Caso de análisis Malware bancario en Uruguay

Centro de Operaciones de Seguridad (SOC)

Datasec

Junio 2022

Contenido

Identificación y análisis del incidente

Una investigación fue llevada a cabo a raíz de una notificación por parte de un cliente de la firma, que había sufrido un incidente cibernético relacionado con su cuenta bancaria de un banco uruguayo.
De acuerdo al relato de la parte afectada, el mismo se habría desencadenado por haber interactuado con un correo electrónico (a través del programa Outlook) el cual fue reenviado por alguien de confianza, pero desestimado al fin.
Según nuestro análisis, el correo en cuestión debió lucir como este:

De: "Sr (a) jperez" <contabi@contabilida.trd.br>
Para: "j perez" <jperez@ejemplo.com.uy>
Enviado: Miércoles, 23 de Marzo 2022 3:27:59
Asunto: Notificación Procuradoria - Junta Departamental 03:27:58

Estimado socio:

Adjunto expediente sobre contribución inmobiliaria e impuestos de ascensores enviado por el ejecutivo, a aprobar por la Junta Departamental.

Archivo Adjunto - Notificación procuradoria

Por favor confirme el recibo , saludos.

En una primera vista del correo electrónico, se puede observar en los encabezados que el remitente tiene un dominio brasileño (.br), pero utiliza un alias genérico (Sr/a) que copia el nombre de usuario del destinatario (xxxxx). Por lo tanto, se evidencia que el emisor intenta pasar desapercibido como un usuario legítimo; en otras palabras, realiza una **suplantación de identidad (phishing)**.

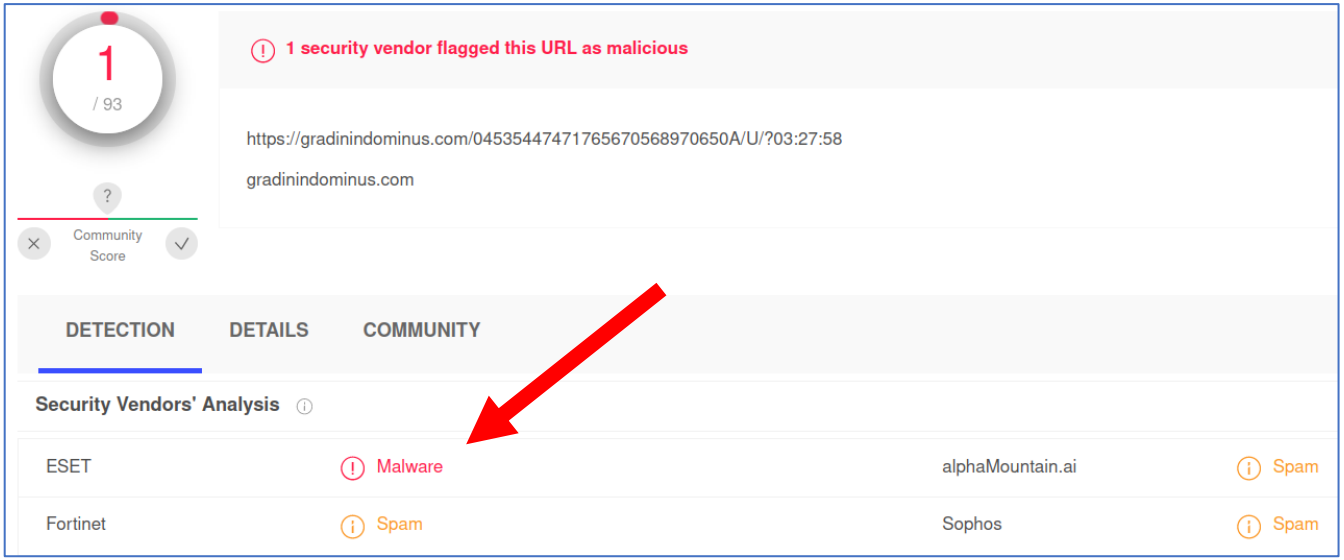
Analizando el contenido del e-mail, se observa la mención a un archivo adjunto, sin embargo, **no hay evidencia de que este haya sido adjuntado**. En su lugar, el mensaje provee un **enlace externo**.
Al abrir el código fuente del mensaje, se aprecia que el mismo está en formato HTML:

```
<html>
  <body>
    <b>De: </b> "Sr (a) jperez" &lt;contabi@contabilida.trd.br&gt;<br>
    <b>Para: </b> "j perez" &lt;jperez@ejemplo.com.uy&gt;<br>
    <b>Enviado: </b> Miércoles, 23 de Marzo 2022 3:27:59<br>
    <b>Asunto: </b> Notificación Procuradoria - Junta Departamental 03:27:58<br>
    <p></p>
    Estimado socio:
    <p></p>
    Adjunto expediente sobre contribución inmobiliaria e impuestos de ascensores enviado por el ejecutivo, a aprobar por la
    Junta Departamental.
    <p></p>
    <a href="https://gradinindominus.com/045354474717656705689706 50A/U/?03:27:58" rel="noopener" target="_blank">Archivo
    Adjunto - Notificación procuradoria</a>
    <p></p>
    Por favor confirme el recibo , saludos.
  </body>
</html>
```

En particular, es posible recabar que el enlace en cuestión dirige al sitio:

https://gradinindominus.com/045354474717656705689706 50A/U/?03:27:58

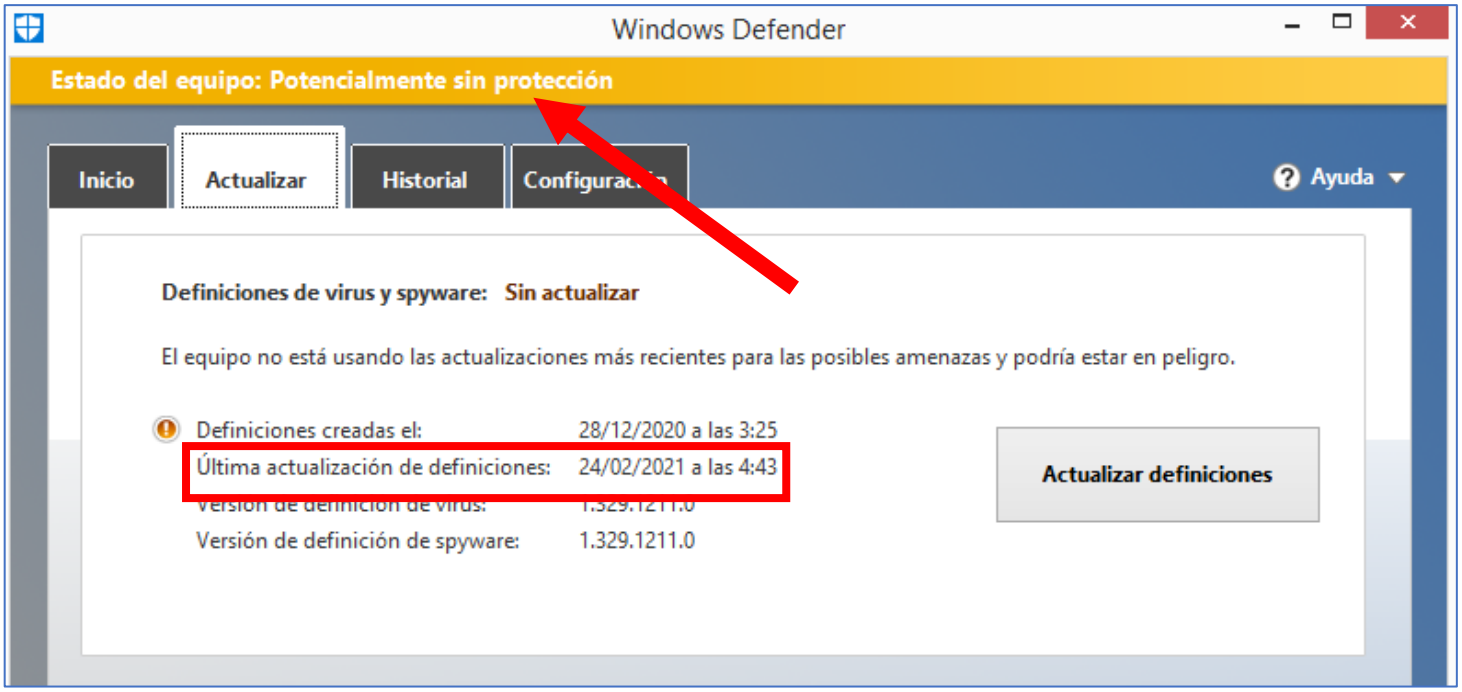
Al analizar esta URL con VirusTotal, se confirma la presencia de malware en el recurso:



