Alerta de Seguridad Informática (8FPH-00031-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 17 de Junio de 2019 | Última revisión 17 de Junio 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 Internos. Los delincuentes buscan engañar a los usuarios insinuando en el título del correo que se trataría de un segundo aviso. El contenido del mensaje advierte a los usuarios que, para evitar una sanción económica que podría ascender a 75 UTM, deben descargar un supuesto documento de restitución de la declaración. Al seleccionar dicho enlace, se desencadena la descarga de archivos maliciosos, que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando además, puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante.

Indicadores de compromisos

Url's:

https[:]//descargadoc[.]com/downloads

http[:]//ajuntament[.]Barcelona[.]cat/casalsgentgransantmarti/modules/syslog/y228/EACpcFCu498FIIIALA8L0BN0a841a0C5F4001K[.]txt

http[:]//ajuntament[.]Barcelona[.]cat/casalsgentgransantmarti/modules/syslog/y228/y228[.]zip

Smtp Host

pau.com [45.12.213.223]

From: (Falso)

msg2w@sii[.]cl

From: (Original)

root@pau[.]com

Subject:

Segundo Aviso (SII)

Archivos adjuntos

Archivo: Doc_view.zip
Size: 161067 bytes
SHA256: B72F5FF282F178A411B7B17550B75E46A7AF9E0A6627A54C803342AC80453FFA

Archivo: y228.zip
Size: 8712747 bytes
SHA256: A975401FC08C1F1147C0175DDF82360CB5996AB7767FDD986D5D1FEF46954FC2

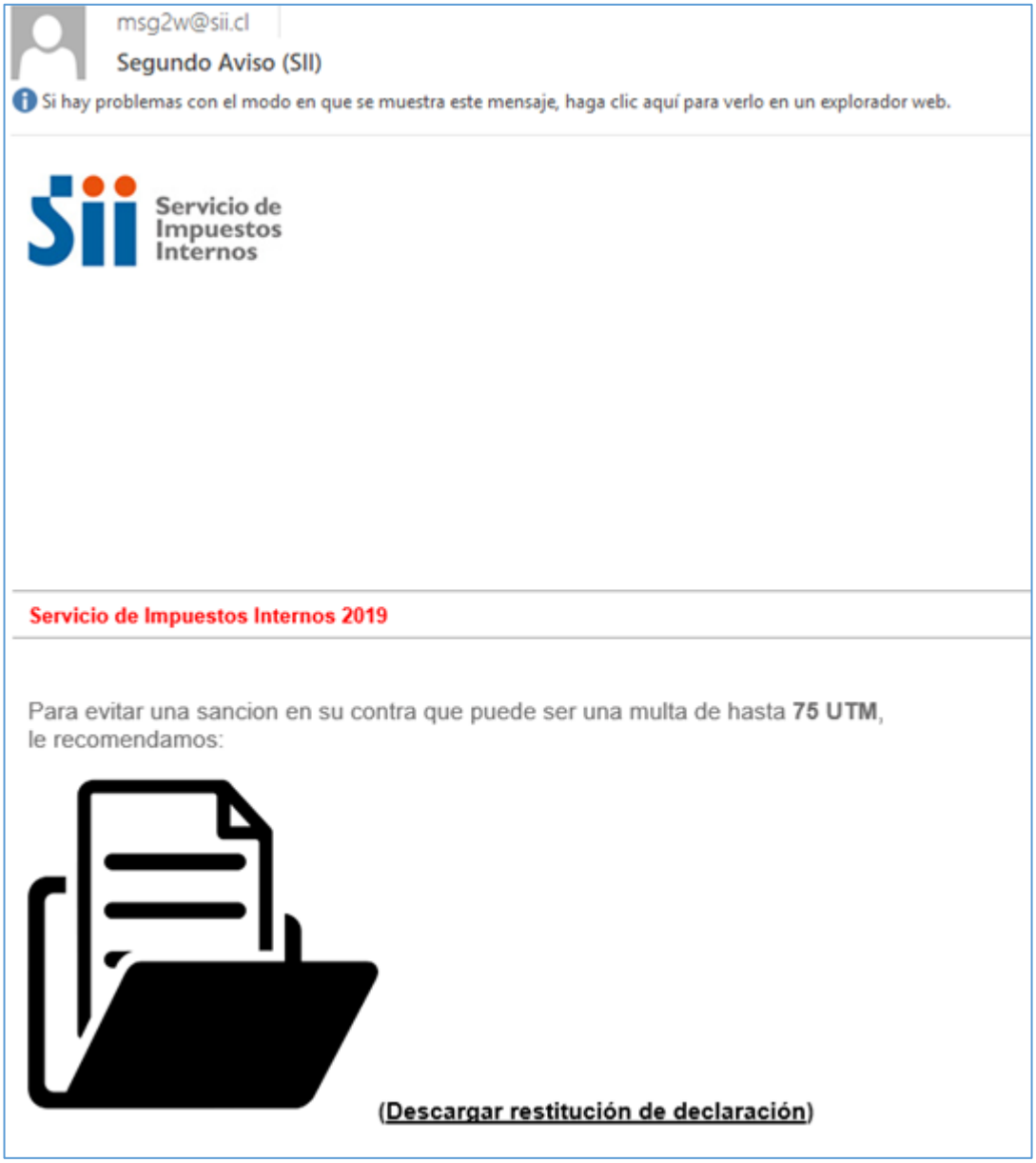
Archivo: Doc_view.msi
Size: 394752 bytes
SHA256: B6089E50238CCFB4CCDA286778396DD2DA125A11C4670B847CCDBF50A492E5DA

Archivo: CFKY5CFXA82GM9ISGG3T1PLR8QATP9G
Size: 800 bytes
SHA256: 5DB207335855900640CC0BA2233900FD282C133A16DBB1E02241EFE418860493

Archivo: FZXXV86CGTIBSTIPJLYKHMVZ48ZU9S
Size: 8501248 bytes
SHA256: 91085940B5FEBDFD9E34910B6DF45BD961B5B30053F7CB0D74F7A346BDF78D2E

Archivo: T4D210QRHE9HIXURZ1DK3LU24RY4KQL9LM
Size: 937776 bytes
SHA256: 8498900E57A490404E7EC4D8159BEE29AED5852AE88BD484141780EAADB727BB

Imagen


msg2w@sii.cl
Segundo Aviso (SII)
Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
Servicio de Impuestos Internos
Servicio de Impuestos Internos 2019
Para evitar una sancion en su contra que puede ser una multa de hasta 75 UTM, le recomendamos:
(Descargar restitución de declaración)

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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob