Alerta de seguridad informática	2CMV22-00296-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 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

Tesorería General de la Republica (TGR) informa que existen obligaciones pendiente

Correo Electrónico

[mssce@server.ony.oyo.mybluehostin.me]
[lynxaviacao@lynxaviacao.com.br]
[mw2pqgpp93@kawahara-law.jp]
[webmaster@24service.co.il]

Servidor de correo

[server.ony.oyo.mybluehostin.me]
[plesklinux01.mandic.com.br]
[kawahara-law.jp]
[vmi827000.contaboserver.net]

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: TGR01400123.zip
SHA256: 03840e262fc8208312074c8c0cc5790c586516c1d36536425f52a0768d69021e

Nombre: TGR01400123.msi
SHA256: 9181e3ecde1ea8f60d4eb0c16f760c51a3f099766bcca1eb9ad19136894a5ada

Nombre: JSON.ahk
SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f

Nombre: libeay32.dll
SHA256: cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967

Nombre: lock.txt
SHA256: 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b

Nombre: ssleay32.dll
SHA256: 754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f

Nombre: ssleay32.dll
SHA256: 754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f

Nombre: vergj8.ahk
SHA256: 16addd40397c045ed4c393f83443a10cb583171e2fe1f95782e06276db474adb

Nombre: vergj8.exe
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: HD812U1NDS71Y.zip
SHA256: 880a365b8d47729b16359bd90136ecbc176e3191eba9a7f18f6285a0cf624620

Nombre: eRQXHtKAjj.aoc
SHA256: ea972fdc38c685ace5c5a23b849ac673825e7e4d257bb5b06312ec43c1645400

Nombre: iiVB08bwtpe95Do670Co2ggg
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

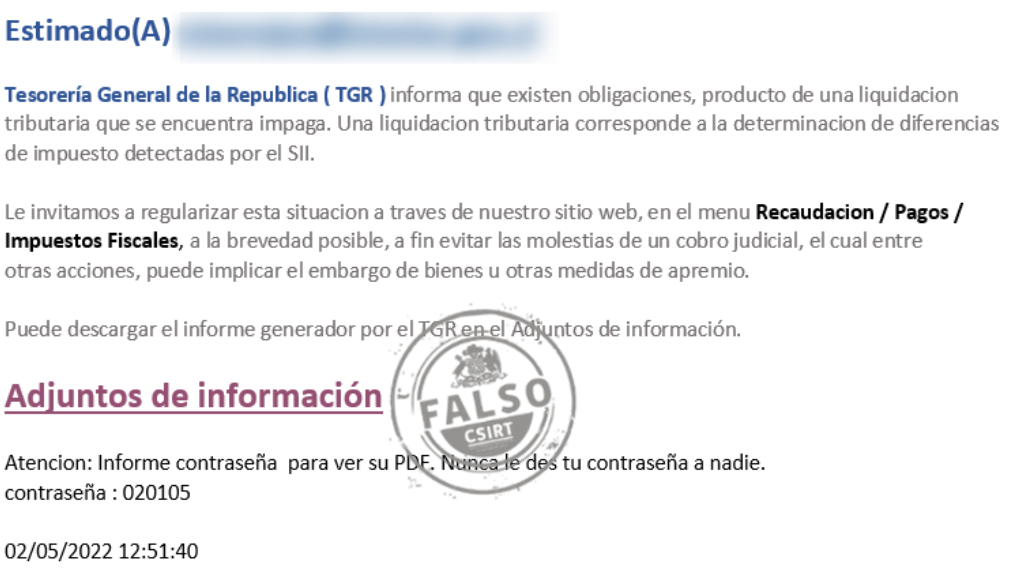
Nombre: lIz4U8voSwZS0ILP3F6Hdchhh
SHA256: 610ce9c0087f8b7a87cb839efe47338121d5681d4a4bd8f248acfc6c29969c47

IoC URLS

https://physionormandie[.]com/wp-content/languages/--/https:/www.tgr.cl

https://www.tri-techmechanical[.]com/components/com_config/dad/HD812U1NDS71Y[.]zip

Imagen del mensaje



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 sitio web, 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 medidas de 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 : 020105

02/05/2022 12:51:40

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: 2022.05.02 12:41:05 -04'00'