	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:

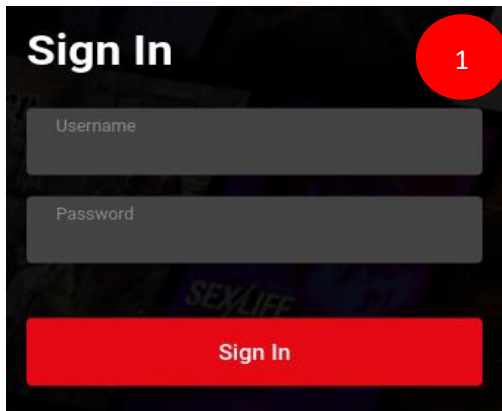


Imagen 1
Sitio web fraudulento de Netflix, informa a la víctima que para ingresar a su cuenta de Netflix debe de registrar las credenciales de acceso (correo electrónico y contraseña).

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.

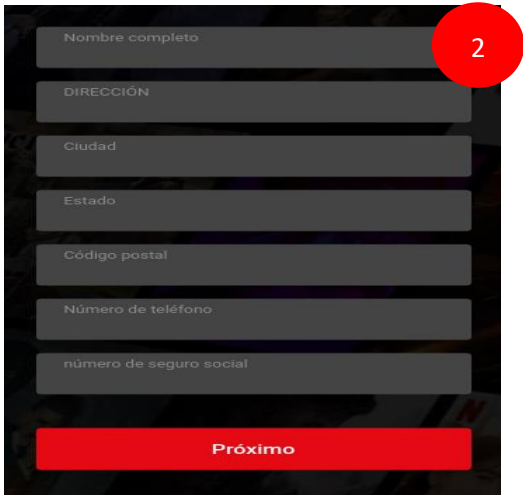
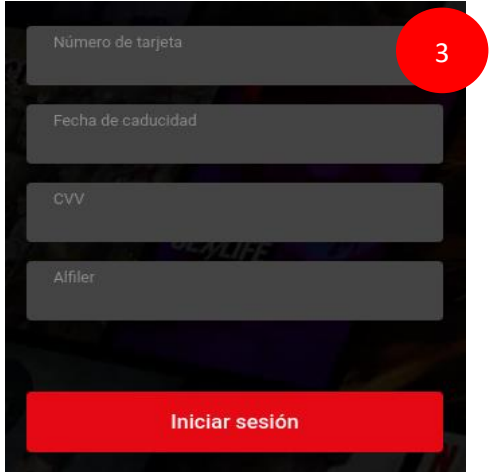
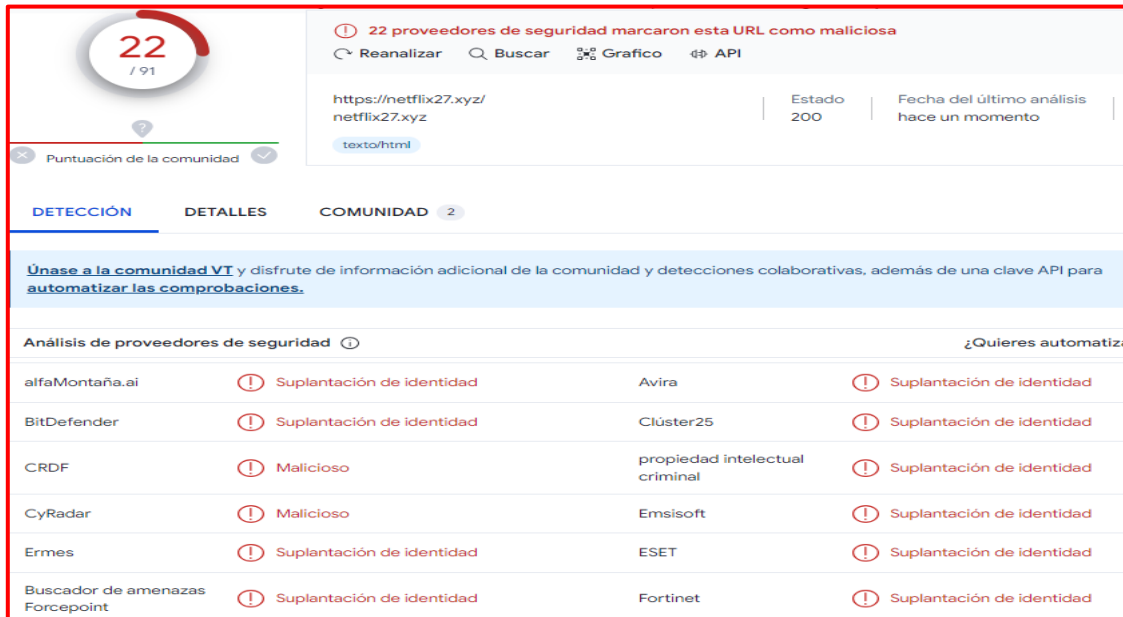


Imagen 3
Luego de darle clic en <Próximo> solicita el número de tarjeta, Fecha de caducidad Y CVV, para iniciar sesión; al completar los datos requeridos de la víctima le dirige automáticamente a un supuesto sitio web de NETFLIX; sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la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



A. INDICADORES DE COMPROMISO:

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



22 / 91
 22 proveedores de seguridad marcaron esta URL como maliciosa
 Reanalizar Buscar Grafico API
 https://netflix27.xyz/ Estado 200 Fecha del último análisis hace un momento
 texto/html
 Puntuación de la comunidad
 DETECCIÓN DETALLES COMUNIDAD 2
 Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.
 Análisis de proveedores de seguridad ¿Quieres automatizar?

Proveedor	Resultado	Detalles	Proveedor	Resultado
alfaMontaña.ai	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		Emsisoft	Suplantación de identidad
Ermes	Suplantación de identidad		ESET	Suplantación de identidad
Buscador de amenazas Forcepoint	Suplantación de identidad		Fortinet	Suplantación de identidad

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



Site	https://netflix27.xyz
Netblock Owner	PDR
Hosting company	Newfold Digital
Hosting country	US

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



Domain	netflix27.xyz
Nameserver	ns1.whois.com
Domain registrar	Unknown
Nameserver organisation	whois.PublicDomainRegistry.com

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



IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
162.0.0-162.255.255	United States	NET162	Various Registries (Maintained by ARIN)
162.251.00.0-162.251.06.255	United States	PUBLICDOMAINREGISTRY-NETWORKS	PDR
162.251.85.174	United States	PUBLICDOMAINREGISTRY-NETWORKS	PDR

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

Otras detenciones

Two screenshots of a security analysis tool showing 'MALICIOSO' (Malicious) results for the URL <https://netflix27.xyz/>. The left screenshot shows a 24% AV detection rate and 3 indicators. The right screenshot shows an 8% AV detection rate and 12 indicators. A red arrow points from these screenshots to a summary box on the right containing the text 'malicioso', 'Puntuación de amenaza: 100/100', 'Detección AV: 67%', and '#suplantación de identidad'.

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.