Alerta de seguridad informática	8FPH20-00143-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Marzo de 2020
Última revisión	25 de Marzo de 2020

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.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing que se está difundiendo a través de un correo electrónico falso que aparentemente proviene del servicio de streaming Netflix.

El mensaje informa que la cuenta del usuario ha caducado y se suspenderá en 24 horas, por lo que solicita actualizar la información para corregir el problema. El atacante dispone un enlace en el mensaje para ser derivado a un sitio falso que imita a la web oficial del servicio de streaming, en la cual le solicitan ingresar sus credenciales para iniciar una sesión. Luego de eso le solicita al usuario actualizar los datos de la tarjeta de crédito. En estos pasos se expone al robo de sus credenciales.

OBSERVACIÓN

Solicitamos tener en consideración las señales de compromiso en su conjunto.

INDICADORES DE COMPROMISO

Urls Redirecciones:
https[:]//www[.]baznasbanten[.]org/vendor/hamcrest/hamcrest-php/hamcrest/netflixredcrion[.]html

Urls sitio falso:
https[:]//mokhtasr[.]net/vendor/guzzlehttp/promises/FOVZ/406b03778b453fc465a3667eb36e729a
https[:]//mokhtasr[.]net/vendor/guzzlehttp/promises/FOVZ/406b03778b453fc465a3667eb36e729a/card.php

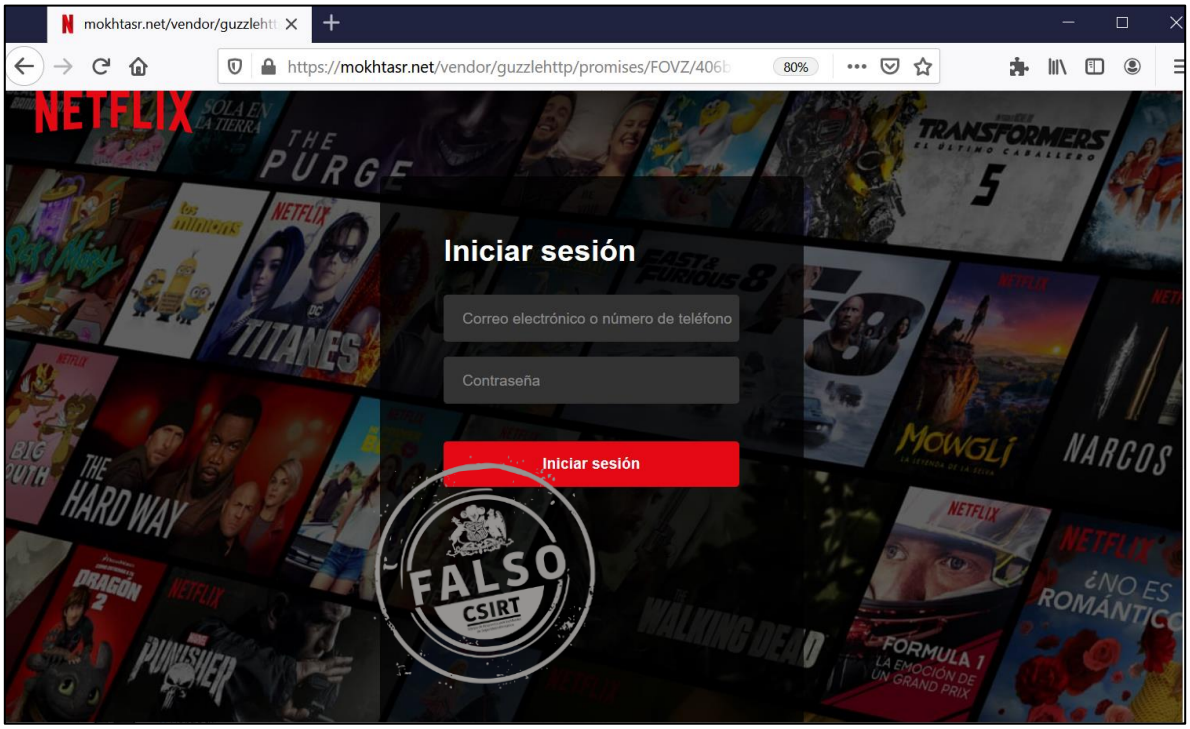
Smtp Host
50[.]7[.]176[.]244
50[.]7[.]176[.]94

