Alerta de seguridad informática	2CMV20-00041-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2019
Última revisión	08 de Enero de 2019

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), con la colaboración del usuario @JosePablo_PUQ, han identificando una campaña de malware que utiliza el nombre de la Tesorería General de la Republica.

El mensaje del malware, alojado en un sitio fraudulento, informa a la víctima que existen obligaciones tributarias impagas detectados por el SII.

La amenaza se pudo identificar en un sitio web, el cual, al momento de ingresar, automáticamente descarga el archivo ZIP. Al descomprimir el archivo se obtiene otro archivo con extensión ejecutable MSI. Al ser ejecutado se gatilla un script que descarga del malware.

Indicadores de compromisos

Url's:
http[:]//peronopuestaessa[.]email/trabajo/
http[:]//www[.]fertitec[.]com[.]br/es/look/J0kill3M[.]zod

Archivos adjuntos.

Archivo : C000000002020TGR.zip
MD5 : ee74abe73e0257ba5240a58e151121b1

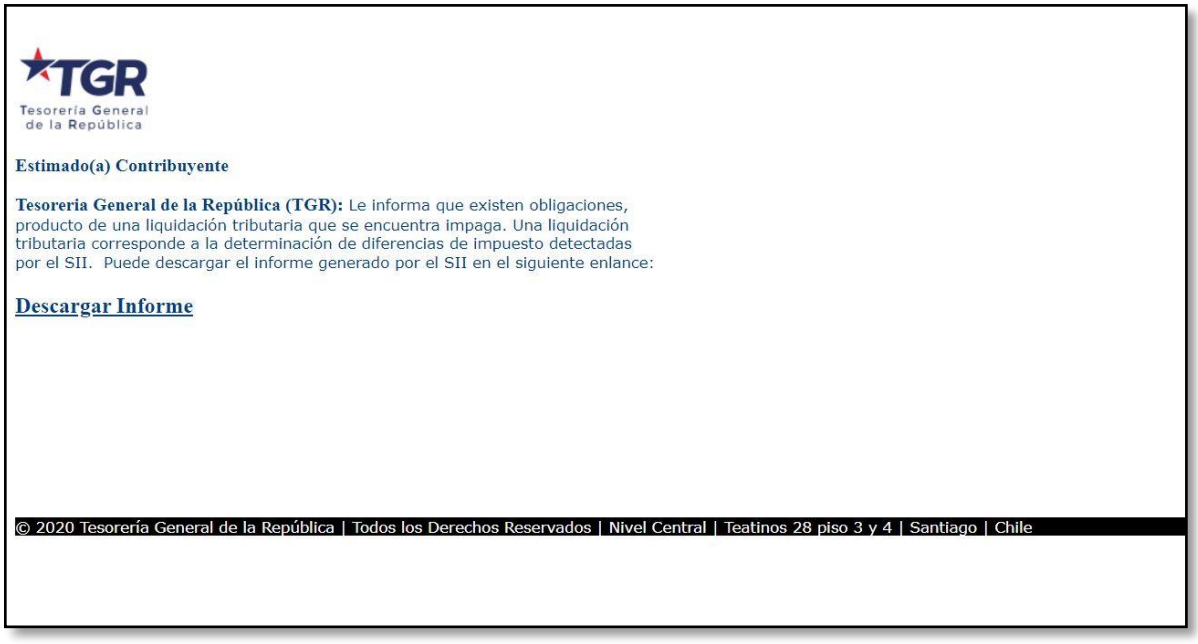
Archivo : C000000002020TGR.msi
MD5 : aba91470ed1dfd8923af22d9a6bc351d

Archivo : ZUH2HW8HNCS6ZWKSPRD2GUFRUVN2X
MD5 : 8eb00ef9a3c67cdb3de0361cf8067d05

Archivo : FRHVW4N246XYTWI22JF7J3IE0TJFOM2G
MD5 : 6002b99633116d3d95e3b3398a509138

Archivo : C8423BQH5D13293RASHQQH93GDHD38OU4CK
MD5 : c56b5f0201a3b3de53e561fe76912bfd

Imagen Mensaje



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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