Alerta de Seguridad Informática (8FPH-00032-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 19 de Junio de 2019 | Última revisión 19 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 de la empresa de streaming Netflix. Los delincuentes buscan engañar a los usuarios insinuando que su cuenta presenta información incorrecta debiendo actualizarla antes de 48h horas, si no se procederá a su suspensión. Persuadiendo seleccionar el link que aparecer en el correo, direccionando un sitio falso.

Indicadores de compromisos

Url's:

https[:]//www.bighornconsult[.]com/net/03078bbd447eb9d281a2943f6be53025/

Smtp Host

thunder.jaws.hu [91.120.21.162]

From: (Original)

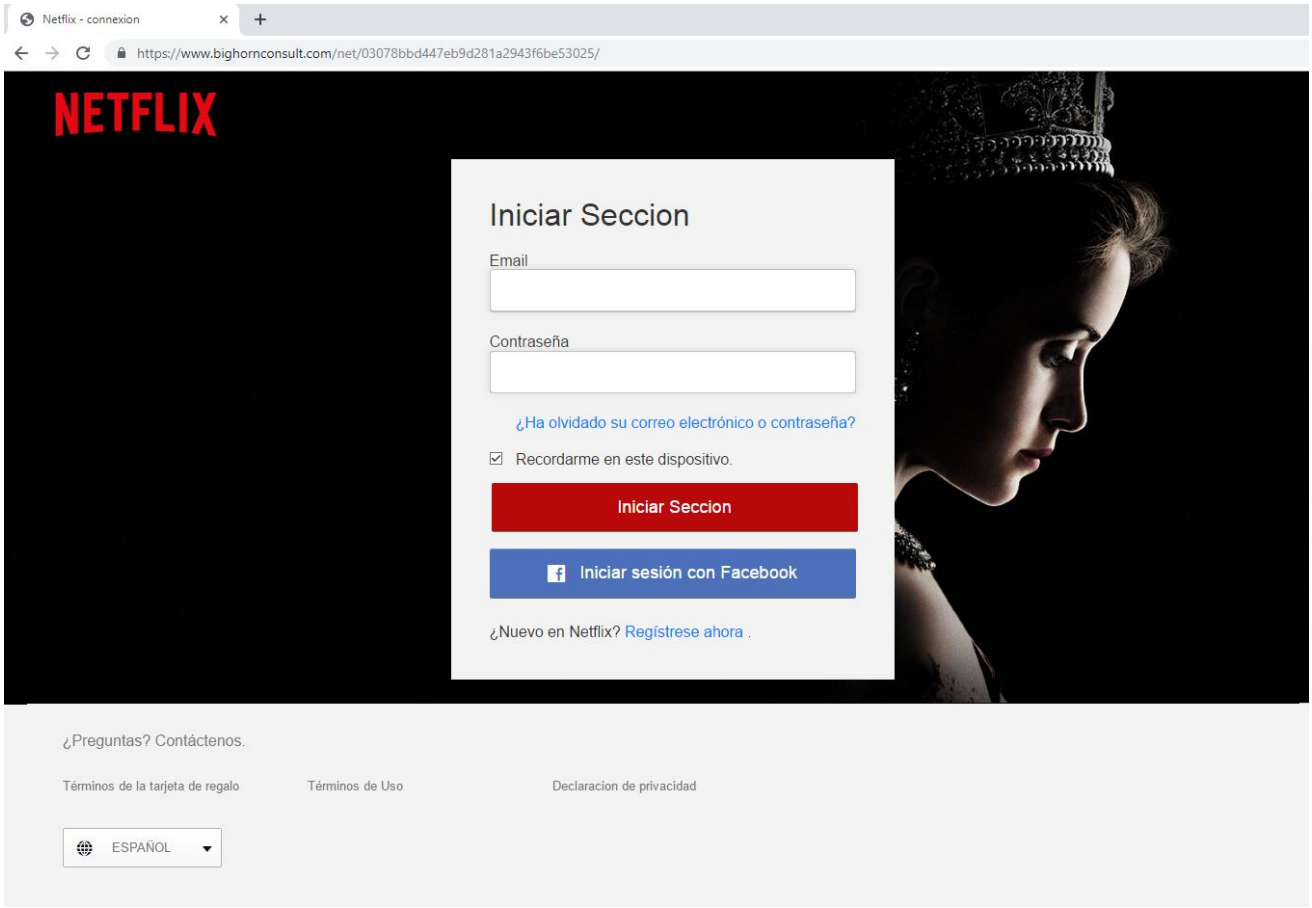
noreply@nfx[.]com

Subject:

notificación de cuenta

Imagen


NETFLIX <noreply@nfx.com>
notificación de cuenta
NETFIX
Estimado cliente,
Alguna información de su cuenta parece estar incorrecta o falta,
actualice su información en un plazo de 48 horas.
Si esto no se hace, nos veremos obligados a suspender su cuenta
actualiza tu información aquí
-El equipo de Netflix


Netflix - connexion
https://www.bighornconsult.com/net/03078bbd447eb9d281a2943f6be53025/
NETFLIX
Iniciar Seccion
Email
Contraseña
¿Ha olvidado su correo electrónico o contraseña?
Recordarme en este dispositivo.
Iniciar Seccion
Iniciar sesión con Facebook
¿Nuevo en Netflix? Regístrese ahora .
¿Preguntas? Contáctenos.
Términos de la tarjeta de regalo
Términos de Uso
Declaracion de privacidad
ESPAÑOL

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