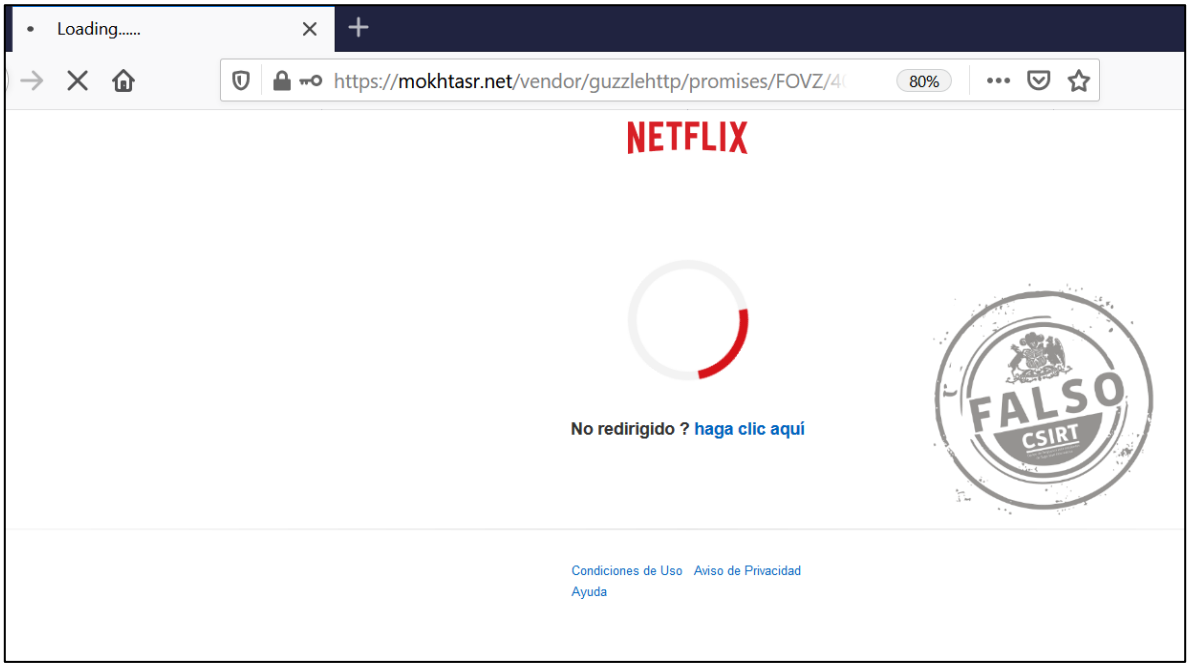
Sender
azure_c9159507871cce52e0b88b355c934311[@]azure[.]com

