Alerta de seguridad informática	**2CMV-00037-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**31 de Octubre de 2019**
Última revisión	**31 de Octubre 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), ha detectado la activación de campañas de phishing con malware asociado, a través de correos electrónicos que suplantan a la Tesorería General de la Republica y a la empresa de telecomunicaciones ENTEL.

En los dos casos el delincuente busca engañar a los usuarios para que estos seleccionen el enlace indicado para infectarse del Malware Bancario. En el caso de la Tesorería General de la Republica existen dos correos circulando. Uno ínsita al usuario para que descargue un Informe tributario que se encontraría impago. El segundo correo informa que se realizó una transferencia electrónica de Fondos (TEF) y trata de persuadir al usuario para que descargue el archivo de transferencia. En relación a la empresa ENTEL en el correo se informa al usuario que tiene una factura correspondiente al tráfico móvil del mes de Mayo, invitando al usuario para visualizar o cancelar la factura.

Indicadores de compromisos

Url's:

https[:]//espacoriodalua[.]com[.]br/erros/express/chile[.]php
http[:]//18[.]209[.]163[.]113/cont/puma[.]php
http[:]54[.]198[.]30[.]41/pela/c3meNt0[.]kok

Sender

www-data@0005[.]disparosnwes[.]com
www-data@[Ip de los Smtp]

Smtp Host

li1149-45[.]members[.]linode[.]com	[45[.]79[.]50[.]45]
li1137-243[.]members[.]linode[.]com	[45[.]79[.]38[.]243]
li1157-144[.]members[.]linode[.]com	[45[.]79[.]58[.]144]
li1971-177[.]members[.]linode[.]com	[172[.]105[.]16[.]177]
li1961-110[.]members[.]linode[.]com	[172[.]105[.]7[.]110]
li1569-27[.]members[.]linode[.]com	[139[.]162[.]89[.]27]
1881-144[.]members[.]linode[.]com	[172[.]105[.]227[.]144]
li1982-106[.]members[.]linode[.]com	[172[.]105[.]27[.]106]
li1968-101[.]members[.]linode[.]com	[172[.]105[.]13.101]
li978-184[.]members[.]linode[.]com	[45[.]33[.]24[.]184]
li693-189[.]members[.]linode[[.]]com	[23[.]239[.]4[.]189]
li2047-241[.]members[.]linode[.]com	[172[.]105[.]86[.]241]
li2050-63[.]members[.]linode[.]com	[172[.]105[.]89[.]63]
li456-148[.]members[.]linode[.]com	[50[.]116[.]10[.]148]
li365-190[.]members[.]linode[.]com	[96[.]126[.]108[.]190]
li2047-241[.]members[.]linode[.]com	[172[.]105[.]86[.]241]
li2069-116[.]members[.]linode[.]com	[172[.]105[.]153[.]116]
li1318-6[.]members[.]linode[.]com	[45[.]79[.]219[.]6]
li1295-182[.]members[.]linode[.]com	[45[.]79[.]196[.]182]
li483-87[.]members[.]linode[.]com	[50[.]116[.]44[.]87]
li318-132[.]members[.]linode[.]com	[66[.]228[.]61[.]132]
li483-87[.]members[.]linode[.]com	[50[.]116[.]44[.]87]

Subject:

Factura ENTEL
Boleta ENTEL
Perdon por la demora en enviar dinero
Aviso T.G.R

Archivos

Nombre : XML00091580B1782064553_.zip
MD5 : 7bcf7ffc5af072b14389976771cfdeb7

Nombre : CNLIYBAD8083567167.msi
MD5 : 8531a21c0a52dcb9858562e97403ba5d

Nombre : c3meNt0.kok
MD5 : c0580449db7701e6f359ca14fb644c49

Nombre : DUFW9YKCNB81ZFGJAQ0ES7D3WBZOMLZ5
MD5 : 522ae69fc7a18916ce9c2859b1b13f68

Nombre : FVZQ2AXVMF9E0R5KLJHEEQHE2MAHI7W6P
MD5 : af7686225ebaf3cb27db27ae9e372c5e

