	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 109	**Fecha: 10-05-2023**
		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 subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. 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 del proceso de estafa de Phishing.

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.

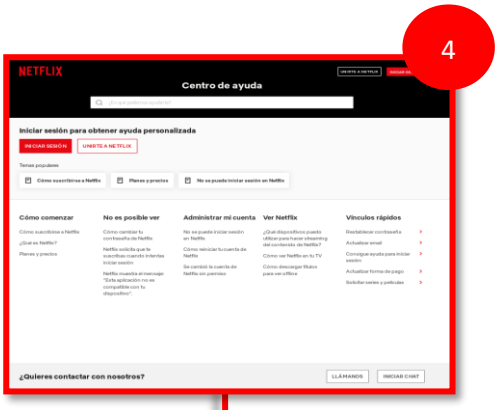


Imagen 4: Por último, redirige automáticamente a un supuesto sitio web de NETFLIX.

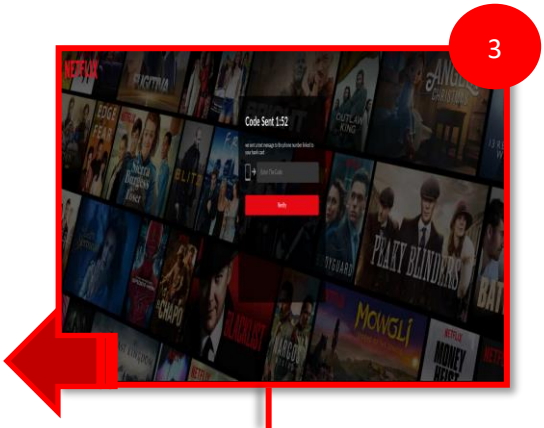


Imagen 3: Redirecciona a una ventana donde solicita un código al que se le envía al número de teléfono proporcionado.

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

a. INDICADORES DE COMPROMISO:

i. URL: hxxps://mynetflix-fix-suspension.com/

ii. Dominio: mynetflix-fix-suspension[.]com

iii. IP: 91[.]215[.]85[.]193

iv. Código: 200

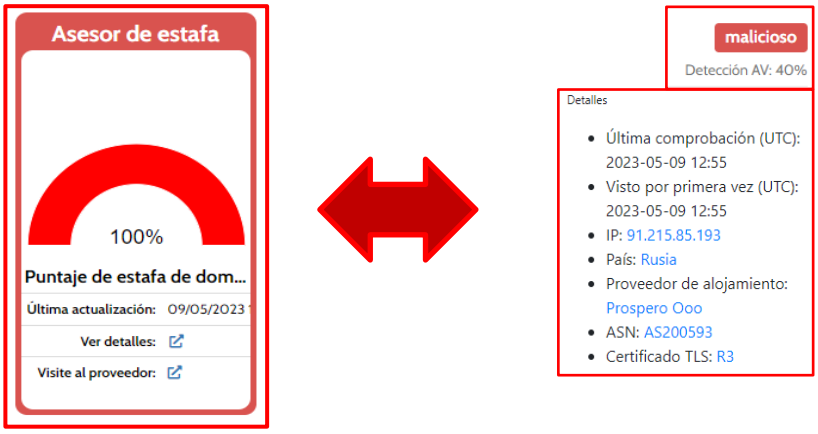
v. Longitud: 1.58KB

vi. SHA-256: b42ca9e99d5f4b5962de58cfaf2848f2d524778f99c51e11c22214d0a5b002b0

vii. El analizador de proveedores encontró **18 proveedores de seguridad marcaron esta URL como maliciosa** de los cuales 9 son suplantaciones de identidad, 6 malicioso y 3 malware.

alphaMountain.ai	Suplantación de identidad	AlphaSOC	Suplantación de identidad
Anti-AVL	Malicioso	Avira	Suplantación de identidad
BitDefender	Malware	CRDF	Malicioso
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
ESET	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	kaspersky	Suplantación de identidad
Leonico	Suplantación de identidad	netcraft	Malicioso
tanque de phishing	Suplantación de identidad	Búsqueda segura	Malicioso
Sophos	Malware	raíz web	Malicioso

4. OTRAS DETECCIONES:



5. Apreciación de la información

- Netflix, es un servicio de Streaming 'transmisión' de vídeo a través de Internet que permite ver una amplia variedad de series, películas, documentales y películas en cualquier dispositivo con acceso a internet; mediante el pago de una tarifa fija mensual.

6. Algunas 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