Alerta de Seguridad Informática (8FPH-00035-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 20 de Junio de 2019 | Última revisión 20 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 a través de un correo electrónico que supuestamente proviene de la empresa de straming Netflix. Buscando engañar que debe actualizar el detalle de pago dentro de las próximas 24 horas para evitar interrupción de sus servicios. Persuadiendo a seleccionar el link que aparece en el correo, direccionando un sitio falso.

Indicadores de compromisos

Url's:

http[:]//news.svnhforum[.]com/wp-content/plugins/legend/loading/
http[:]//brockvacations[.]com/wp-ontent/plugins/zetpeck/NetflixEs/netflix/996ba314fdf70b903c9a34364/

Smtp Host

msr14.hinet.net [168.95.4.114]) [23.152.0.42]
msr9.hinet.net [168.95.4.109]
cmta18.telus.net [209.171.16.91]
cmta19.telus.net [209.171.16.92]
cmta16.telus.net [209.171.16.89]

From: (Original)

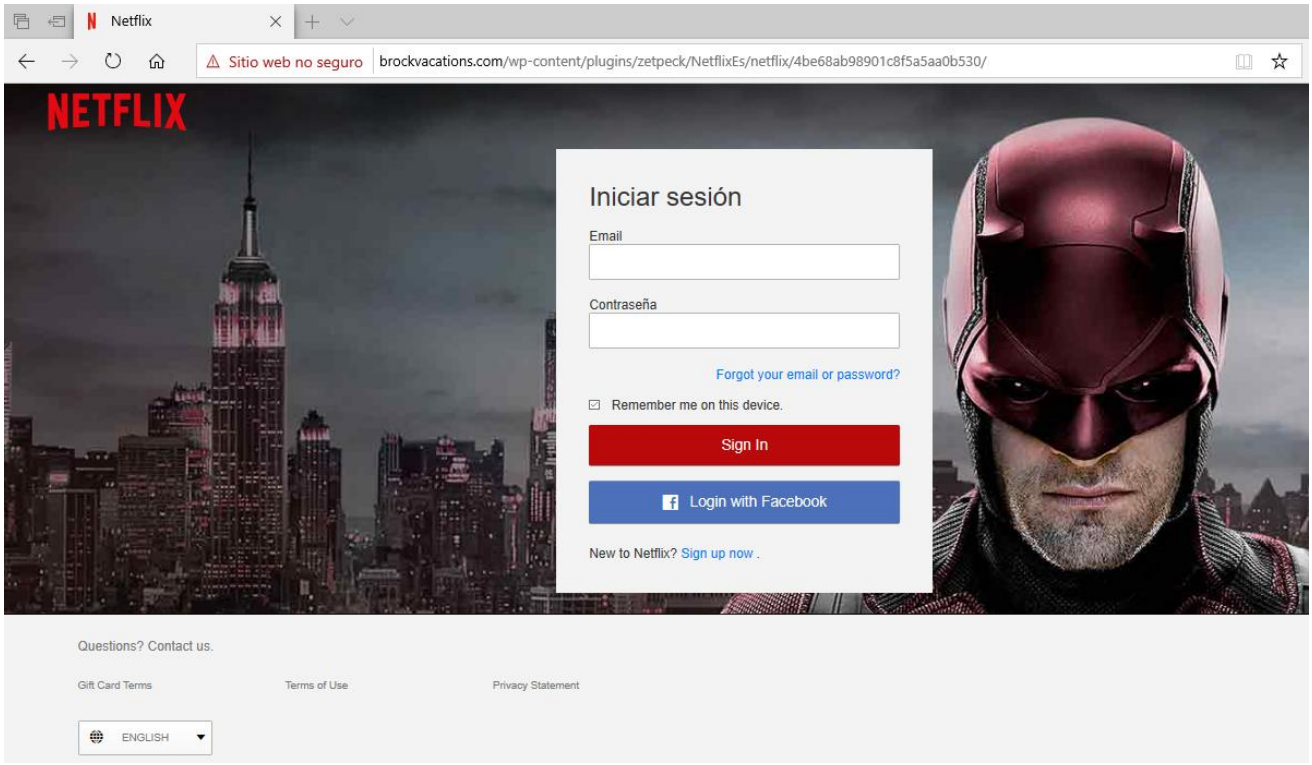
testi@telus[.]net
testi@telus[.]net

Subject:

Confirma tu método de pago

Imagen


Netflix Inc <testis@hinet.net>
onex_1182@hotmail.com
Confirma tu método de pago
Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
NETFLIX
Estimado cliente,
Desafortunadamente te informamos que Su cuenta de Netflix será desactivada .
Por favor, actualice sus detalles de pago dentro de las próximas 24 horas para evitar interrupcion de sus servicios .
Para actualizar sus informaciones.
Si tienes alguna duda, estamos a tu disposición. feliz de ayudar.
Simplemente llámenos en cualquier momento al 0800 096 6380.
The Netflix Team


Netflix
Sitio web no seguro
brockvacations.com/wp-content/plugins/zetpeck/NetflixEs/netflix/4be68ab98901c8f5a5aa0b530/
NETFLIX
Iniciar sesión
Email
Contraseña
Forgot your email or password?
Remember me on this device.
Sign In
Login with Facebook
New to Netflix? Sign up now .
Questions? Contact us.
Gift Card Terms
Terms of Use
Privacy Statement
ENGLISH

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