	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 150	Fecha: 26-06-2023
		Página 34 de 37

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de identidad de la empresa de entretenimiento y plataforma de Streaming 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 Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se vienen llevando a cabo una campaña de Phishing, quienes vienen suplantando la identidad de la empresa de entretenimiento y plataforma de Streaming Netflix, el supuesto sitio web cuenta con logos característicos al oficial, el cual tiene como finalidad robar sus credenciales de acceso y datos bancarios.

2. **DETALLES:**

El proceso de estafa de Phishing es el siguiente:

Imagen 1: Sitio web fraudulento de Netflix, donde solicita acceder a la plataforma a través de las credenciales de acceso (correo electrónico y contraseña).

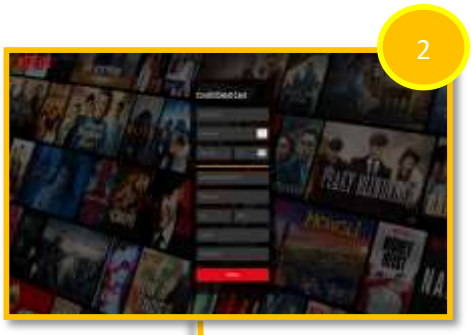


Imagen 2: Una vez ingresado las credenciales de acceso redirige a una ventana en donde solicita ingresar datos bancarios de la tarjeta.

Imagen 4: Por último, redirige automáticamente a un supuesto sitio web de NETFLIX.

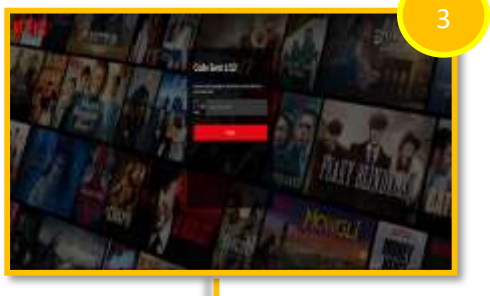


Imagen 3: Redirecciona a una ventana donde solicita un código al que se le envía al número de teléfono proporcionado.

A. INDICADORES DE COMPROMISO:

La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como SUPLANTACIÓN DE IDENTIDAD:

- **URL:** hxxp://netflix-clone-8tofe8hh5-jaker94[.]vercel[.]app

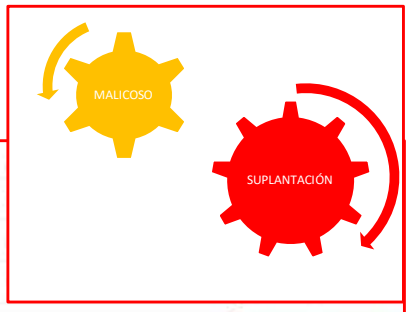
- **Dominio:** vercel[.]app

- **IP:** 76[.]76[.]21[.]93

- **Proveedor de alojamiento:** AMAZON-02

- El analizador de proveedores encontró **23 proveedores de seguridad detectaron esta URL como maliciosa** de los cuales 17 son suplantaciones de identidad, 6 malicioso.

SUPLANTACIÓN
MALICIOSO



Anti-AVL	Malicioso		
BitDefender	Suplantación de identidad		
CRDF	Malicioso		
Emsisoft	Suplantación de identidad		
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	Navegación segura de Google	Suplantación de identidad
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad
netcraft	Malicioso	OpenPhish	Suplantación de identidad
Base de datos de phishing	Suplantación de identidad	Segasec	Suplantación de identidad
Sophos	Suplantación de identidad	Onda de confianza	Suplantación de identidad
Inteligencia de amenazas de Viettel	Suplantación de identidad	VIPRE	Malicioso
ratz web	Malicioso		

B. OTRAS DETECCIONES:

3. RECOMENDACIONES:

- No abras correos, ni mensajes de dudosa procedencia.
- Sé escéptico (desconfiado) frente ofertas, promociones o premios increíbles que se ofrecen por internet que te soliciten ingresar tus datos personales y bancarios.
- No introduzcas datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Mantén actualizados todas las plataformas de tecnologías y de detección de amenazas.

Fuentes de información	Análisis propio de redes sociales y fuente abierta