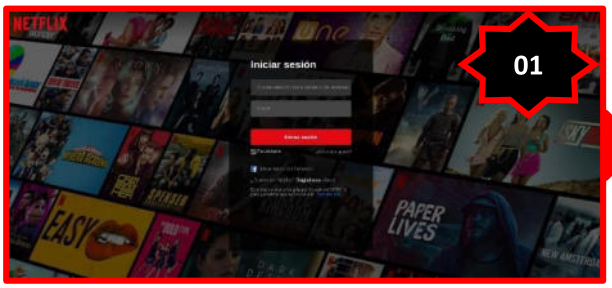
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 092	Fecha: 02-04-2022
		Página 5 de 7

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing que suplantan la identidad de 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 vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, quienes vienen suplantando la identidad de la plataforma de entretenimiento "NETFLIX", el supuesto sitio web cuenta con colores y logos característicos idénticos al sitio web oficial, el cual tiene como finalidad robar información confidencial de las posibles víctimas, como dirección de correo electrónico, contraseña, datos bancarios (nombre y número de la tarjeta de crédito o débito, fecha de expiración de la tarjeta, etc.).

2. ***Imagen: detalles del proceso de Phishing***.



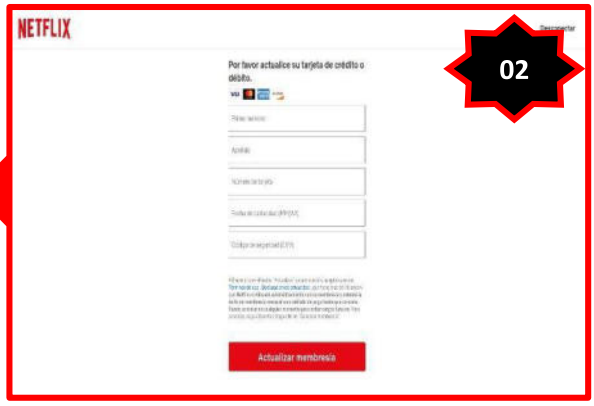
Paso Nº 01

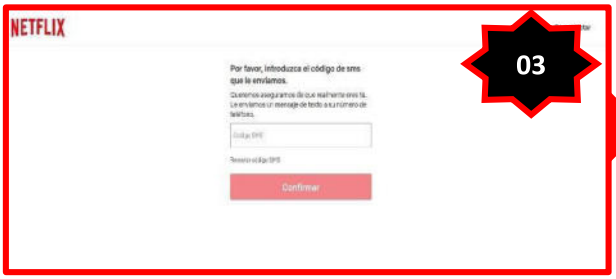
Requiere las credenciales de acceso (correo electrónico o número de teléfono móvil y contraseña) de la plataforma de entretenimiento Netflix, para luego dar clic en <Iniciar sesión>.

Paso Nº 02

Una vez ingresado las credenciales de acceso y dar clic en <Iniciar sesión>, aparece una pantalla donde solicita a la víctima actualizar datos de la tarjeta bancaria para actualizar la membresía, como:

- Nombre y apellido del titular de la tarjeta bancaria.
- Número de la tarjeta de crédito o débito
- Fecha de vencimiento de la tarjeta bancaria.
- Código de seguridad (CVC).



