	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 29-01-2024
		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 plataforma de entretenimiento en línea 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		

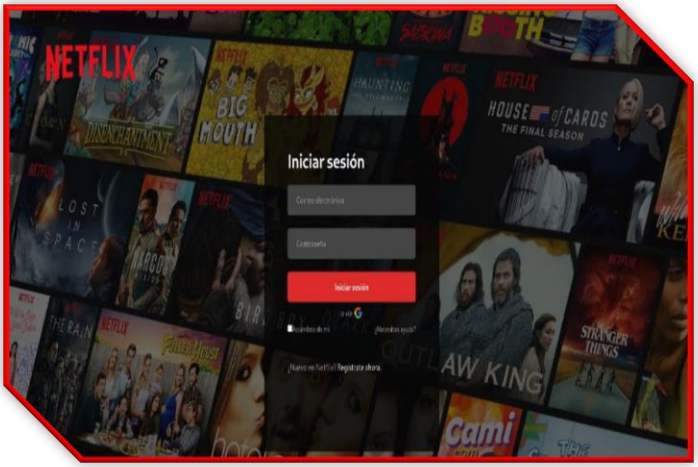
Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que ciberdelincuentes 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 del Phishing es el siguiente:



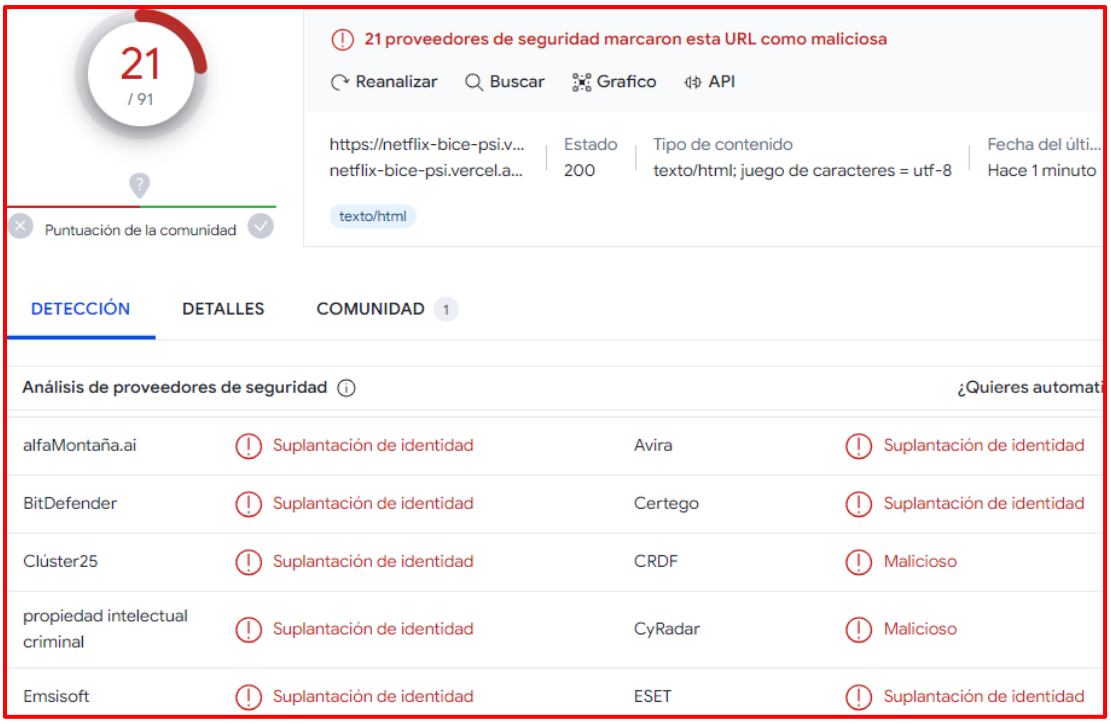
Paso N.º 01

Sitio web fraudulento de Netflix, solicita a la víctima registrar las credenciales de acceso (Correo electrónico y contraseña), para luego dar clic en <**Iniciar Sesión**>. Pero, pasados unos segundos, redirige al sitio web oficial de la plataforma de entretenimiento; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

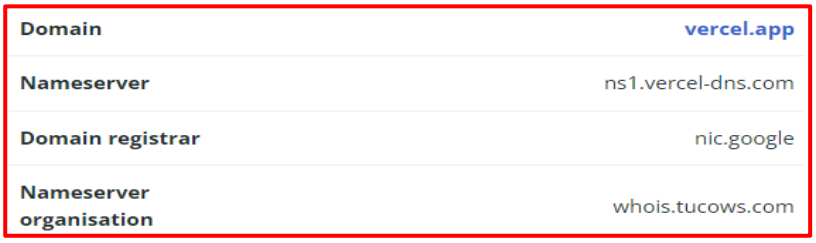
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento POSEE protocolo de seguridad de red (https), sin embargo, es malicioso.
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. Proveedores de seguridad informática ALERTAN COMO SUPLANTACIÓN DE IDENTIDAD - PHISHING.

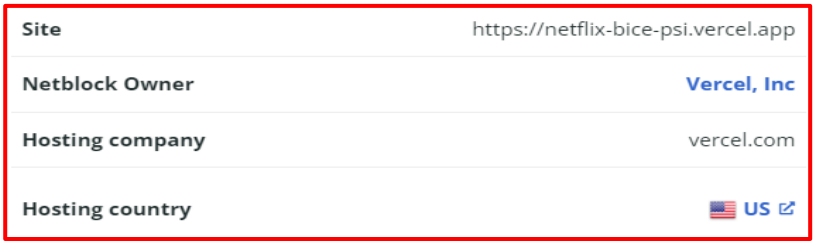


C. Indicadores de compromiso (IoC)

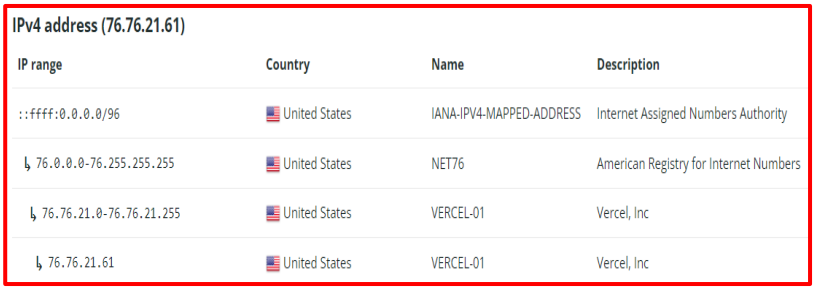
- Dominio : vercel[.]app



- URL : hxxps://netflix-bice-psi[.]vercel[.]app



- IP : 76[.]76[.]21[.]61



- Servidor : Vercel
- SHA-256 : 4573293eb1d01dfd0aef9d39eeb619b728157bb3f641ed12f035cd480e62b16c
- Tipo de tex. : Text/Html

D. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.).

E. Referencia:

- Phishing o suplantación de identidad, es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).

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