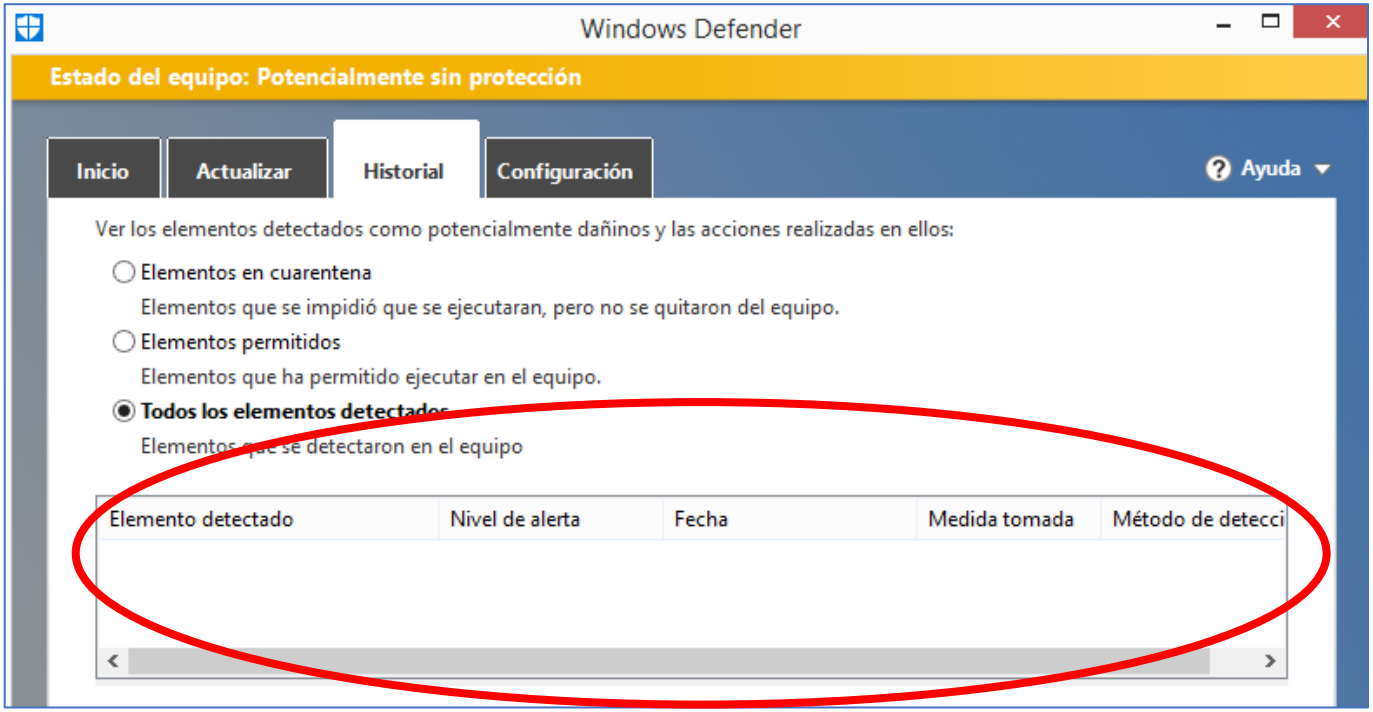
Por lo tanto, se procedió a escanear el sistema donde se produjo la afección.