Nombre : ITJB3ID9TVG6XQJON0YK7OACK19M
MD5 : c56b5f0201a3b3de53e561fe76912bfd

Imagen Phising de Correo 1

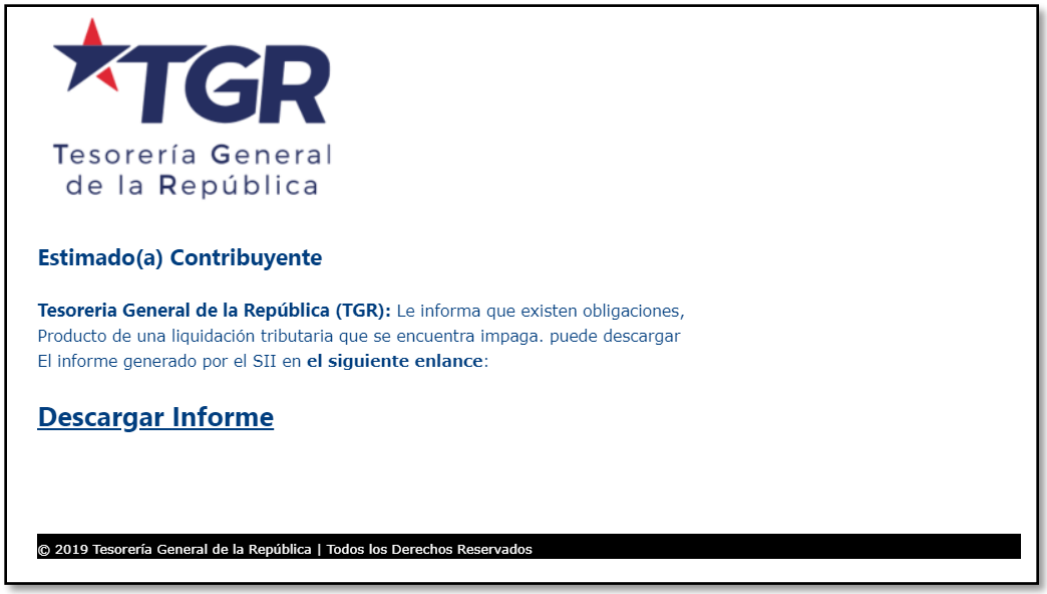


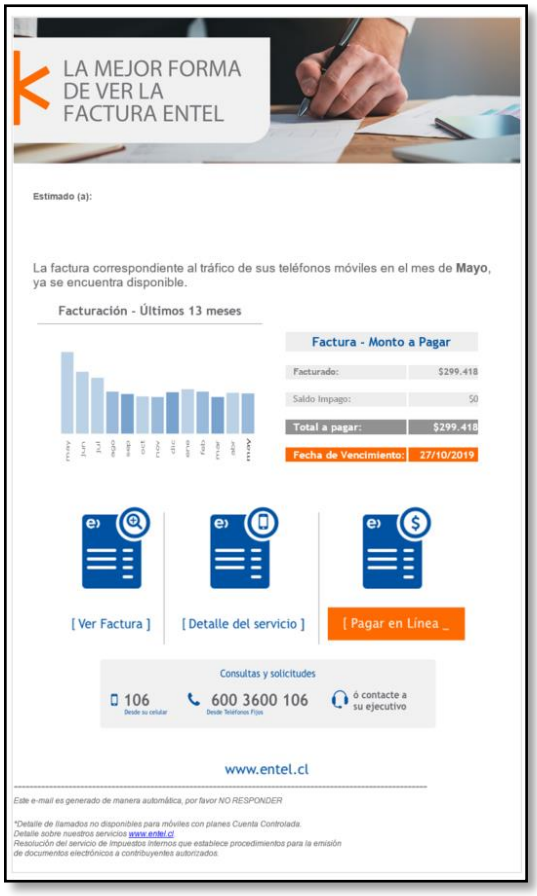
Imagen Phising de Correo 2

AVISO! Comprobante Transferencia,

Estimado (a)

Informamos que se realizó una transferencia electrónica Fondos (TEF) en su cuenta el 29/10/2019 - N: 216565468789

Imagen Phising de Correo 3



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: 2019.10.31 07:57:19 -03'00'