Alerta de seguridad informática	2CMV22-00284-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de marzo de 2022
Última revisión	16 de marzo de 2022

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 de Gobierno) ha identificado una nueva campaña de phishing con malware. El mensaje que proviene, supuestamente, de la Tesorería General de la República (TGR) informa que existen obligaciones impagas y que puede revisar el informe generado por la TGR en el archivo adjunto, ingresando la contraseña que se indica en el correo. Al descargar el archivo y ser ejecutado, se gatilla la infección del equipo.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto
Fw:enc: Informe de liquidacion tributaria.

Correo electrónico
viv@viv.az

Servidor de correo
[159.69.42.89]

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: PDF-0027430505S3B101lF3.zip
SHA256: 5C4E6F90364DFEB19C1E7EA55B516F8BA211B2DCE1FF4F93B7C8DD32A61F2CC6

Nombre: PDF-0027430505S3B101lF3.exe
SHA256: 85EB1D4FD5DC78552361BB1DA4422C0865BBAE3784470C2FAA551E461FB35D52

IoC URL

https://5aa20a4eab0b.ngrok[.]io/PDF-0027430505S3B101lF3.zip

https://makeupkala[.]com/well-known/acme-challenge/l/z/c218B3505l1016S502i3.zip

https://zakatalquds[.]org/profiles/contts/hd218b0s5S20d1l322cj.php

Imagen del mensaje

✓ Fw:enc: Informacion de Liquidacion Tributaria - (245726088993)

CT Contacto-TGR 18019515 @ TGR.cl
Para [redacted]

TGR
Tesorería General de la República

Estimado(A) [redacted]

Tesorería General de la Republica (TGR) informa que existen obligaciones, producto de una liquidacion tributaria que se encuentra impaga. Una liquidacion tributaria corresponde 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**, a la brevedad posible, 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 descargar el informe generador por el TGR en el Adjuntos de información.

Adjuntos de información

Atencion: Informe contraseña para ver su PDF. Nunca le des tu contraseña a nadie.
contraseña : 0032022

15/03/2022 09:34:53

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: 2022.03.16 16:22:20 -03'00'