Verificación de vectores de acceso y propagación

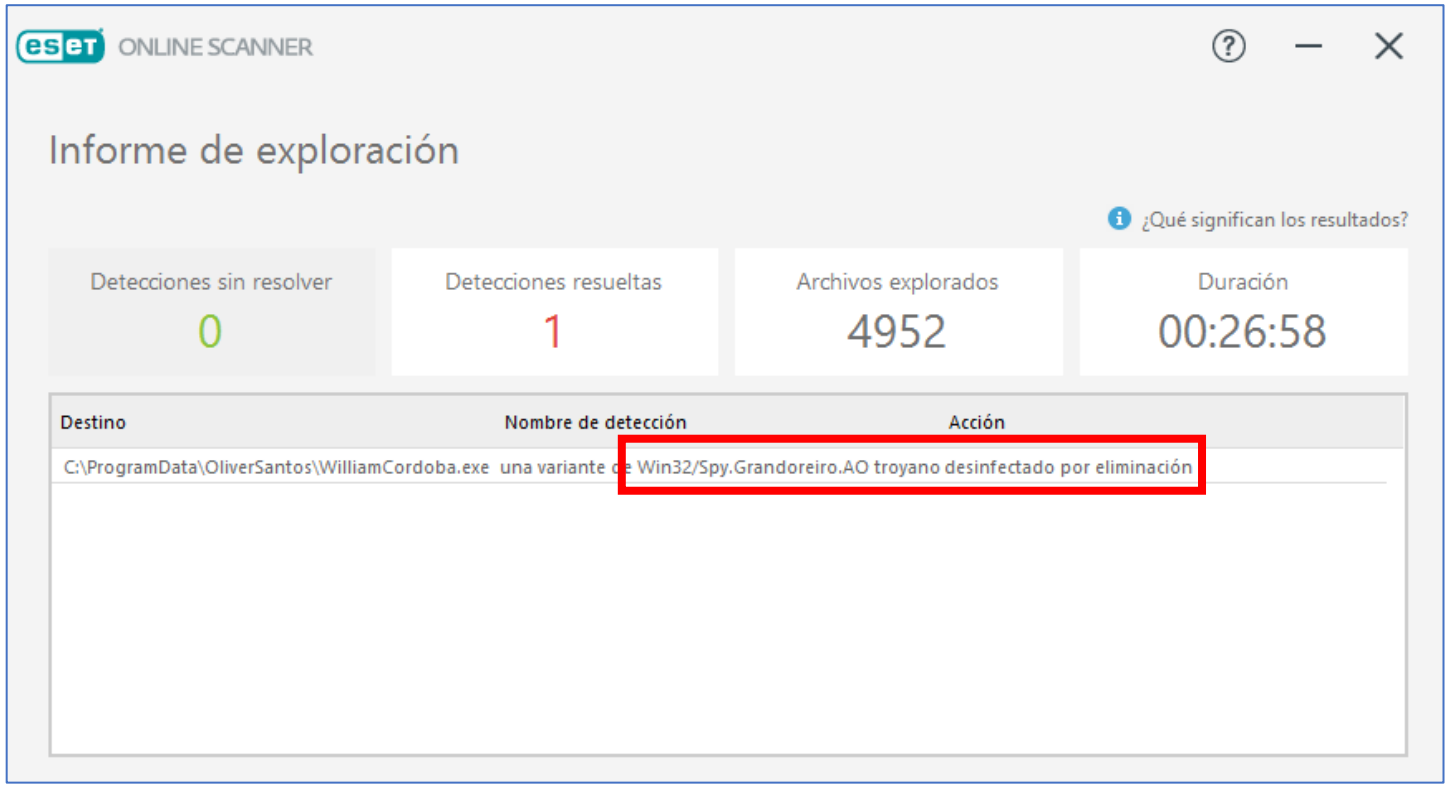
En primera instancia se pudo comprobar que la única protección con la que cuenta la computara de la parte afectada, es la más básica que está integrada en el propio sistema operativo: el antivirus Windows Defender. Sin embargo, como se exhibe en la próxima imagen, este programa se encontraba **sin actualizaciones desde hace más de un año**:



Dada la celeridad con la que se produce nuevo software malicioso, consideramos que la base de datos de este antivirus estaba obsoleta y, por tanto, **la protección del sistema contra amenazas era nula**. Tal como lo vaticinamos, yendo al historial de este antivirus se comprueba que jamás detectó algo:



Por consiguiente, más allá del criterio de la víctima para discernir un correo de phishing, queda claro que **el principal vector de acceso del malware al equipo, es su imposibilidad de frenar cualquier amenaza**. En virtud de esta deficiencia, y considerando que el análisis suministrado por VirusTotal mostró resultados con el antivirus ESET, se procedió a descargar la versión de prueba de ESET Online Scanner. Efectivamente, este antivirus encontró la carpeta donde se alojaba el ejecutable del malware, y acto seguido lo eliminó del sistema:



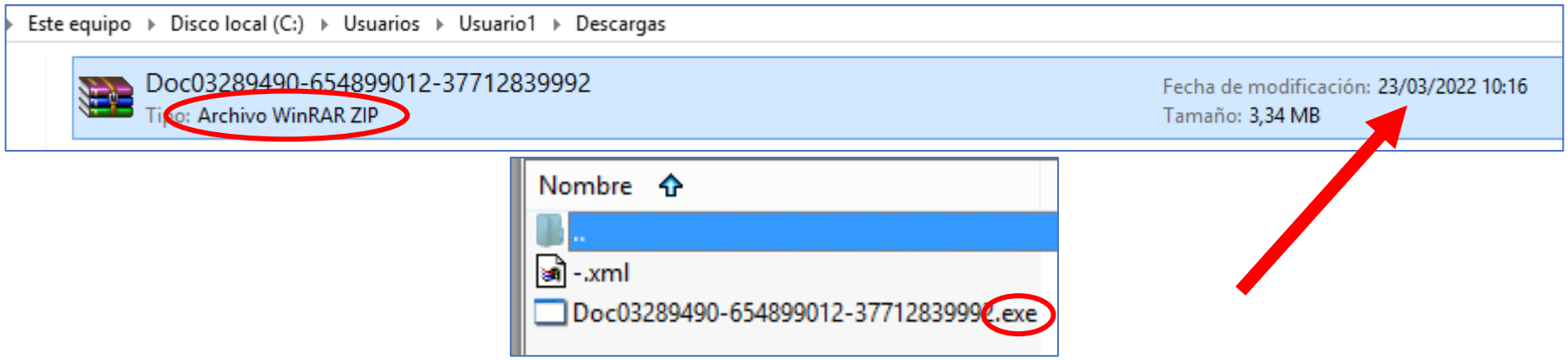
Concretamente, **la afección es el troyano *Grandoreiro***.

De acuerdo a nuestras averiguaciones, se trata de un spyware de origen brasileño, que una vez se instala en la computadora de su víctima, este se mantiene latente a la espera de que algún usuario ingrese por voluntad propia a alguna página bancaria y realice una transferencia. Cuando el programa detecta este comportamiento, captura los datos de la web y los modifica apropiadamente para redirigir la transacción monetaria y/o crear otra.

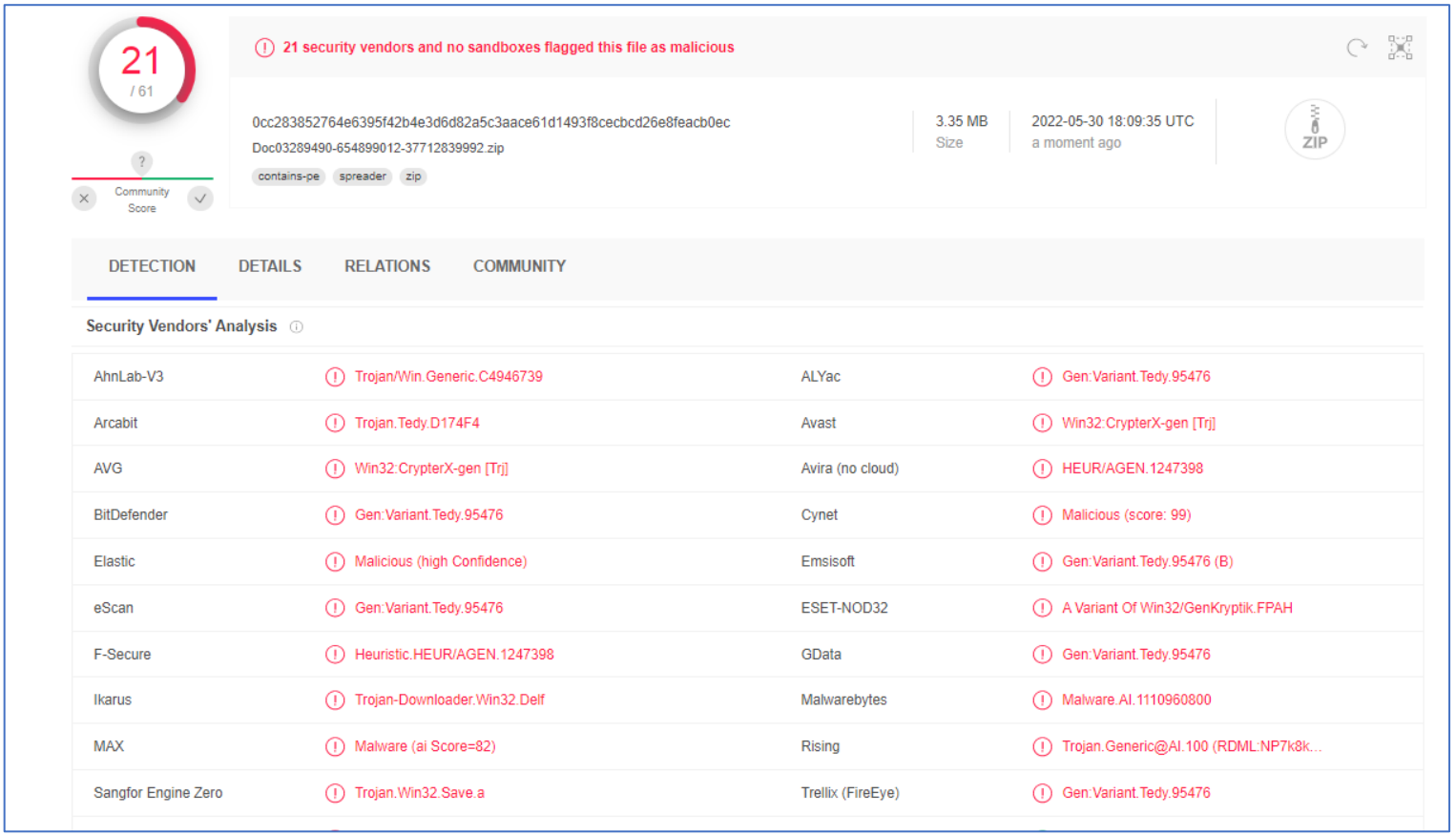
Esta descripción coincide completamente con el relato de la parte afectada.

Dado que el malware es bien conocido, fue posible recabar el dato de que la consecuencia inmediata de haber cliqueado el enlace del correo electrónico, habría sido la descarga de un archivo comprimido ".zip" que en su interior contiene un ejecutable que —por su nombre— intenta engañar al usuario como si fuera un documento.

Al explorar la carpeta de Descargas del equipo, efectivamente encontramos un archivo comprimido tipo ZIP, con fecha 23 de marzo de 2022 (la misma en la que se recibió el correo de phishing). En su interior, como era de esperar, se observa la presencia de un ejecutable (archivo ".exe") con un nombre sospechoso que comienza con "Doc":



Analizando el comprimido con VirusTotal, se comprueba que una gran cantidad de antivirus lo reconocen como malicioso, por lo tanto, nuevamente queda evidenciado que no contar con una protección de esta índole fue el principal vector de acceso del troyano:



En última instancia vale la pena aclarar que, por tratarse de un troyano, el ***Grandoreiro* no afecta otros archivos** almacenados en la computadora, dado que no tiene capacidad de replicación propia. Su vía de distribución es básicamente a través de correos de spam.

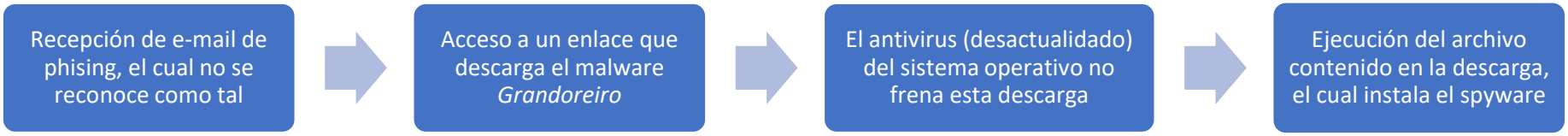
Sin perjuicio de lo anterior, no se descarta la posibilidad de que esta versión del malware contara con la capacidad de grabar las teclas presionadas por el usuario, con lo cual haya podido robar las contraseñas ingresadas en diferentes sitios web. Por lo tanto, recomendamos enfáticamente **cambiar sus contraseñas** en todos los servicios que utilice.

