Alerta de seguridad informática	8FPH20-00104-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Enero de 2020
Última revisión	31 de Enero 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 a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios de la empresa de Streaming Netflix.

El correo indica que existe un problema con el monto de pago y solicita, a quien lo recibe, que normalice la situación lo antes posible para evitar problemas e interrupciones en el servicio. El atacante disponibiliza un enlace, que al ser seleccionado, redirige al usuario a un sitio semejante al de Netflix. En el sitio se solicita del usuario su nombre, número de tarjeta de crédito, fecha de caducidad y código de seguridad.

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

Indicadores de compromisos
Url's:
http[:]//a0396139[.]xsph[.]ru/ri/

Smtp Host
[219.94.128.17]
[219.118.72.112]
[110.50.207.32]
[110.45.144.166]

Sender
sato@loungedesigns.co[.]jp
ryo-t@cityfujisawa.ne[.]jp
love@adelaidesarang[.]com

Subject:
NETFLIX- Acerca de su cuenta

Imagen Phishing Correo

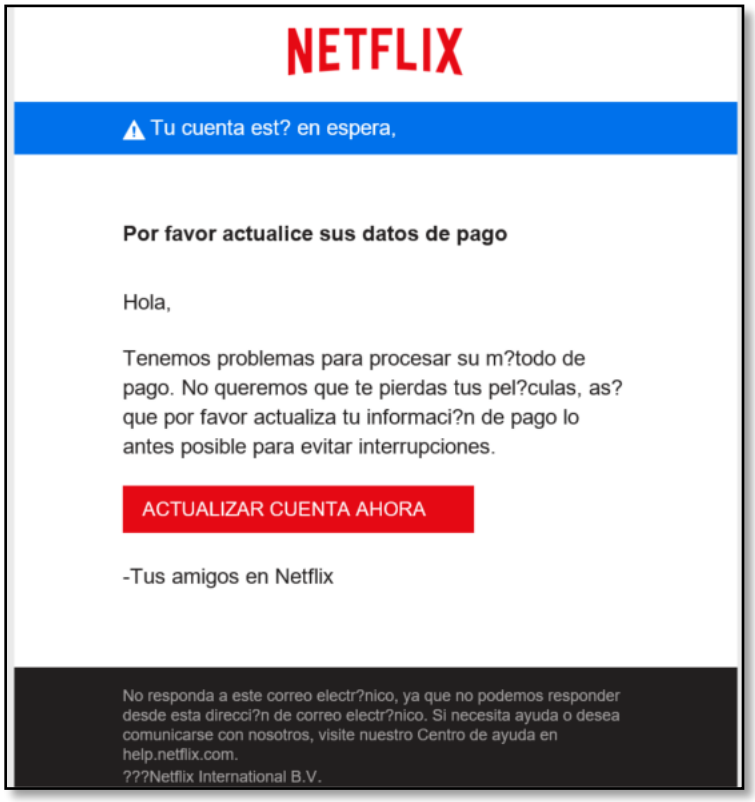
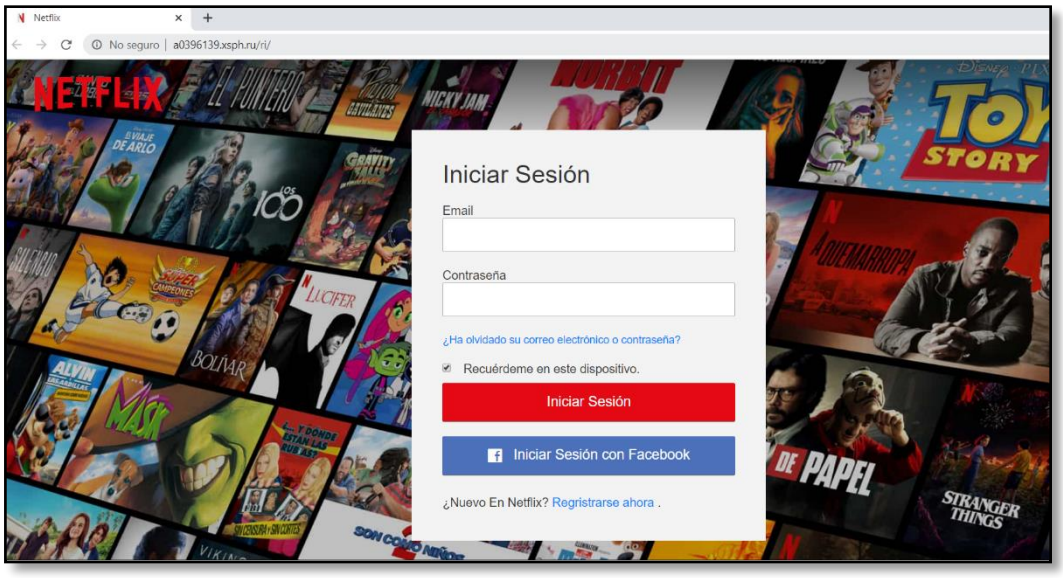
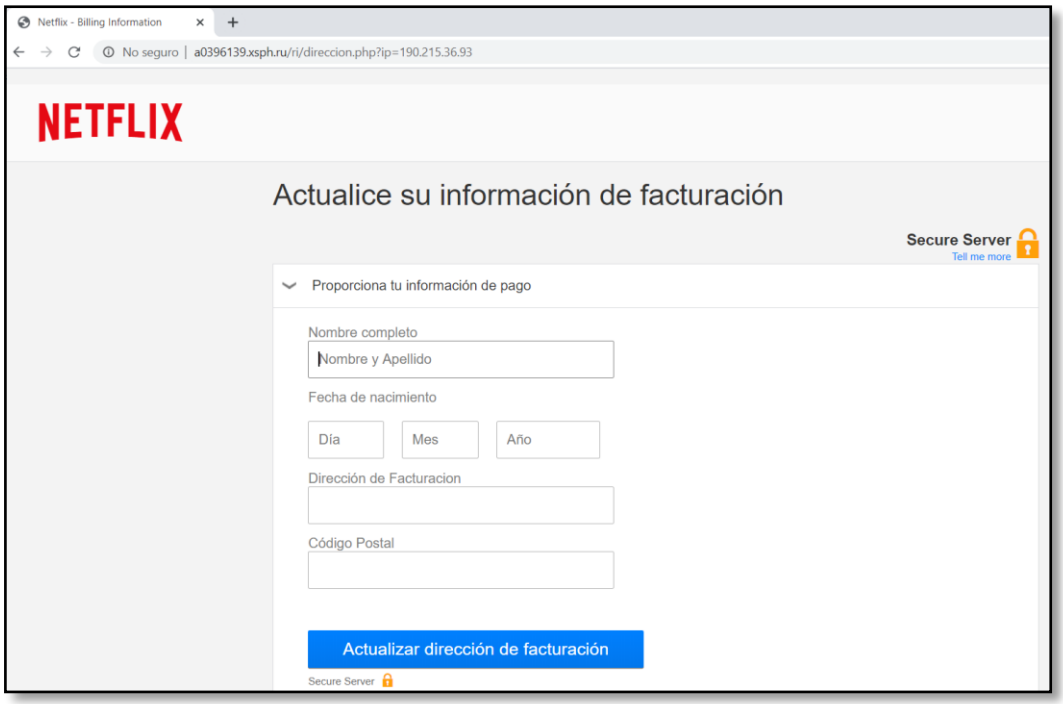
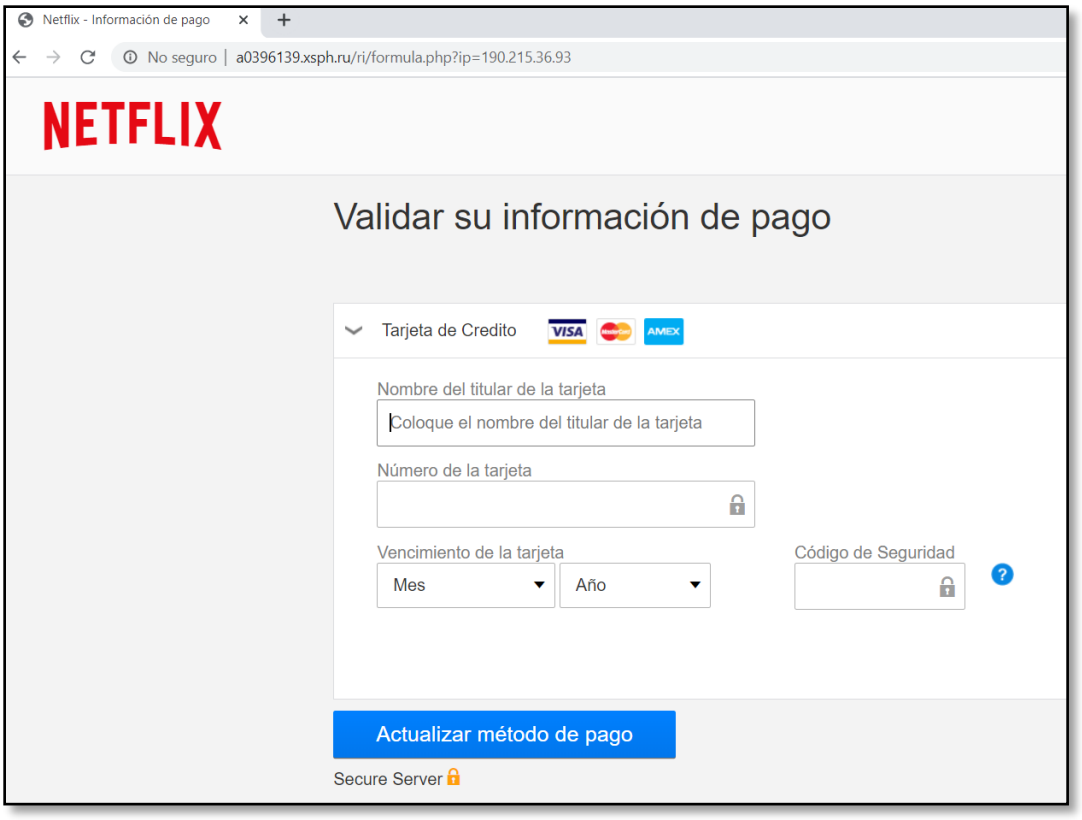


Imagen Sitio Web







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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.31 19:33:34 -03'00'