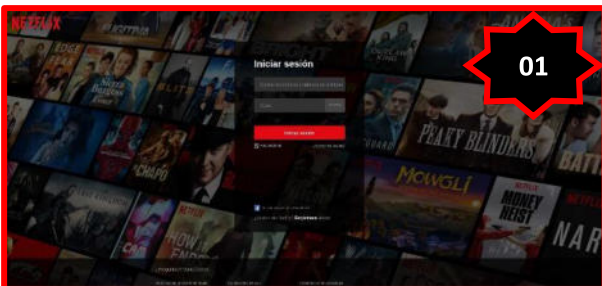
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 085	Fecha: 26-03-2022
		Página 4 de 6
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ	
Nombre de la alerta	Campaña de Phishing que suplantan la identidad de NETFLIX.	
Tipo de Ataque	Phishing	Abreviatura Phishing
Medios de propagación	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.



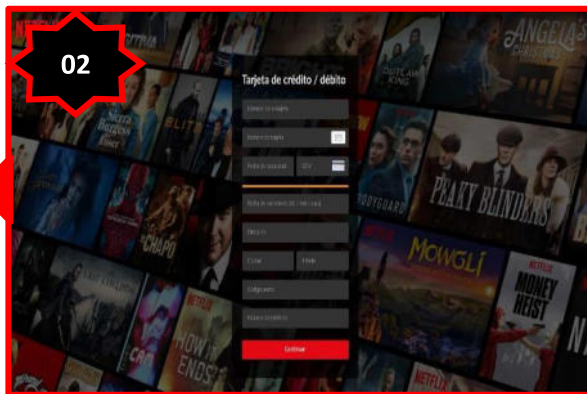
Paso N° 01

Requiere las credenciales de acceso (correo electrónico y contraseña) de la plataforma de entretenimiento Netflix, para luego dar clic en <Iniciar sesión>.

Paso N° 02

Una vez ingresado las credenciales de acceso y dar clic en <Iniciar sesión>, aparece una pantalla solicitando a la víctima datos bancarios como:

- Nombre del titular de la tarjeta bancaria
- Número de la tarjeta de crédito o débito
- Fecha de vencimiento de la tarjeta bancaria.
- Código de seguridad (CVC).
- Dirección y código postal.
- Número de teléfono móvil.

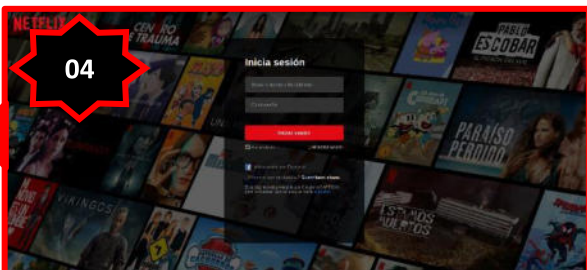


Paso N° 03

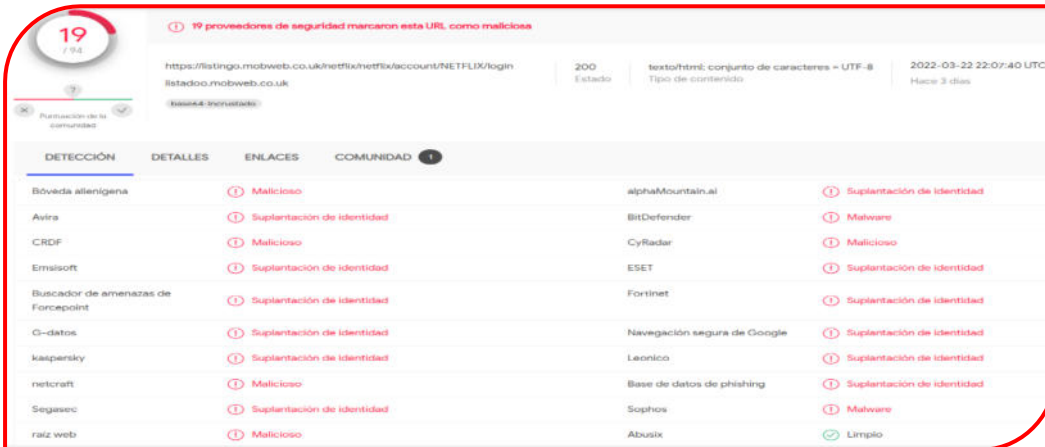
Luego de dar clic en <Continuar> en el paso N° 02, se muestra a una ventana con la descripción que registre el código enviado al número del teléfono móvil, vinculado a la tarjeta bancaria; para después dar clic en <verificar>.

Paso N° 04

Después de registrar el código de verificación, enviado vía mensaje texto al teléfono registrado en el paso N° 02, al dar clic en <verificar>, es redirigido al sitio web oficial de la plataforma de entretenimiento NETFLIX; sin embargo, los ciberdelincuentes obtuvieron los datos brindado por la víctima.



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



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

- ✓ URL : hxxps://listingo[.]mobweb[.]co[.]uk/netflix/netflix/account/NETFLIX/login
- ✓ Dominio : listadoo[.]mobweb[.]co[.]uk
- ✓ SHA-256 : eb72fe2b7fa9bbdaea1e647b2723c151d4b9f4db5543fa5abb4e6b19d1be2703
- ✓ IP : 23[.]231[.]24[.]26

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 envíos 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.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta
------------------------	----------------------------------------------------