Alerta de seguridad informática	2CMV21-00144-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Febrero de 2020
Última revisión	11 de Febrero de 2020

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. El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

El mensaje del correo indica que se adjunta un informe generado por el Servicio de Impuestos Internos, ya que la Tesorería General de la República informa que existen obligaciones impagas.

El atacante adjunta un vínculo para ser seleccionado y de esa forma descargar el archivo malicioso, el cual al ser ejecutado 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:

Servidor Smtp

[dns3.sgpnet.com.br]
[host.netpix.com.br]
[epsilon.imcconseil.fr]
[smtp-sp217-160.kinghost.net]
[smtp-sp217-19.kinghost.net]
[smtp-sp217-112.kinghost.net]
[smtp-sp217-168.kinghost.net]
[smtp-10c.idc2.mandic.com.br]

Correo Electrónico
[contato@rgbviagens.com.br]
[suporte@akinternet.com.br]
[mmca@64149hpv095002.ikoula.com]
[imprensa@engenhodanoticia.com.br]
[fabio.bastos@emilcardio.com.br]
[compras2@postochegadao.com.br]
[alex@gnorte.com.br]
[domingos@nordestao.com.br]

Asunto
Enc: Notificación - Tributaria al Contribuyente

IoC Archivo Adjunto

Archivos que se encontraban adjunto en el correo

Nombre : TGR_03002170038Bi1.zip
SHA256 : F3F9F269C75D5F7085A3D401C83600EE14E1D6920F60336D864BF38C211438E8

Nombre : TGR_03002170038Bi1.msi
SHA256 : AA295649CBF6159FE91D2CEBC2E641988D827EF37B7C7BF0D1273C5A2C9737A4

IoC Comunicación de Red

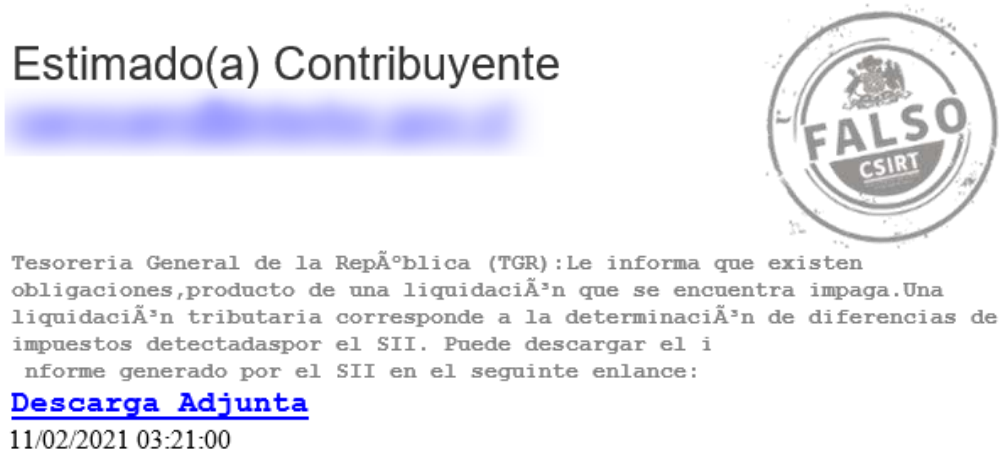
URL

https://selfhelpwomendevelopment[.]com/wp-includes/images/mail/descarga[.]php

http://www.aralimp.com[.]br/wp-content/upgrade/pixes/TGR_03002170038Bi1[.]zip

104.214.107[.]176

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: 2021.02.11 16:46:41 -03'00'