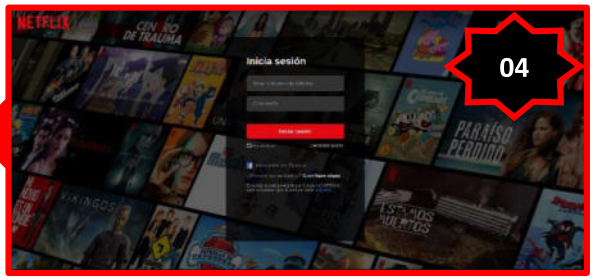


Paso Nº 03

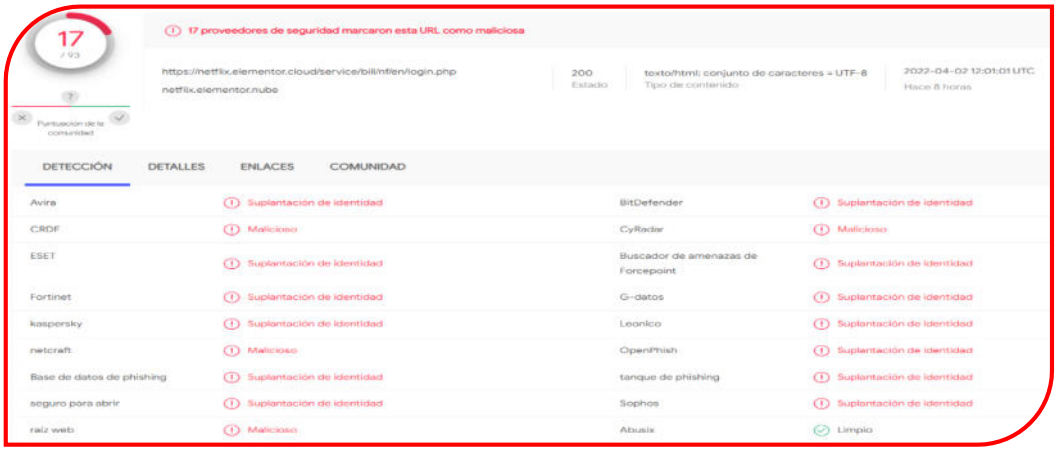
Luego de dar clic en <Actualizar Membresía> en el paso Nº 02, se muestra a una ventana con la descripción que registre el código enviado al número del teléfono móvil o correo electrónico, registrado en el paso Nº 01; para después dar clic en <Confirmar>.

Paso Nº 04

Después de registrar el código de verificación en el paso Nº 03, al dar clic en <Confirmar>, es redirigido al sitio web oficial de la plataforma de entretenimiento NETFLIX; sin embargo, los ciberdelincuentes obtuvieron los datos brindado por la víctima.



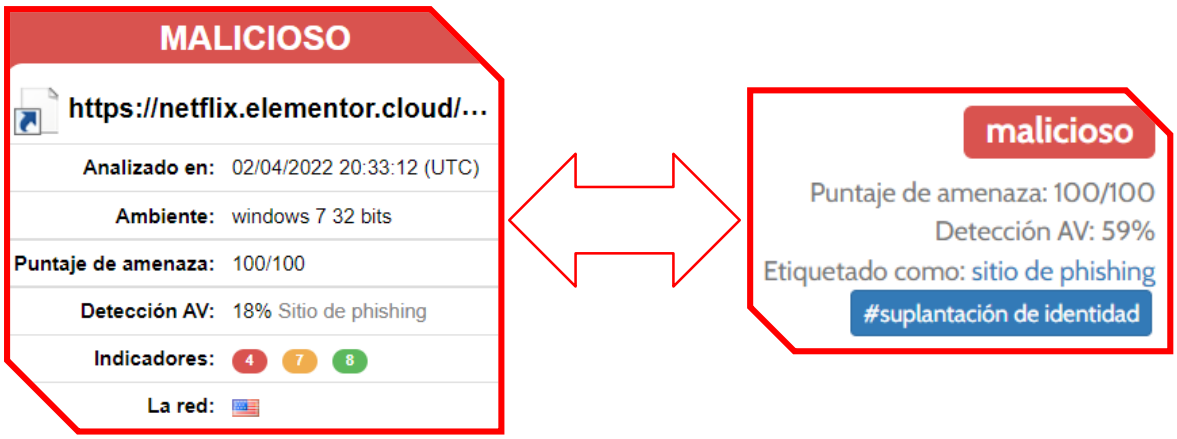
3. ***Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.***



4. ***Indicadores de compromiso (IoC)***

- ✓ URL : hxxps://netflix[.]elementor[.]cloud/service/bill/nf/en/login[.]php
- ✓ Dominio : elementor[.]cloud
- ✓ SHA-256 : ef575a826f1fd5ccbf84947121a415201e61069f23e4f99a699e826e5196d5d4
- ✓ IP : 162[.]159[.]138[.]9

5. ***Otras detecciones:***



6. ***Apreciación de la información*:**

- La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso e información bancaria (tarjetas de crédito o débito) de los usuarios de la plataforma de entretenimiento NETFLIX.
- La propagación del sitio web fraudulento se realiza mediante envió masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger y mensajes de textos (SMS).

7. ***Algunas recomendaciones:***

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta