Alerta de seguridad informática	**2CMV-00028-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**02 de Septiembre de 2019**
Última revisión	**02 de Septiembre 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 delincuentes buscan engañar a los usuarios advirtiéndoles sobre la existencia de una factura electrónica por la cual es necesario seleccionar el hipervínculo indicado en el correo. Para dar la impresión de legitimidad del remitente, el correo informa que las transacciones efectuadas entre los contribuyentes y su sitio web viajan de forma segura y confidencial, ya que el sistema de impuestos internos tiene implementado el sistema SSL.

Toda la información que entrega el atacante intenta confundir al usuario para ganar su confianza y así, convencerlo para que descargué los archivos que permiten ejecutar y desencadenar a infección de malware.

Indicadores de compromisos

Url's:

http[:]//3.87.11.10/CH/OsistemaX[.]php
http[:]//3.87.11.10/CH/App[.]php

Smtp Host

hwsrv-581423.[]hostwindsdns[.]com [192.119.111.200]
hwsrv-581422[.]hostwindsdns[.]com [192.119.67.111]
96.9.222.107

Sender

root@hwsrv-581422[.]hostwindsdns[.]com
root@hwsrv-581423[.]hostwindsdns[.]com
root@zeusito[.]com

Subject:

El sistema detectó y generó una alerta sobre un crédito del año 2019

Archivos adjuntos.

Archivo : SII-DocumentoAgostoSIIPERS010-2019_32.zip
MD5 : 6d938e3a19b2ade6cb13cc83821a2aae
SHA256 : 782857099a8fb7cc0b7e97f4304efe25e20a8e75a2b6ec6a296865ea3b6a0e02

Archivo : SII-DocumentoAgostoSIIPERS010-2019_32.vbs
MD5 : ba4da15fbadbb9f87ec52b94df08cfb4
SHA-256 : 58fc653acc4e3f325d0645e0ee12acb1386e1da1354b2f79265b63f2cee29895

Archivo : SII-DocumentoAgostoSIIPERS010-2019_32.pdf
MD5 : 9bea4f71bcfb64d2f7693966826fb21a
SHA-256 : 76d5983b10f21cd8f132fc7d896c3b6716388b2ae4575414f1bfa55b5075971e

Archivo : Articulo de política de privacidad SII-N02C-32
MD5 : c82e59b3c5e249a9a71d9a31d640755f
SHA-256 : cc6eac6b81af3243ddd33ad2780a8666519e01a2f02b794e894ec2ab445e14b4

Imagen de Archivos.

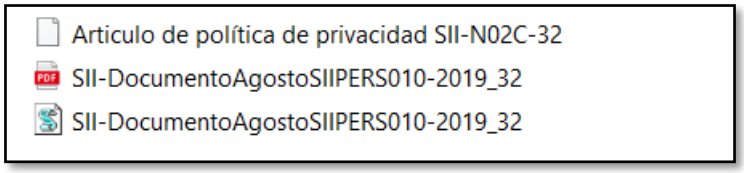
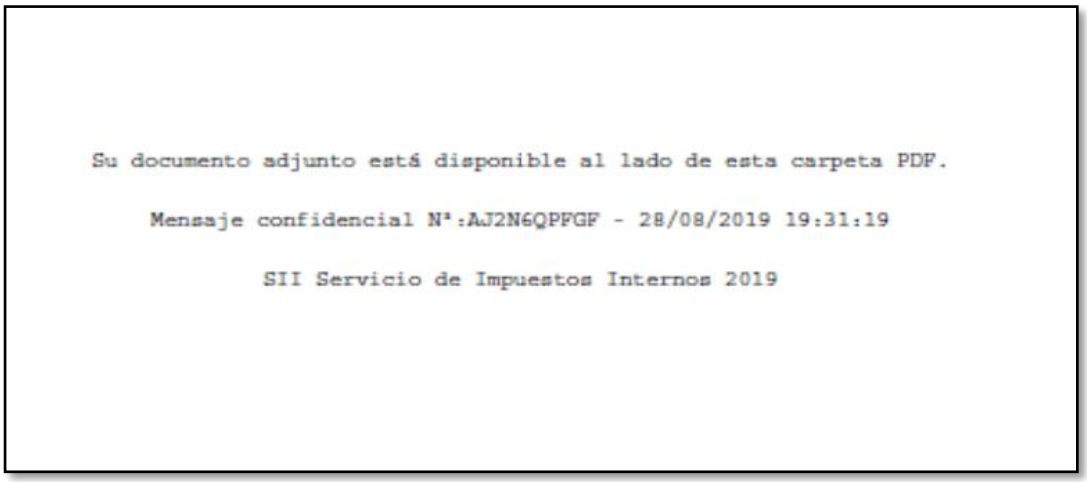


Imagen Phising de Correo

Imagen PDF



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: 2019.09.02 13:10:45 -04'00'