Calificación de impacto

El impacto de este incidente es **crítico**, ya que la naturaleza del mismo deja de manifiesto el poco conocimiento de la víctima sobre cómo prevenir estafas informáticas, y asimismo ella manifiesta haber constatado un débito considerable en su cuenta bancaria. Más aún, actualmente no está claro que el banco desde donde se produjo la estafa vaya a reintegrarle el dinero sustraído por los atacantes.

Acciones correctivas y recomendaciones

En base a toda nuestra investigación, resumimos la causa del incidente en el siguiente diagrama de flujo:



Luego, en base a esto podemos listar algunas acciones que —de aplicarlas— mejorarán su postura de ciberseguridad, y por tanto mitigarán la posibilidad de que incidentes como este se vuelvan a repetir:

- **Observar con detenimiento el origen de los correos**:

  A través del nombre de usuario (parte anterior al símbolo @), usted podría inferir si el emisor de un e-mail luce como alguien de su confianza o no. De igual manera, observando el servidor de correo (parte posterior al símbolo @) usted podría verificar

la presencia de elementos sospechosos, como por ejemplo, dominios países que no se corresponden con quien dice ser el emisor, o caracteres aleatorios que no forman ninguna palabra conocida para usted.

- **Verificar la coherencia del mensaje:**

  Si en el mensaje se le indica abrir un archivo adjunto, busque los elementos en la sección de "archivos adjuntos" de su aplicación de correo. Nunca cliquee en enlaces que dicen ser el archivo en cuestión.

- **Comprobar la integridad de los archivos adjuntos:**

  Tenga especial atención con los archivos terminados en ".exe", ya que este es el tipo de archivo correspondiente a los programas ejecutables de Microsoft Windows. En particular, esta es una terminación frecuente en los programas maliciosos que atacan a estos sistemas. Un documento de texto, una hoja de cálculo o una presentación de diapositivas, jamás deberían tener esta terminación.

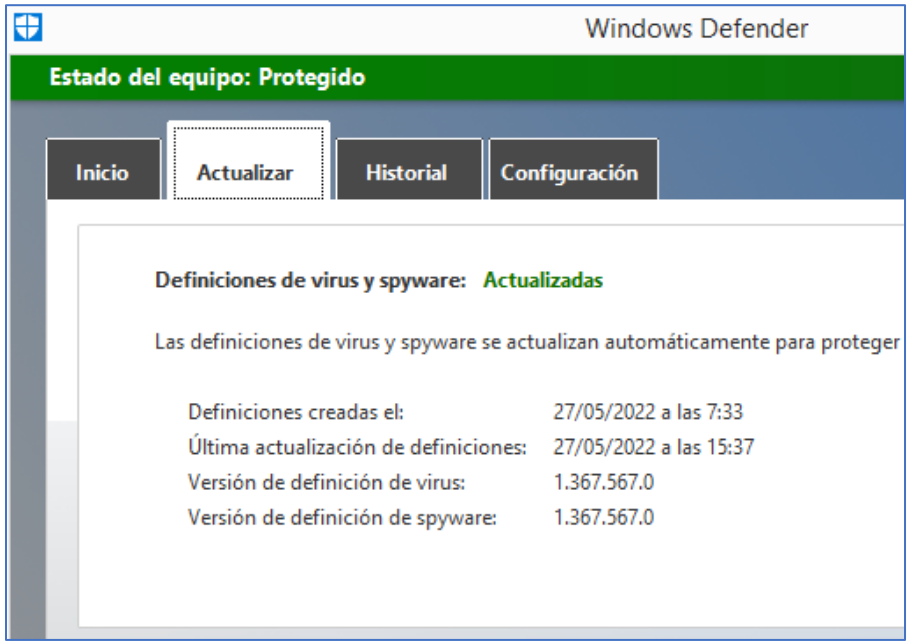
- **Trasladar correos fraudulentos a la carpeta de spam:**

  Una vez que usted detecta que ha recibido un correo electrónico con información falsa, mueva el mismo a la carpeta de spam, en lugar de limitarse a eliminarlo. Esto provocará que su aplicación de correo agregue el remitente malicioso a una "lista negra" interna, para así no volver a mostrarle mensajes provenientes de él.

