Alerta de seguridad informática	2CMV20-00046-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Enero de 2020
Última revisión	31 de Enero 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 producto de una liquidación tributaria que se encuentra impaga.

En el mensaje se agrega un enlace a través del cual se descarga un archivo ZIP. Una vez que se descomprime 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
[45.90.57.38]
[45.90.57.42]
[45.90.57.41]

Sender
root@per.com
root@ver.com

Asunto
Segundo Aviso (TGR) 2020

Url's:
https[:]//fastupload[.]co/3834
https[:]//fastupload[.]co/down/3834/TVRrd0xqSXhOUzR6Tmk0NU13PT0=
www[.]paunocudoreport[.]com/service/LCE4YCLAP4ZXJ55[.]php
lifedeltalagoon[.]eu/proyectos/setentaetres[.]ire

Archivos adjuntos.
Archivo : VV-TGR02020.zip
MD5 : a1c29a91fae15f38eed5b4ad53472660

Archivo : VV-TGR02020.msi
MD5 : e85b595247cc5e54cce968f2b0e1b55e

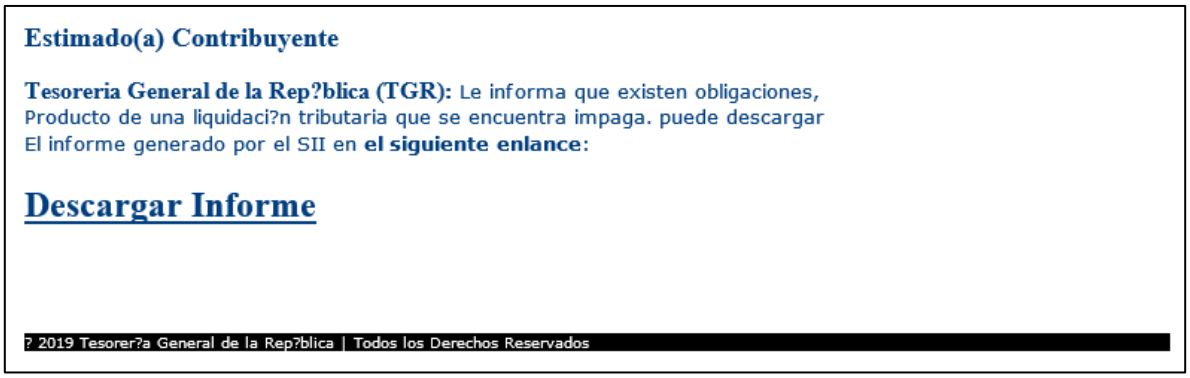
Archivo : setentaetres.ire
MD5 : 600b669c1cbfc5abceb6874d6965dbc3

Archivo : OOKX5JYDX5KREW3CRSOWBELAOOXPMPIYL1LB
MD5 : 84bdcb85ccc185bfe9a0daace0661e6e

Archivo : WI54E4FRMSJKF04EM76ORU5ZWH07293KKKXF0L
MD5 : c56b5f0201a3b3de53e561fe76912bfd

Archivo : YVXL5RLUKW2VIC78R22H2UAGII4YPCKWE48
MD5 : 84904f89b3a057f54f4ce553c84a5c28

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: 2020.01.31 20:12:12 -03'00'