Alerta de Seguridad Informática (8FPH-00037-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 21 de Junio de 2019 | Última revisión 21 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 aviso y/o 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:

http[:]//descargadoc[.]com/downs/?ACAO=descargar.cgi

http[:]//cembritbold[.]pl/cembritbold/public/cembritbold/Win_doc.zip

http[:]//ajuntament[.]Barcelona[.]cat/casalsgentgransantmarti/modules/syslog/y2230/y230.btc

http[:]//ajuntament[.]Barcelona[.]cat/casalsgentgransantmarti/modules/syslog/y2230/ftZsMenaAHEB90C96I0742NIN86FaaN2D0F22.txt

Smtp Host

m[.]it [45.66.8.186]
gugutico.duckdns[.]org [185.62.189.216]

Sender

root@gugutico.duckdns.org
root@m.it

From (Falso)

msg2@sii.cl
msg3@sii.cl

Subject:

Segundo Aviso (SII)
Aviso (SII)

Archivos adjuntos

Archivo : Win_doc.zip
Tamaño : 4397 bytes
SHA256 : 30DA68F49A9739E18165BAA6D9918CEEF5C1D16F1BC88B25A4BD6A6921128CF8
MD5 : 368cff975ada1ed7e1a03eb1a26fae05

Archivo : Win_doc.cmd
Tamaño : 23942 bytes
SHA256 : B52DBC029F0D4625B57E45B37A6A898B979C6CCB5DD9FE41325ECA9E9FA289F4
MD5 : aa3d9571f4f1ccb9e1b2c60d567e3d34

Archivos : y230.zip
Tamaño : 8681913 bytes
SHA256 : E3D51EF7000174700AB62FB1D63CDF0C3656570E9842F16DED3CFD832050FA37
MD5 : acc90fae7e7910d225c1ff920529049b

Archivos : FLZQKH2B1R9UZCRB646IZQ22P71X6
Tamaño : 8468992 bytes
SHA256 : 30E6F28101AFDD3DC85DA734C505A02320E784FA423DD8B39CF6AF6C72B76036
MD5 : 63a03f303061b150349e64a6906be3fc

Archivo : RWLBENIXJ8N4BMZ9VIK8M1ZETE1OO76US
Tamaño : 937776 bytes
SHA256 : 8498900E57A490404E7EC4D8159BEE29AED5852AE88BD484141780EAADB727BB
MD5 : b06e67f9767e5023892d9698703ad098

Archivo : Z8ENN6VD6Q5CLBLQZGVOOP4HZRNV
Tamaño : 806 bytes
SHA256 : 68F8469355948891DD42059B03DE5EDEC8C5FFB52B797A5426C1290CAA4C554D
MD5 : 6f8dcf7daba1d0af79634174b1c2cb0e

Imagen

msg3@sii.cl
Aviso (SII)

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

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