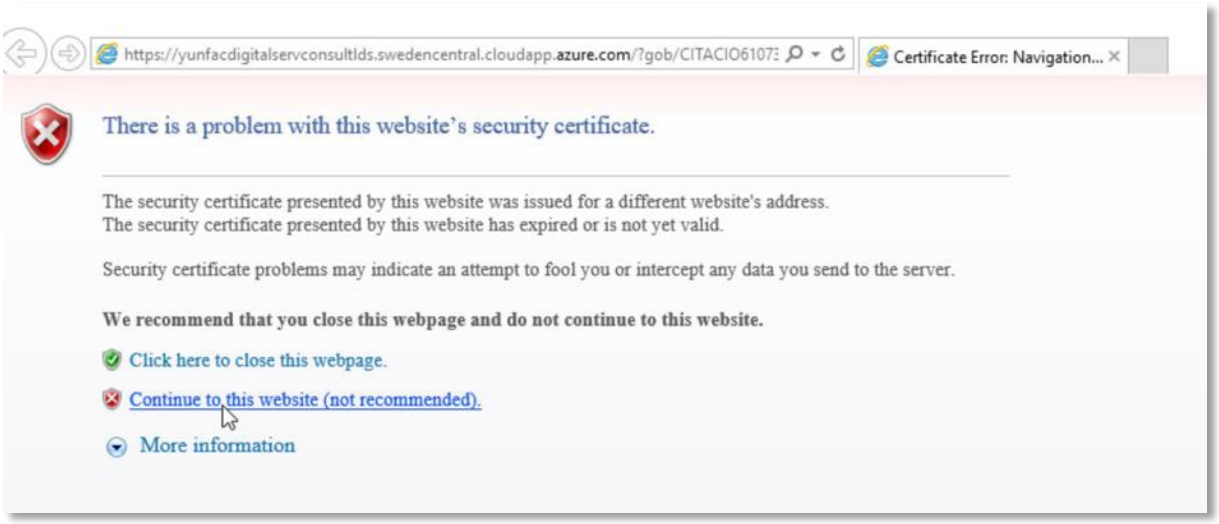


Imagen 2. Advertencia de seguridad.

Al acceder al enlace se descarga un archivo que se ejecuta automáticamente mostrando una ventana en blanco con el nombre **"dummy"**.

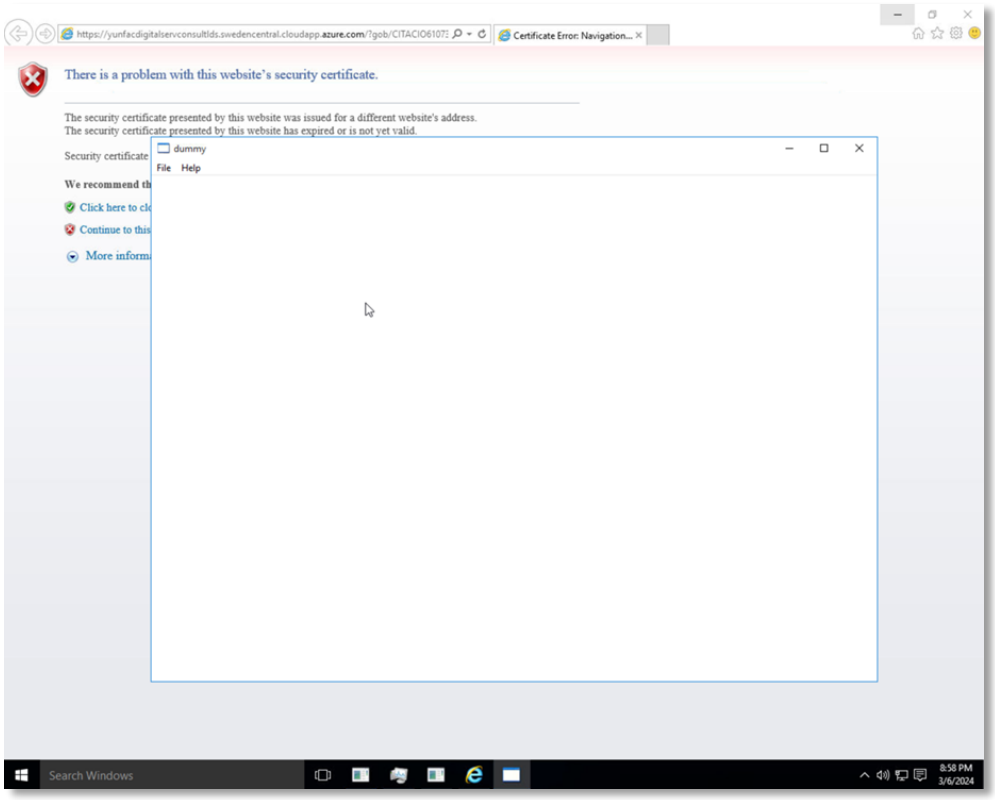


Imagen 3. Ejecución del archivo E104.exe.