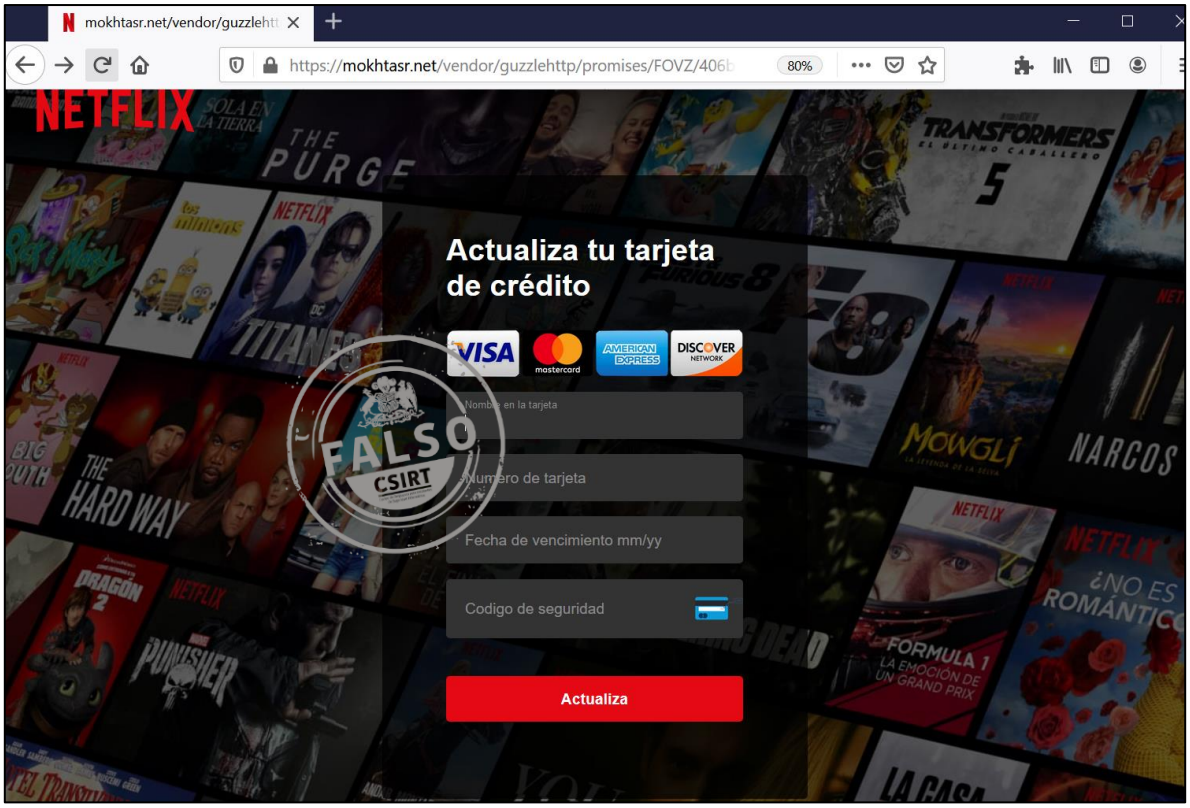
Asunto
Confirma tu forma de pago

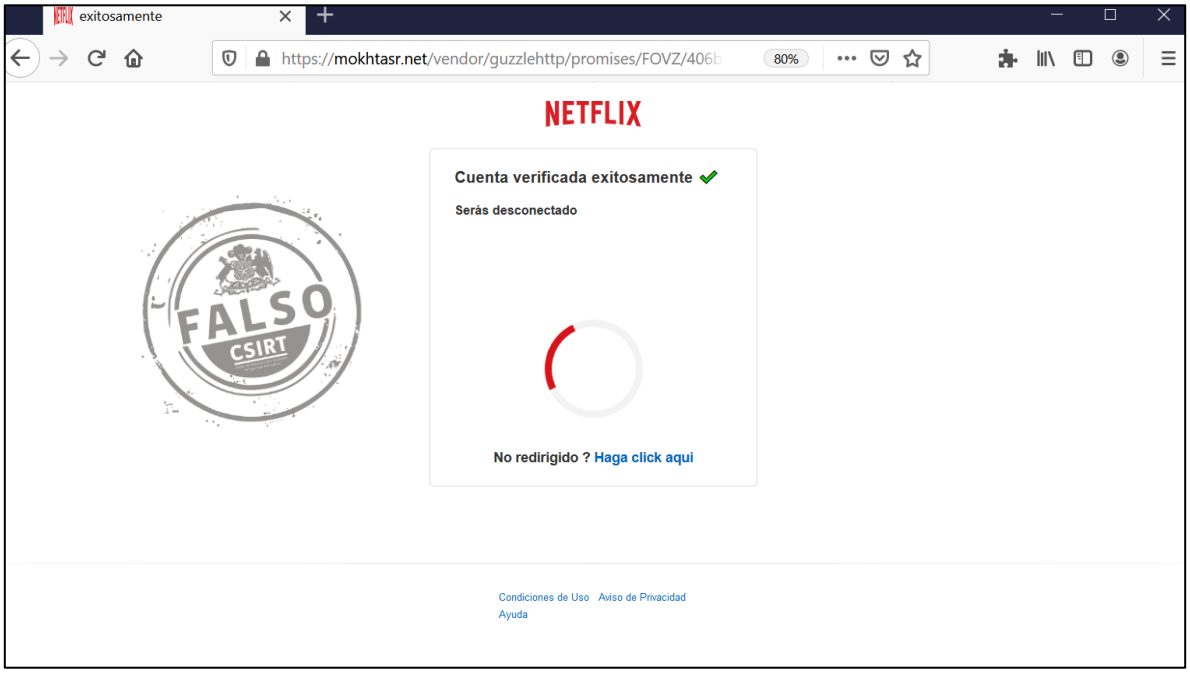
IMAGEN DEL MENSAJE

IMAGEN DEL SITIO






mokhtasr.net/vendor/guzzlehtt
https://mokhtasr.net/vendor/guzzlehttp/promises/FOVZ/406b
80%
NETFLIX
Actualiza tu tarjeta de crédito
VISA
mastercard
AMERICAN EXPRESS
DISCOVER NETWORK
Nombre en la tarjeta
Número de tarjeta
Fecha de vencimiento mm/yy
Codigo de seguridad
Actualiza
FALSO
CSIRT


exitosamente
https://mokhtasr.net/vendor/guzzlehttp/promises/FOVZ/406b
80%
NETFLIX
Cuenta verificada exitosamente
Serás desconectado
No redirigido ? Haga click aqui
FALSO
CSIRT
Condiciones de Uso
Aviso de Privacidad
Ayuda

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 sean los oficiales.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.25 20:21:51 -03'00'