	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°285	Fecha: 29-11-2023
		Página: 9 de 12

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	G01
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:**

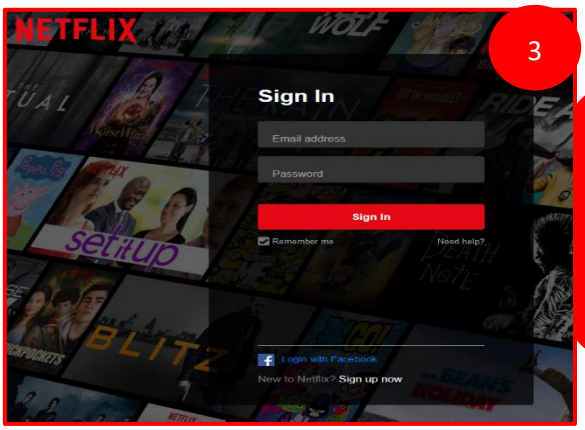
El proceso de estafa de Phishing es el siguiente:

1

Imagen 1
Sitio web fraudulento de Netflix, informa a la víctima que para crear o reiniciar su membresía tiene que registrarse en la plataforma a través de credenciales de acceso (correo electrónico y contraseña).

2

Imagen 2
Luego de darle clic en <empezar>, el atacante le solicita a la víctima registrar la contraseña para poder ingresar.



3

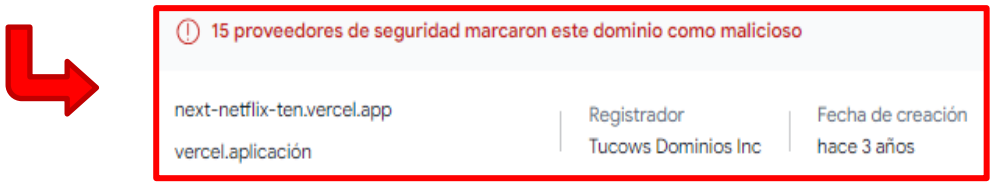
Imagen 3
Luego de completar los datos requeridos, le redirige a la víctima automáticamente a un supuesto sitio web de NETFLIX; sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la víctima.

A. INDICADORES DE COMPROMISO:

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

alfaMontaña.ai	Suplantación de identidad	AlfaSOC	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Clúster25	Suplantación de identidad	CRDF	Malicioso
propiedad intelectual criminal	Suplantación de identidad	CyRadar	Malicioso
ESET	Suplantación de identidad	Datos G	Suplantación de identidad
Kaspersky	Suplantación de identidad	leonico	Malicioso
OpenPhish	Suplantación de identidad	Base de datos de phishing	Suplantación de identidad
Sofos	Suplantación de identidad		

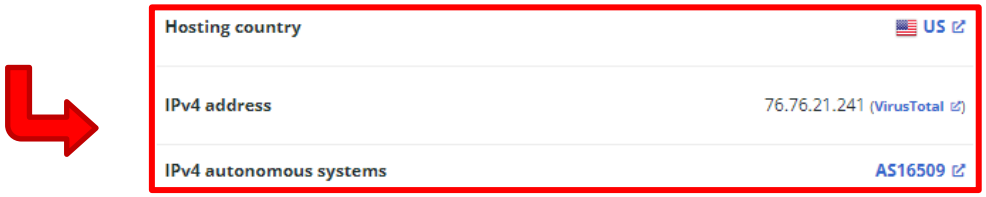
- **URL:** hxxp://next-netflix-ten[.]vercel[.]app



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

	Prueba	Resultado
✖	Registro DMARC publicado	No se encontró ningún registro DMARC
✖	Registro DNS publicado	Registro DNS no encontrado
!	Política DMARC no habilitada	Política de cuarentena/rechazo DMARC no habilitada

- **IP:** 76[.]21[.]241



- **SHA-256:** baae518719f177a5d49d056ad6bbc42fb382329305db69a059d4edeba51b8a13

3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial de Netflix.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.
- Ingresar desde fuentes oficiales (hxxps://www.netflix.com/browse).

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