	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°007	Fecha: 08-01-2024
		Página: 10 de 13

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:

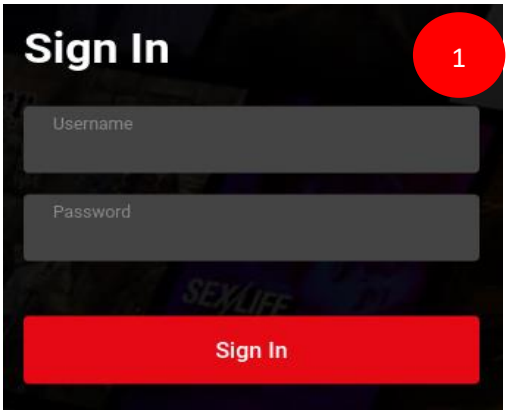


Imagen 1
Sitio web fraudulento de Netflix, informa a la víctima que para ingresar a su cuenta de Netflix debe de registrar las credenciales de acceso (correo electrónico y contraseña).

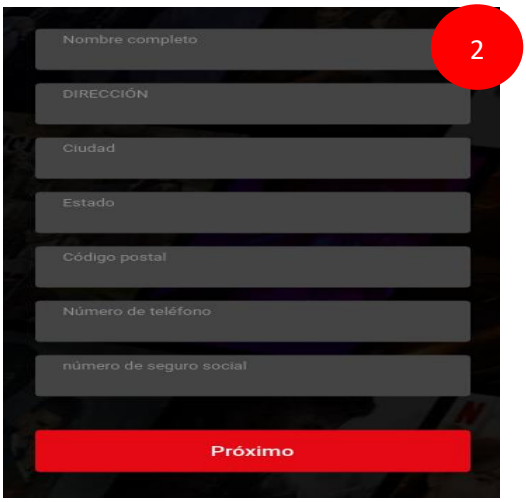


Imagen 2
Luego de darle clic en <Ingresar>, el atacante le solicita a la víctima registrar su nombre completo, Dirección, Ciudad, Estado, Código Postal, Número de teléfono y su número de seguro social, para poder actualizar sus datos.

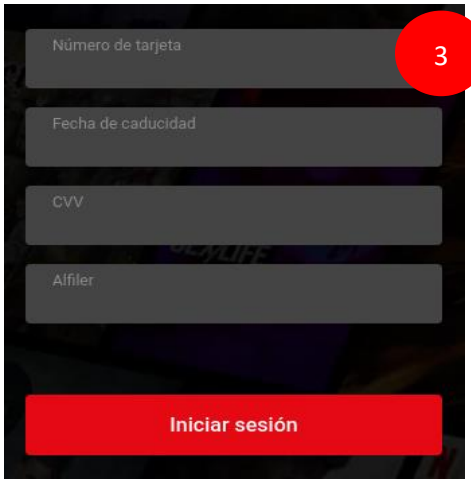
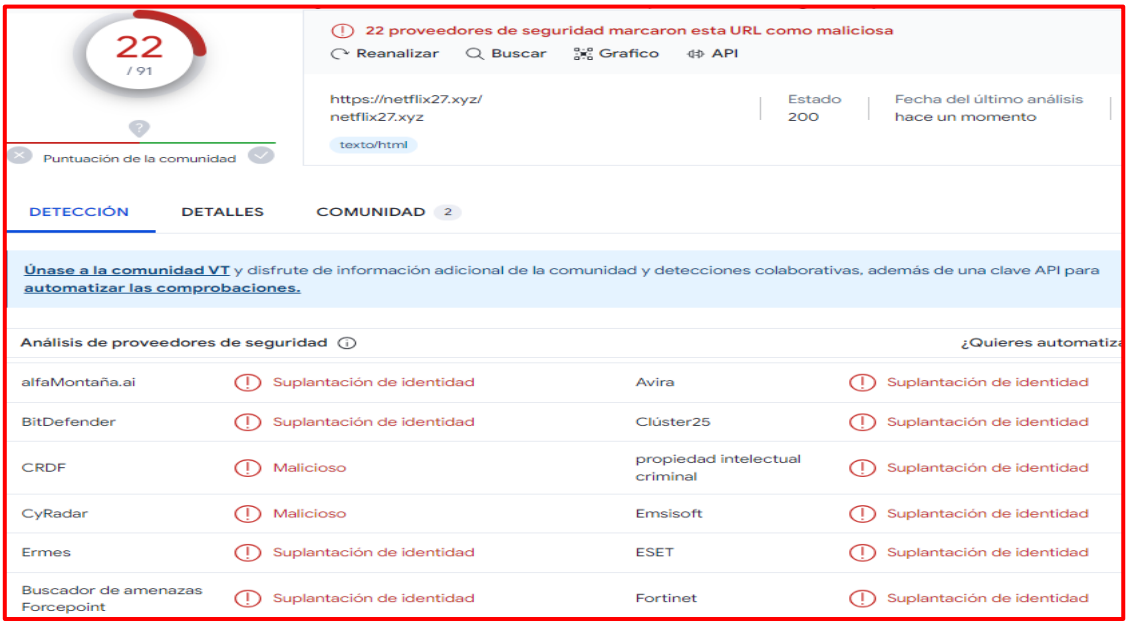


