Alerta de seguridad informática	2CMV20-00049-01
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 a través de un correo electrónico que utiliza el nombre de la Tesorería General de la República. El mensaje del correo indica que existen obligaciones de deuda producto de una liquidación tributaria que se encuentra impaga.

En el mensaje se agrega un enlace que, una vez seleccionado, descarga un archivo ZIP. Al descomprimir el archivo se obtiene otro archivo con extensión ejecutable MSI. Al ser ejecutado, se realiza un proceso falso de instalación, pero en realidad se gatilla un script que descarga el malware.

Indicadores de compromisos

Servidor Smtp
[13.84.134.242]
[13.92.255.204]
[23.99.97.237]
[23.101.210.70]
[40.69.28.21]
[40.78.44.186]
[40.78.128.224]
[40.89.156.120]
[40.89.177.122]
[40.113.84.152]
[51.143.7.33]
[51.144.134.131]
[52.141.6.62]
[52.175.64.57]
[52.177.64.12]
[52.178.101.205]
[52.187.1.120]
[52.187.171.123]
[52.231.54.87]
[52.250.14.83]
[65.52.13.104]
[102.37.13.146]
[102.37.14.216]

Sender
www-data[@]live[.]com

Asunto
Tesoreria General de la República (TGR)

Url's:
http[:]//tgrestado[.]xyz/home/

IP:
[34.216.250.212]
[172.217.4.238]
[18.204.210.148]

Archivos adjuntos.
Archivo : l11022020001508Bl.zip

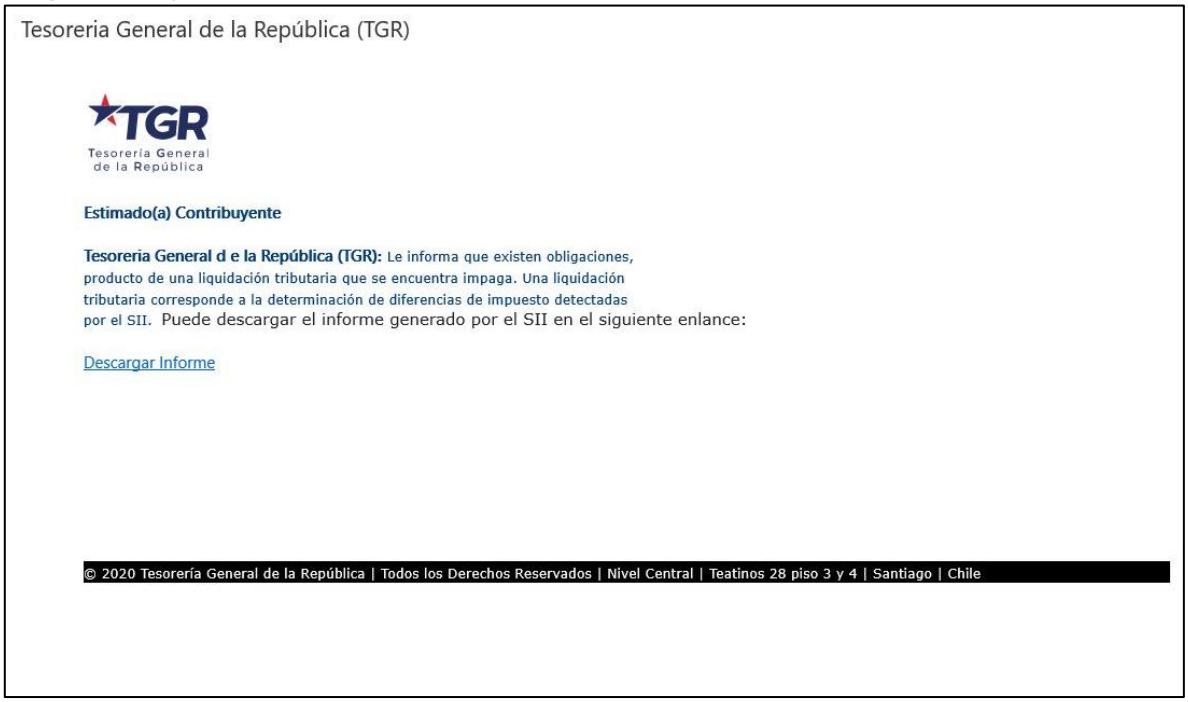
SHA-256 :90DD31A63B4968E279D0C8FB0646C8668BED5361ACCDBFA60B578DC4A2DF568F

Archivo : IMG--1102202015206004.msi
SHA-256 : F088D595398D7C79065F2392D5075BE8523E5CA79372A5EC407174F5BA924101

Archivo : msiexec.exe
SHA-256 : 83D965138A2FC05F5A403D43C9425AFC1360EB793B3D94C64037F0F848467E22

Archivo : 4eGeVYCm.exe
SHA-256 : 237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D

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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.11 19:22:28 -03'00'