Alerta de Seguridad Informática (8FPH-00019-001)

Nivel de Riesgo: Alto

Tipo: Phishing-Malware

Fecha de lanzamiento Original: 09 de Mayo de 2019 | Última revisión 09 de Mayo 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-Malware asociado, a través de un correo electrónico que busca engañar a los usuarios advirtiéndoles de una multa de tránsito impaga, la que se apoya en imágenes del supuesto momento en que se produce la infracción. En el correo, se trata de persuadir a las personas para que accedan al detalle de la multa por medio de un link malicioso.

Indicadores de compromisos

Url's: (Payload delivery)

http[:]//intranet.landsoft[.]com.co/sites/default/files/download/

http[:]//mundoclima24[.]cl

http[:]//sc.artgallery.wa.gov[.]au/CMD_RUN.zip

http[:]//rapport.lcto[.]lu/ag97/ag97.zip

Archivos adjuntos

Name: CMD_RUN.zip
Size: 4184 bytes (4 KiB)
SHA256: 9eeb079ea1dbf6c434e82d1c1e9e19fca5b10f8d0915a075d2632565167f9dff

Name: CMD_RUN.cmd
Size: 21888 bytes (21 KiB)
SHA256: b30ee101db2f9b303cd771b72dd57e3e92913477b592bf4766df6b6b7265e2bf

Name: ag97.zip
Size: 8698448 bytes (8494 KiB)
SHA256: f6d36d3b5be598dab96c75a7487e6f8af82fc25d11a45b70421300523d339577

Name: OKJHLSG3JMMDX1FT4CD8IYKCMEV691U
Size: 794 bytes
SHA256: 6adce7636609c36772d3c8e0b247375d1c1ba26a0bb044365e9febf8b7f73615

Name: UR9U75O0I2NYPPT0TQANGKFHACA6A5KL50
Size: 8507904 bytes (8308 KiB)
SHA256: a08e7ffa3c2a15490d89690d1bcd57f79956b37646ceb1127f97e63b139c9221

Name: chfcb.exe (WPTSVZT754Y5XJ0HBWDQTA9LE8VWAKRMTTGWDCO)
Size: 937776 bytes (915 KiB)
SHA256: 8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727bb

Smtp Host

sm05.inetweb.com.br
maya.onda.com.br
gw08.site4future.com
antispam-scan01.netsite.com.br
ns1.clealco.com.br
ipn.servidor-celeste.com
[177.137.208.10]
blue.dogwood.relay.mailchannels.net

From:

emergencia@hospitaldasbonecas.com.br
dommilton@onda.com.br
contato@blcaminhoes.com
migliori@netsite.com.br
comunicacao@clealco.com.br
ibimec@ibimec.com.br
publiqueweb@brsuper.com.br
reservas@machadosplazahotel.com.br
saporiti@onda.com.br

Subject:
Numero de Controle 5648093872 Data: 08/05/2019
Multa No Pago

Imagen

publiqueweb@brsuper.com.br | 0

Multa No Pago Número de Controle 1896501364 Data: 09/05/2019

Registro Civil e Identificación
Presente en toda tu vida
Ministerio de Justicia

Estimado(a)Conductor

Detectamos en nuestro sistema un registro de multa de transito no pagada. Debido a que usted no se notifico en el tribunal de faltas correspondiente le Reenviamos las Foto-multas via internet.

Para mayor informacion sobre la multa de transito, descarque el detalle en lo siguiente link:

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre 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
https://www. linkedin.com/company/csirt-gob
@CSIRTGOB