Alerta de seguridad informática	2CMV21-00243-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Noviembre de 2021
Última revisión	03 de Noviembre de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware que proviene aparentemente de la Tesorería General de la República. El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

El mensaje del correo Informa que existen obligaciones tributarias impagas, por lo que debe regular la situación. El atacante adjunta un vínculo donde supuestamente puede revisar el informe detalladamente, sin embargo, al seleccionarlo la persona descarga el malware y al ser ejecutado en el equipo se gatillará la infección del equipo.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp

[www-data@vm139fpua.yourlocaldomain.com]
[www-data@vm176ezdv.yourlocaldomain.com]
[www-data@vm321qkus.yourlocaldomain.com]

Correo Electrónico
@vm139fpua.yourlocaldomain.com
@vm176ezdv.yourlocaldomain.com
@vm321qkus.yourlocaldomain.com

Asunto
Tesorería General de la República

IoC URL

http://www.secrata[.]be/_templates/default/css/2021/index1.php

http://viv[.]az/2C11L033/4C6GH1XD7J/CC0S244/323798/dow.php

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : C003I7GF0S8F920G600203.zip
SHA256 : 25D8C96E61388BB29EEA3FDA8E1A601A6842350B725E35A193468D8F2BE6368F

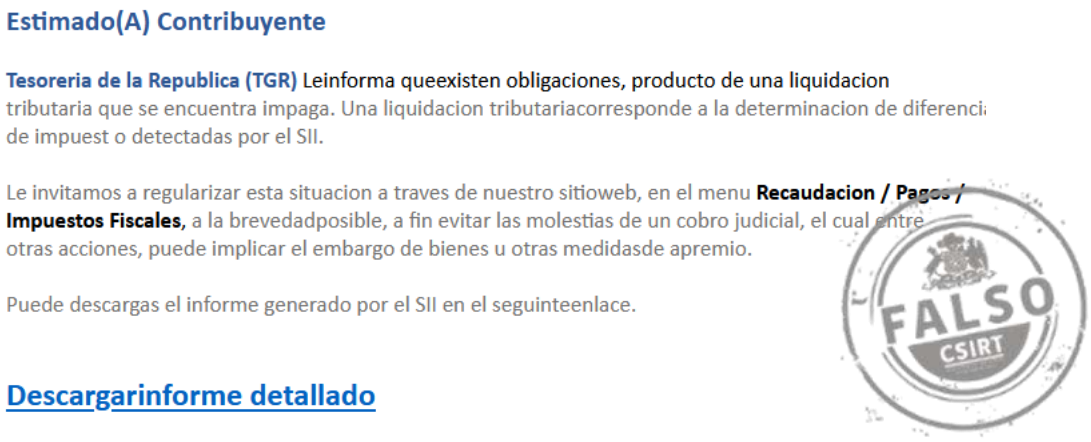
Nombre : C003I7GF0S8F920G600203.msi
SHA256 : 77E19EEB9AC37EFB541EF647F401A372F5ED2098690156AE6A42AE65B906DEA6

Nombre : HPDofzXZkq.dll
SHA256 : A15EE764618CC1AA648F341C0419B8A1FB933CD9DA404A27F385CE5FF8BA1405

Nombre : ls50U85K1K27YxuXbH88b17F7
SHA256 : AC0E0AAFCAB69E4F471BD8C7F91238EAD6931B8BAE074EC5852762AF551037C1

Nombre : Vk5OSNAZ1qGr0gp2STA6jj7mn
SHA256 : 945ADADA6CF6698B949359D9B395A5F905989D0D1EB84F537DE492ECC1263148

Imagen del mensaje



Estimado(A) Contribuyente

Tesoreria de la Republica (TGR) Leinforma queexisten obligaciones, producto de una liquidacion tributaria que se encuentra impaga. Una liquidacion tributariacorresponde a la determinacion de diferenci de impuest o detectadas por el SII.

Le invitamos a regularizar esta situacion a traves de nuestro sitioweb, en el menu **Recaudacion / Pagos / Impuestos Fiscales**, a la brevedadposible, a fin evitar las molestias de un cobro judicial, el cual entre otras acciones, puede implicar el embargo de bienes u otras medidasde apremio.

Puede descargas el informe generado por el SII en el seguinteenlace.

Descargarinforme detallado

Para mayor informacion, comuniquese con nosotros al 600 4000444 de lunes a viemes de 08:30 a 19:30 horas

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.03 09:22:37 -03'00'