Alerta de Seguridad Informática (8FPH-00046-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio 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.

El correo trata de persuadir que debe actualizar sus datos para continuar con el servicio, ya que su cuenta se encuentra cancelada por existir un problema con el pago.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

- https://login[.]netfiix[.]com[.]oeihe[.]com/NT_ACCOUNT_ACCESS/login/index[.]php
- http://soqol-ostirish[.]uz/DH827W23/

Smtp Host

- 91.83.93.101
- 103.12.84.195
- 210.1.224.91
- 36.255.220.26
- 46.242.146.6
- 148.251.232.146
- 85.128.147.38
- 177.70.124.60
- 192.185.46.113
- 94.126.20.178
- 195.238.232.90
- 93.104.212.249
- 198.23.53.43

From:

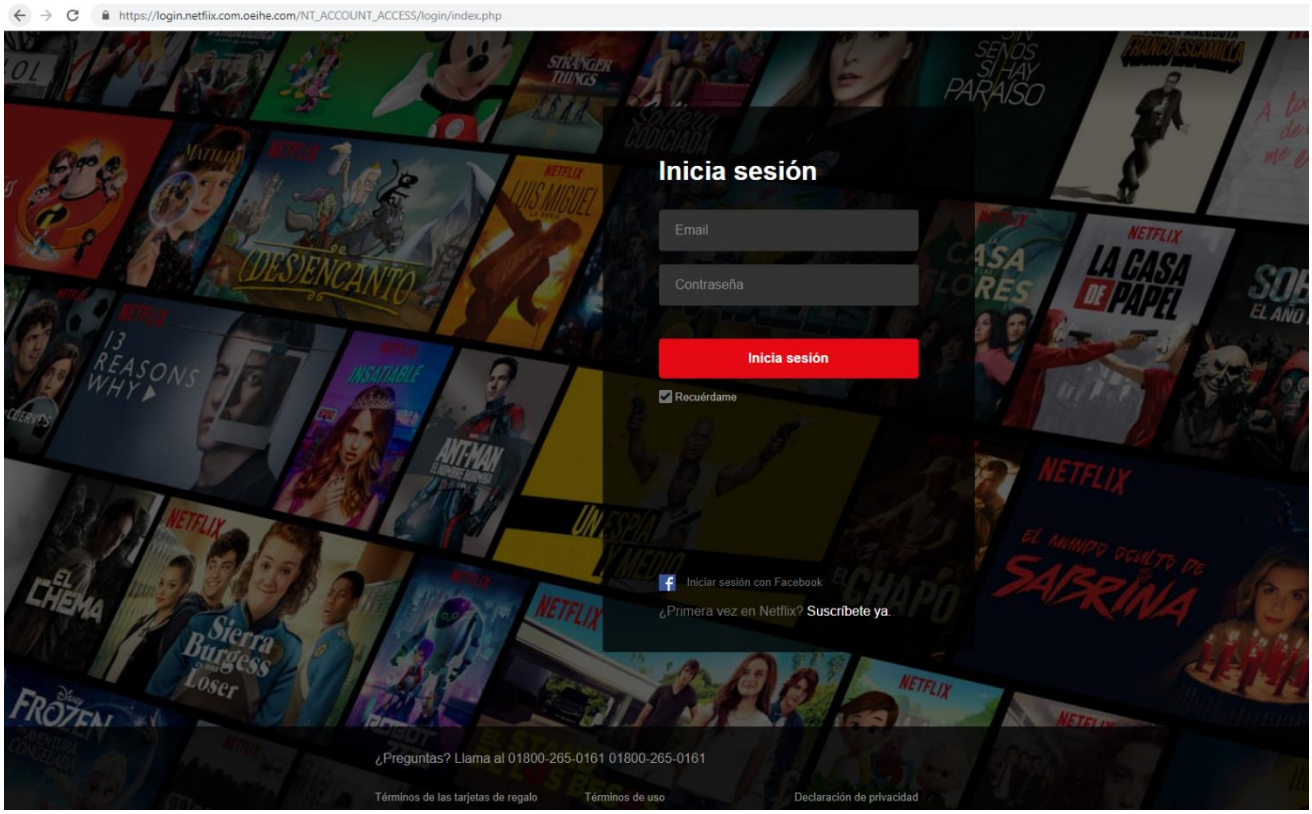
- info@hulladekkor.hu
- admin@kotaku.pu.go.id
- info@hawaiian7478bbq.com
- admin@dinenergy.com
- admin@foge.pl
- sales@gmkpistachio.com
- admin@rynkowa30.pl
- aliandra@cotrisel.com.br
- contact@icanfly.co
- info@tribusurbaines.com
- mail@uncon.org
- info@caspianconcept.com
- info@securethatjob.com

Subject:

- Su cuenta puede ser bloqueada hoy¡

Imagen Phishing correo

Imagen Sitio Web



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
- Visualizar los sitios web que se ingresen que sean los oficiales

Contactos

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

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.07.17
19:31:49 -04'00'