Al revisar las aplicaciones que se están ejecutando en el administrador de tareas, encontramos una aplicación llamada "**E104**" y dentro del mismo se halla el proceso "**dummy**".

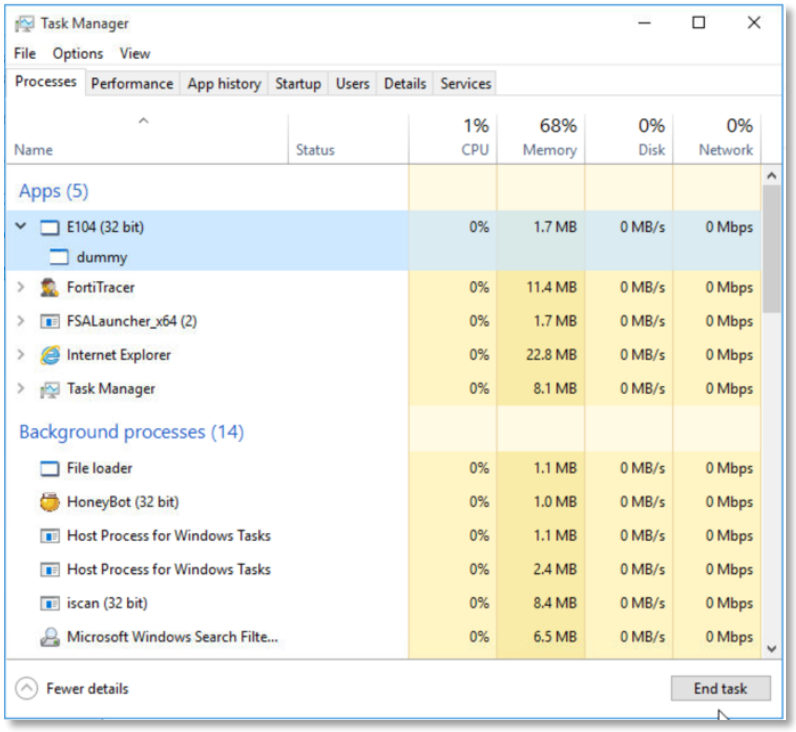


Imagen 4. Identificación de procesos dentro del administrador de tareas..

En este ocasión el archivo se llama "**E104.exe**", el cual se aloja en la siguiente ruta: dentro de los archivos temporales: "**C:\Users\Administrator\AppData\Local\Temp\FDM**".

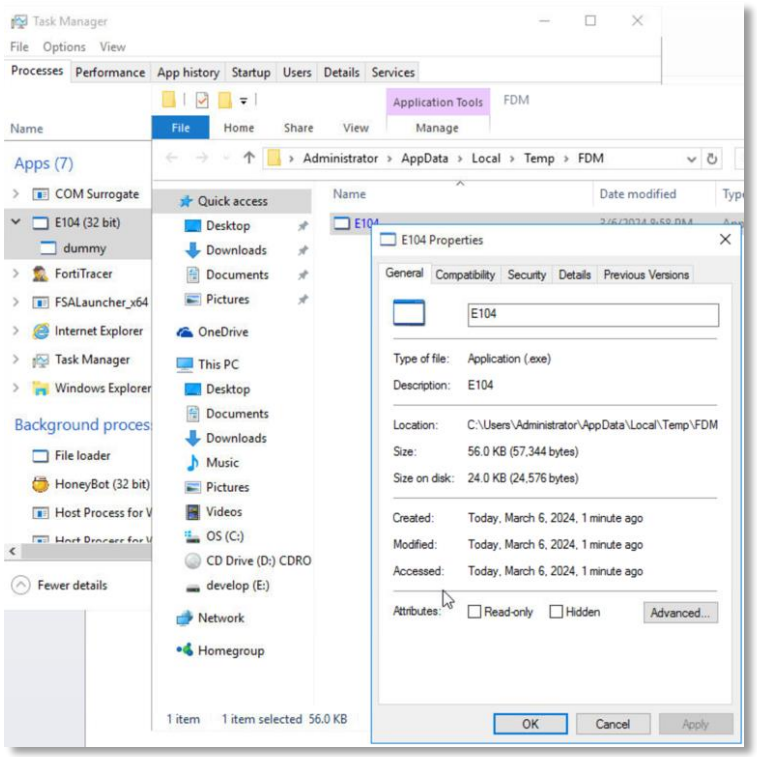


Imagen 5. Ubicación de archivo descargado.

A continuación se detallan los procesos que se ejecutaron al acceder al segundo enlace, en donde los que se encuentran en color rojo son los que se inyectaron en el equipo automáticamente.

