Alerta de seguridad informática	2CMV22-00287-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de marzo de 2022
Última revisión	22 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 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
Fw:enc: Informacion 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: 003BF101I702T5V6Di920C55s.zip
SHA256: 3316B967FFBE7806CCEC9E58C7991092BFD7BA35C8433B8D66BD2818AF6FB66B

Nombre: 0033B101I702T5v6Di920.msi
SHA256: 7C3265CA51A663AFF433106C49303EDEBE6D7129748DB603DEB9D72FCAEA4375

Nombre: software.exe
SHA256: 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4

Nombre: software.ahk
SHA256: 853985D2A30CBAF89A21A0198B63475D3FE50718E9D6A28948E604578DFF4CA5

Nombre: 10f3eZ79s5091ks202Ns.zip
SHA256: CA79C0C2A3F3C80BB8DFE22F0E3E4EEE778E8AFFA095BF25F7A76A14AF40B5B0

Nombre: BQsCWdQapA.dll
SHA256: 4F3F8F99DDECA9006024287F7A1DCA881AD2784F15FE055040B23AE743F372E9

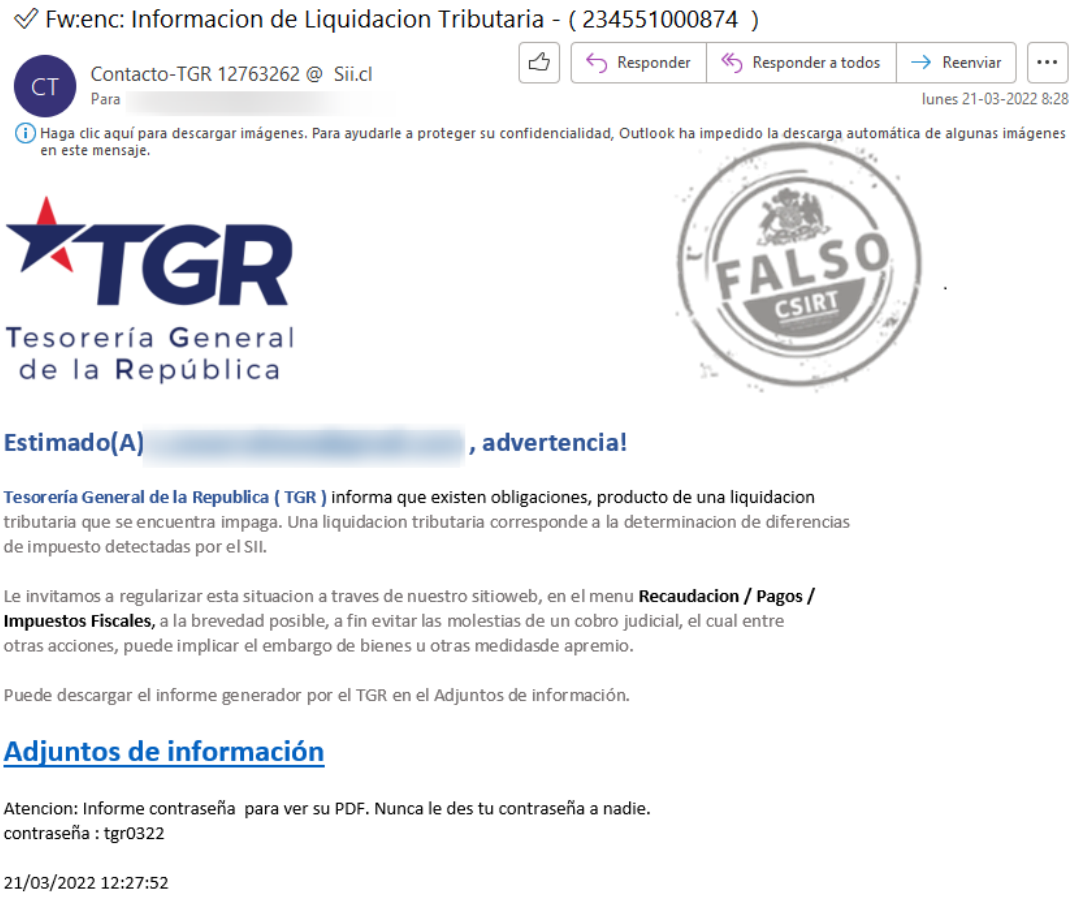
Nombre: G9hIZ0oqtDjRydX1D4mmKevobbb
SHA256: 8341BAAB4C8A940C780FBF2D427026616D3ED76B8C7568448F09768F35887BCC

Nombre: Ti8bskrfO94gpXDO0aaa
SHA256: 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4

IoC URL

http://54.242.169.255/imbox/?mail/u/0/#inbox/FMfcgxwLtkcJcnBvtbzkZMVxLsXfPCXv
https://dkloja.com.br/signup/file/10f3eZ79s5091ks202Ns.zip

Imagen del mensaje



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: 2022.03.22 11:34:28 -03'00'