PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 02 de mayo de 2022

N° 120-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 120	Fecha: 02-05-2022
		Página 3 de 5

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing que suplantan la identidad de NETFLIX.		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la plataforma de entretenimiento "NETFLIX", el supuesto sitio web cuenta con colores y logos característicos idénticos al sitio web oficial, el cual tiene como finalidad robar información confidencial de las posibles víctimas, como dirección de correo electrónico, contraseña, datos bancarios (nombre y número de la tarjeta de crédito o débito, fecha de expiración de la tarjeta, etc.).

2. ***Imagen: detalles del proceso de Phishing***.

Paso Nº 01

Sitio web fraudulento de Netflix, donde solicita a la víctima, actualizar dirección de facturación y método de pago.

Paso Nº 02

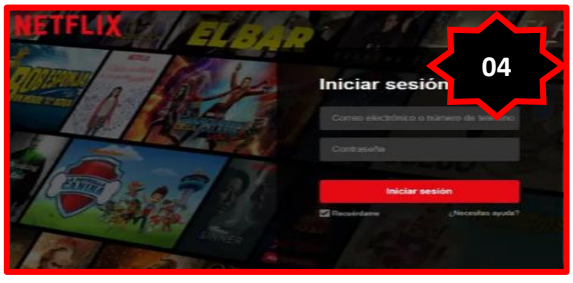
Una vez hecho clic en <Asegure su cuenta>, aparece una pantalla solicitando que requiere actualizar los datos personales de la víctima:

- Nombre y Apellido del titular de la tarjeta bancaria
- Dirección
- Ciudad
- Número de teléfono móvil.
- Fecha de nacimiento

Paso Nº 03

Luego de <Actualizar la dirección de facturación> aparece otra ventana que requiere confirmar el método de pago:

- Nombre y Apellido del titular de la tarjeta bancaria
- Número de tarjeta
- Fecha de caducidad
- Código de seguridad



Paso Nº 04

Por último, es redirigido al sitio web oficial de Netflix.

3. ***Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.***

Veredicto de Comodo Valkyrie	Suplantación de identidad	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	kaspersky	Suplantación de identidad
netcraft	Malicioso	tanque de phishing	Suplantación de identidad
Segasec	Suplantación de identidad	Sophos	Suplantación de identidad

4. ***Indicadores de compromiso (IoC)***

- ✓ URL : hxxps://www[.]pintana[.]cl/au/netflix/update/
- ✓ Dominio : pintana.cl
- ✓ SHA-256 : 042b9877bd63faaa3ddfc69cd7213a40a416f67c09bba052441d858ea60079f3
- ✓ IP : 200[.]27[.]210[.]230

5. ***Otras detecciones:***

6. ***Apreciación de la información*:**

- La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso e información bancaria (tarjetas de crédito o débito) de los usuarios de la plataforma de entretenimiento NETFLIX.
- La propagación del sitio web fraudulento se realiza mediante envió masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger y mensajes de textos (SMS).

7. ***Algunas recomendaciones:***

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético