Alerta de seguridad informática	2CMV21-00157-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Marzo de 2021
Última revisión	24 de Marzo 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 supuestamente proveniente del Servicio de Impuestos Internos. El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp
[3.18.31.46]
[192.99.45.147]

Correos Electrónicos
gitadmin@janusapps.com.mx
rgarcia@globalproventus.com

Asunto
Segundo Aviso: Regularizar situación fiscal.

IoC Archivo Adjunto

Archivos que se encuentran en la amenaza

Nombre : FACTURA_A2043.zip
SHA256 : 1C4FEB5B1CF3132C0B426F6FFC47E33B5E0EB163AFBC9DD1828B8546B94FF0F9

Nombre : FACTURA_A2043_24-03-2021.zip
SHA256 : 80DFB1D76D1F6E7BDB44E101EEC5F49FB6988FDA14A78B0E8689C361C93A2CCF

Nombre : FACTURA_A2043_59062.exe
SHA256 : 3A58CF08A6046804EA9F1CD262474C82DA2A249E41BF47534A48E2747BA69228

IoC Comunicación de Red

URL

https://facturasenlinea[.]icu/

https://grandmining[.]mn/wp-includes/rest-api/endpoints/898/index.php

IMAGEN DEL MENSAJE

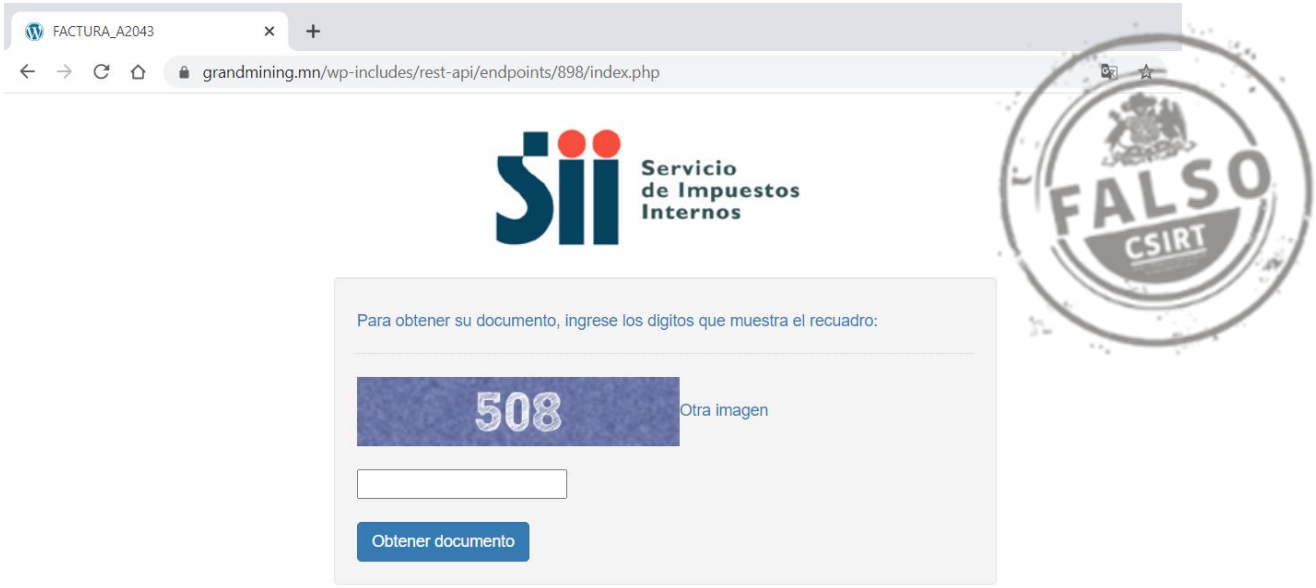
Servicio de Impuestos Internos

Segundo Aviso:

Fecha: 23-marzo-2021
Estimado:

El **Servicio de Impuestos Internos** se ha percatado que en diversos despachos alrededor del País, Ud. ha propuesto esquemas para **evadir el pago de impuestos** y hemos detectado **anomalías en su situación fiscal.** Para evitar una sanción en su contra que puede ser **una multa de hasta 50 UTM,** le recomendamos revisar su factura en el siguente Enlace.

IMAGEN DEL SITIO WEB



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: 2021.03.24 16:41:48 -03'00'