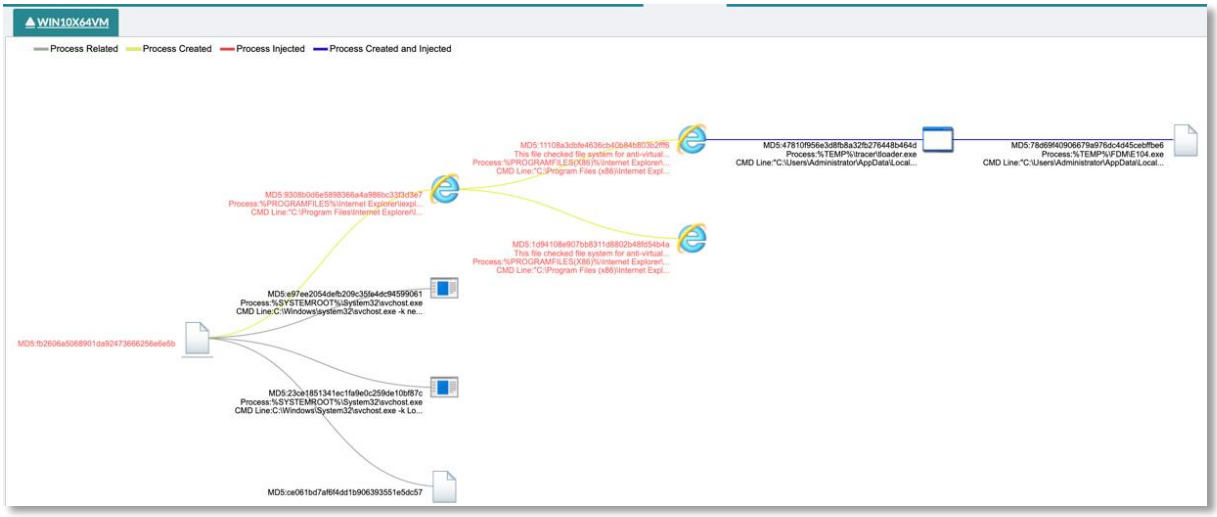


Imagen 6. Árbol de procesos de FortiSANDBOX

Se analizó en diferentes vendors el archivo ejecutable "**E104.exe**" el cual arrojó como resultado coincidencias con la descripción de malware tipo "troyano".

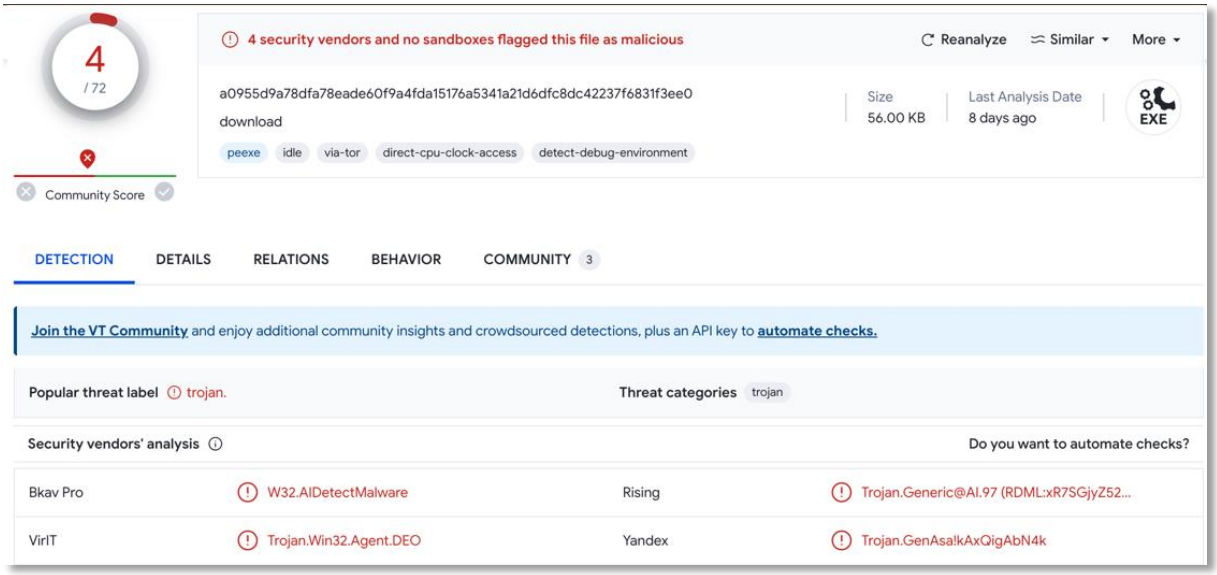


Imagen 7. Score de diferentes vendors de seguridad

Conclusión

En base a lo expuesto en el presente informe, y en referencia al enlace remitido desde el correo denunciasdelitosfederales@policiafederal.gov.ar.com enviado por la División DELITOS TECNOLOGICOS, se determinó que el dominio "@policiafederal.gov.ar.com" es apócrifo y que se trata de un malware tipo phishing. Este simula una citación para comparecer en el Departamento Central de la Policía Federal Argentina, y dentro del mismo un enlace el cual descarga un archivo ejecutable en la siguiente ruta "C:\Users\Administrator\AppData\Local\Temp\FDM", creando la carpeta "FMD" en los archivos temporales, modificando los registros del sistema.

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

En relación al dominio mencionado en NOTA 389-01-000584-2024 "policiavirtual@funcionpublica.com" no se adjunta información para su análisis

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.