

Alerta de seguridad informática	8FPH20-00144-01
Clase de alerta	Fraude
Tipo de incidente	Smishing
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 Smishing, que se está difundiendo a través de mensaje de texto falso que aparente proviene de Netflix. El mensaje informa que la suscripción de Netflix se ha suspendido, 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 solicita ingresar sus credenciales para iniciar sesión, luego de eso le solicita al usuario actualizar los datos de la tarjeta de crédito.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Urls sitio falso:

[https://pagosnetflix\[.\]com/cl/pago/](https://pagosnetflix[.]com/cl/pago/)

Asunto

Confirma tu forma de pago

IMAGEN DEL MENSAJE



IMAGEN DEL SITIO



← → ↻ ⚠ Peligrosa | pagosnetflix.com/cl/

NETFLIX

Confirme su identidad para continuar.

¡Solo 2 pasos y listo! Odiamos el papeleo, también.
PASO 1 DE 2
Ingrese su email y contraseña.

Email

Contraseña

CONTINUAR



¡Solo un último pasos más y listo!

PASO 2 DE 2
Ingrese su tarjeta de crédito o débito.

VISA  

Nombre

Apellido

Numero de Tarjeta

Fecha de Vencimiento (MM/AA)

Codigo de Seguridad (CVV)

CONTINUAR

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.