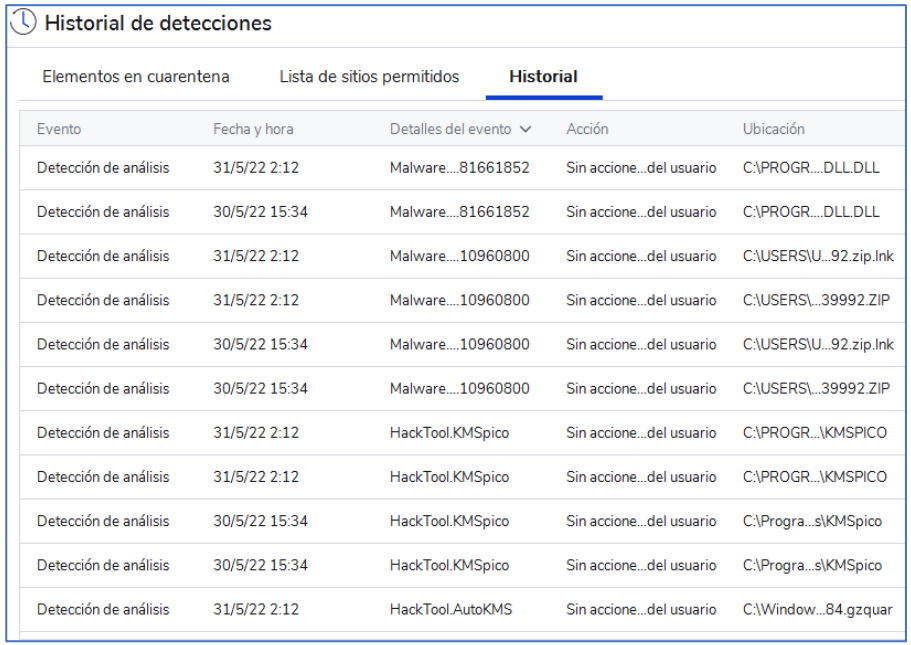
- **Instalar un antivirus en los equipos de trabajo, y mantener su software actualizado:**

  Siempre que adquiera un equipo para su organización, tenga la consideración de activar el sistema operativo (si esto le es requerido), descargar las actualizaciones disponibles, y —fundamentalmente— instalar un software antivirus. Datasec puede apoyar en estas tareas a través de sus servicios de remediación.

Finalmente, dejamos constancia que tanto el sistema operativo como el Windows Defender del equipo estudiado fueron actualizados, y se pasaron antivirus para liberarlo de esta y otras amenazas. Recomendamos que adquiera su propio antivirus para instalar cuanto antes en este equipo.



Windows Defender actualizado



Evento	Fecha y hora	Detalles del evento	Acción	Ubicación
Detección de análisis	31/5/22 2:12	Malware....81661852	Sin accione...del usuario	C:\PROGR....DLL.DLL
Detección de análisis	30/5/22 15:34	Malware....81661852	Sin accione...del usuario	C:\PROGR....DLL.DLL
Detección de análisis	31/5/22 2:12	Malware....10960800	Sin accione...del usuario	C:\USERS\U...92.zip.lnk
Detección de análisis	31/5/22 2:12	Malware....10960800	Sin accione...del usuario	C:\USERS\...39992.ZIP
Detección de análisis	30/5/22 15:34	Malware....10960800	Sin accione...del usuario	C:\USERS\U...92.zip.lnk
Detección de análisis	30/5/22 15:34	Malware....10960800	Sin accione...del usuario	C:\USERS\...39992.ZIP
Detección de análisis	31/5/22 2:12	HackTool.KMSpico	Sin accione...del usuario	C:\PROGR...\KMSPICO
Detección de análisis	31/5/22 2:12	HackTool.KMSpico	Sin accione...del usuario	C:\PROGR...\KMSPICO
Detección de análisis	30/5/22 15:34	HackTool.KMSpico	Sin accione...del usuario	C:\Progra...s\KMSpico
Detección de análisis	30/5/22 15:34	HackTool.KMSpico	Sin accione...del usuario	C:\Progra...s\KMSpico
Detección de análisis	31/5/22 2:12	HackTool.AutoKMS	Sin accione...del usuario	C:\Window...84.gzquar

Otras amenazas detectadas y eliminadas