Alerta de seguridad informática	2CMV-00040-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2019
Última revisión	11 de Diciembre 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 identificado una campaña de phishing con malware asociado, a través de un correo electrónico que supuestamente proviene del Servicio de Impuesto Interno.

Los cibercriminales buscan engañar a los usuarios informando que este correo fue generado por un proceso de emisión de factura electrónica detectada el año 2018. A la potencial víctima, se le ofrece la posibilidad de descargar la factura electrónica desde un hipervínculo en el mismo correo. Al descargar el archivo y ser ejecutado, se desencadena la infección del malware.

Indicadores de compromisos

Url's:

http[:]//3[.]84[.]242[.]96/trs/contacto[.]php
http[:]//54[.]198[.]30[.]41
http[:]//3[.]84[.]242[.]96/TRS/OsistemaX[.]php

Smtp Host

[79[.]143[.]187[.]144]
[192[.]119[.]111[.]19]
[192[.]236[.]146[.]134]
[192[.]236[.]147[.]28]

Sender

root@vmi326290[.]contaboserver[.]net
root@hwsrv-652688[.]hostwindsdns[.]com
root@hwsrv-652153[.]hostwindsdns[.]com
root@hwsrv-652169[.]hostwindsdns[.]com

Subject:

El sistema detecto y genero una alerta sobre un debito
El sistema detecto y genero una alerta sobre un debito del 2018

Archivos adjuntos.

Archivo : FacturaElectronica-00365698-2019-10_2.zip
MD5 : da77ab29f2e5304c8c71412ebc55f56c
SHA256 : 88CAE6413D9F51B5BCC151E8826F8B3A7EA9F3FEBF5B37FCF563E01ECF9BA7DD

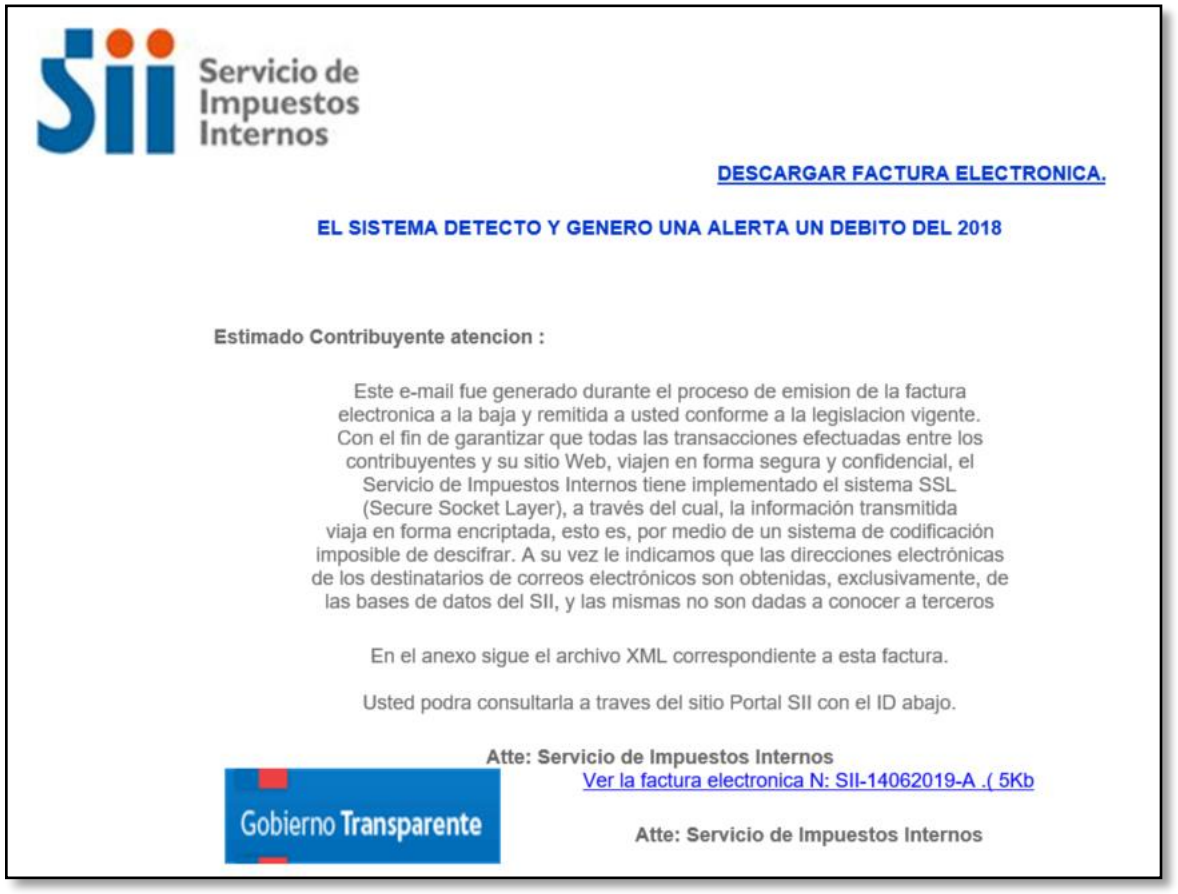
Archivo : FacturaElectronica-00365698-2019-10_2.vbs
MD5 : 5a1f935c30e95b65d8e475b3fb963067
SHA256 : 781db34730e6b87b19b581ad4e538551b2697a31a3e2a6a983d2a8164106f522

Archivo : Politica de privacidad-2
MD5 : 76dfd561e5305c1d3ad2ca63f1eb80f6
SHA256 : f711d08800cb104c79ca3bf9738181c27f9522862ca42a20723c2313d4d6bbed

Otros IOC asociados.

F7C427E0A0F059DB601FB38B028BD8B2
E089DB1AB7F228CE40425ED22AD0B32A
BF07173B7F0244C07DB9AAD7A73D8F4D

Imagen Phising de Correo


Servicio de Impuestos Internos

DESCARGAR FACTURA ELECTRONICA.

EL SISTEMA DETECTO Y GENERO UNA ALERTA UN DEBITO DEL 2018

Estimado Contribuyente atencion :

Este e-mail fue generado durante el proceso de emision de la factura electronica a la baja y remitida a usted conforme a la legislacion vigente. Con el fin de garantizar que todas las transacciones efectuadas entre los contribuyentes y su sitio Web, viajen en forma segura y confidencial, el Servicio de Impuestos Internos tiene implementado el sistema SSL (Secure Socket Layer), a través del cual, la información transmitida viaja en forma encriptada, esto es, por medio de un sistema de codificación imposible de descifrar. A su vez le indicamos que las direcciones electrónicas de los destinatarios de correos electrónicos son obtenidas, exclusivamente, de las bases de datos del SII, y las mismas no son dadas a conocer a terceros

En el anexo sigue el archivo XML correspondiente a esta factura.

Usted podra consultarla a traves del sitio Portal SII con el ID abajo.

Atte: Servicio de Impuestos Internos

Ver la factura electronica N: SII-14062019-A .(5Kb

Gobierno Transparente

Atte: Servicio de Impuestos Internos

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: 2019.12.11 12:47:39 -03'00'