Alerta de seguridad informática	2CMV21-0264-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de diciembre de 2021
Última revisión	23 de diciembre 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 supuestamente de la Tesorería General de la República (TGR).
El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.
Para convencer a su víctima, el falso correo informa que existen obligaciones tributarias impagas, por lo que debe regular la situación. Para esto, dispone de un enlace donde adjunta un supuesto informe, sin embargo, se descarga un malware, el cual al ser ejecutado 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

Correo electrónico
viv@viv[.]az

Servidor de correo
[159.69.42.89]

Asunto
Advertencia Tesorería General de la Republica (TGR)

IoC URL

http://viv[.]az/chat/domino/stone/mail/?cid//id/AQQkADAwATYwMAItZjIyAGUtZGU5My0wMAItMDAKABAAoMPyI%

54.193.3.31

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : TGR990606S5901J2311092.zip
SHA256 : 8A4EED8C0743024BD75892723167CB79C709EBA11398725ED80FCE4004D24062

Nombre : TGR990606S5901J2311092.msi
SHA256 : 8A17EF86BB6E20E5F814402EC29418A9CA40D02529C5099663206DFE2795B988

Nombre : qQbKLAAa.dll_1
SHA256 : 9a22ea7afb147c33a49ad8b521d1ee847db3710afc3ffe929a01db98026381d3

Imagen del mensaje

Fwc: Advertencia Tesoreria General de la Republica. (TGR) - (931071917060)

TGR 35855864@Contacto-TGR.cl

Para

FALSO CSIRT

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 diferencias

de impuesto detectadas por el SII.

Le invitamos a regularizar esta situacion a traves de nuestro sitioweb, en el menu **Recaudacion / Pagos /**

Impuestos Fiscales,

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 viernes de 08:30 a 19:30

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: 2021.12.23 15:14:52 -03'00'