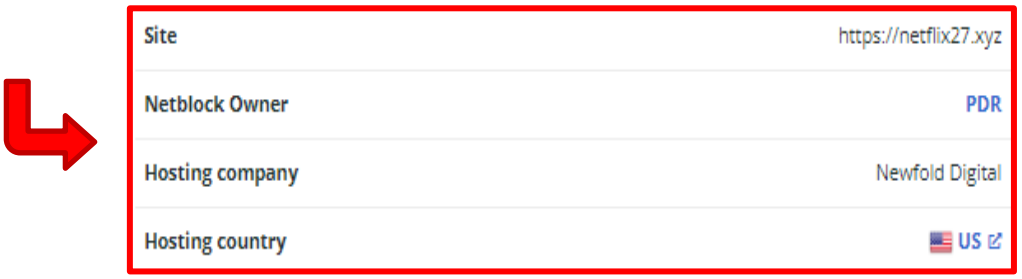
Imagen 3
Luego de darle clic en <Próximo> solicita el número de tarjeta, Fecha de caducidad Y CVV, para iniciar sesión; al completar los datos requeridos de la víctima le redirige automáticamente a un supuesto sitio web de NETFLIX; sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la víctima.

A. INDICADORES DE COMPROMISO:

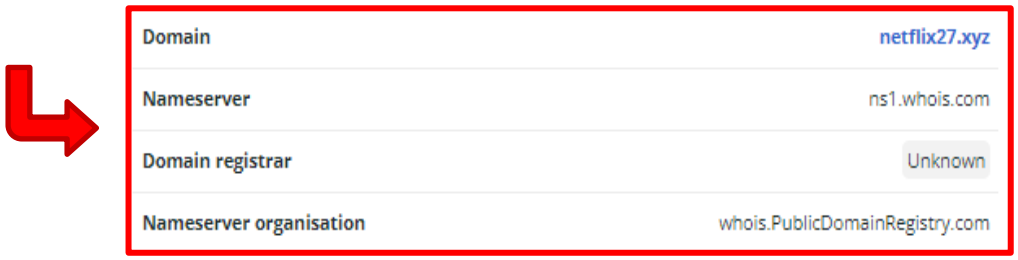
La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD**:



- **URL:** hxxps://netflix27[.]xyz/



- **Dominio:** netflix27[.]xyz



- **IP:** 162[.]251[.]85[.]174

- **SHA-256:** c066a93b948ec4ce5b255e4e20bdab9e1ce96b79a0f72367fdd2315549ea5921
- **Servidor:** Apache

- **Otras detenciones**

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 (https://www.netflix.com/browse).

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