	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 081	Fecha: 22-03-2022
		Página 8 de 10

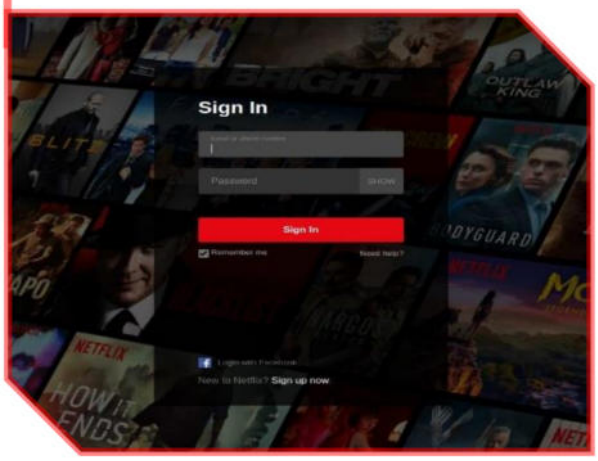
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ			
Nombre de Alerta	Nueva campaña de phishing dirigidos a usuarios de Netflix.			
Tipo de Ataque	Phishing		Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros			
Código de familia	G	Código de subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

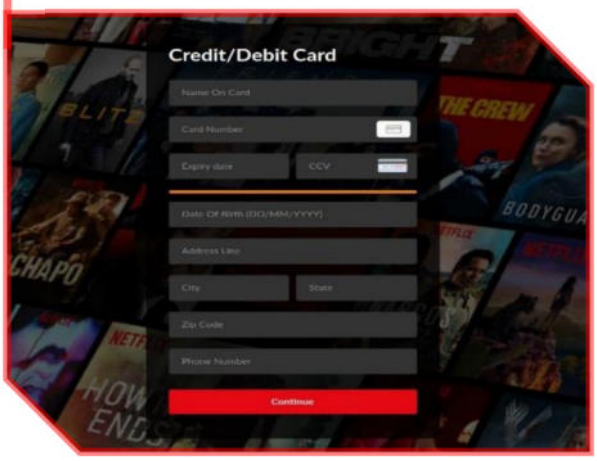
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de phishing, por medio de la creación de un sitio web falso similar a la oficial de Netflix, lo que hace convincente al usuario ingresar al sitio web falso, con el objetivo robar credenciales de acceso, datos personales y bancarios.

2. Proceso del ataque phishing:

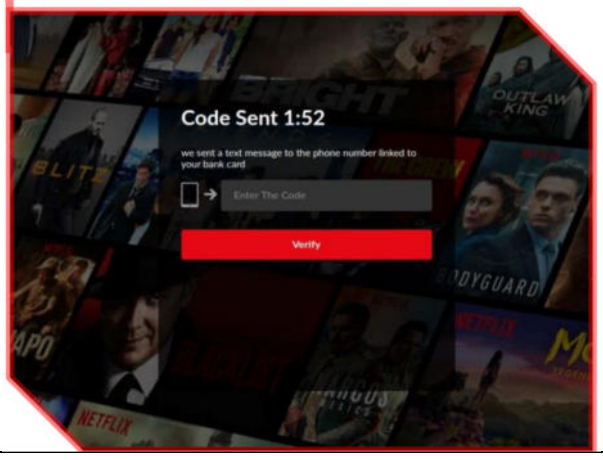
Etapa 01: Sitio web falso que simula ser Netflix, solicita a la víctima, ingresar sus credenciales de acceso (correo electrónico y contraseñas), para luego <Iniciar sesión>.



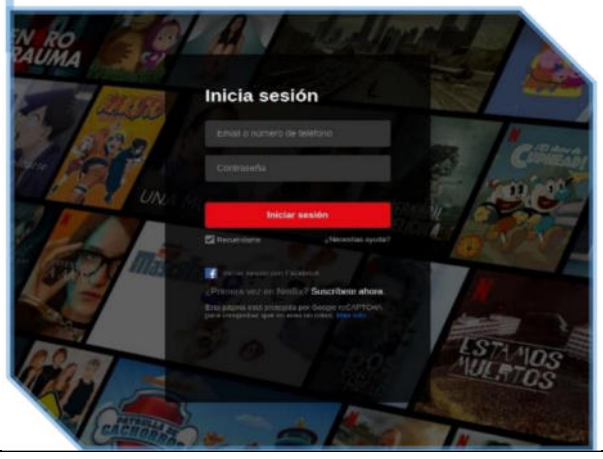
Etapa 02: Una vez ingresado las credenciales de acceso y hecho clic en <Iniciar sesión>, aparece en la pantalla un formulario solicitando datos de la tarjeta de crédito o débito, y número de teléfono para después <continuar>.



Etapa 03: Luego, de haber hecho clic, en <Continuar>, el sitio web falso aparenta enviar un código vía mensaje de texto al número de teléfono proporcionado, el cual deberá ingresar y verificar.



Etapa 04: Pasado unos 20 segundos (luego de haber esperado el código presuntamente enviado por el sitio web fraudulento), es redirigido al sitio web oficial Netflix, aludiendo un aparente error de autenticación; sin embargo, los datos fueros capturados por los ciberdelincuentes.

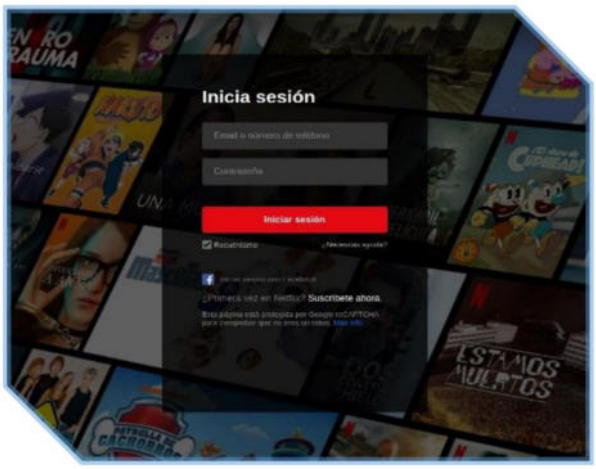


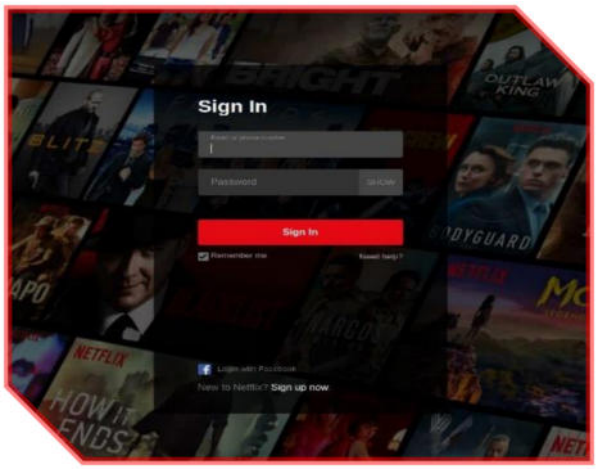
3. Comparación del inicio de sesión del sitio web oficial y el sitio web falso:

Sitio web Oficial
URL: https://www.netflix.com/pe/login

Sitio web falso
URL: hXXps://listingo[.]mobweb[.]co[.]uk

Comparación de Dominios





- Existen similitudes entre el fondo y forma de cada sitio web.
- Ambas URL´s utilizan el protocolo HTTPS, lo que hace convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, debido el dominio del sitio web fraudulento no corresponde con el oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado lo siguiente:

- Indicadores de compromiso:

  - URL: hXXps[:]//listingo[.]mobweb[.]co[.]uk/netflix/netflix/account/NETFLIX/login
  - Dominio: listadoo[.]mobweb[.]co[.]uk
  - Dirección IP: 23[.]231[.]24[.]26
  - Código: 200
  - Longitud: 340.81 KB
  - SHA-256: d09f70319c032eded27c141b54bdd67e93cf3568067ae39f2eb6d53cbbbe772d

5. Recomendaciones:

- Evitar abrir correos de usuarios desconocidos o que no hayas solicitado, elimínalos directamente.
- No brindar información personal a sitios web de dudosa procedencia.
- Escribir directamente la URL de la entidad en el navegador, en lugar de llegar a ella a través de enlaces disponibles desde páginas de terceros o en correos electrónicos.
- 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