	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°212	Fecha: 08-09-2023
		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 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:

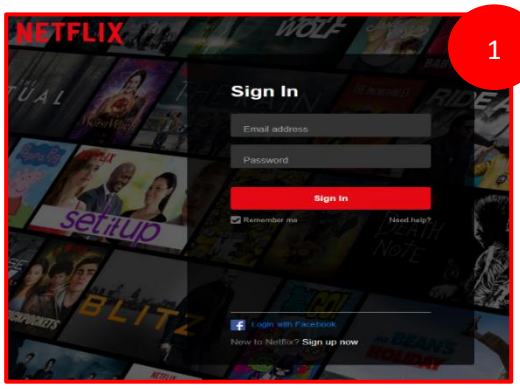


Imagen 1
Sitio web fraudulento de Netflix, solicita a la víctima acceder a la plataforma a través de credenciales de acceso (correo electrónico y contraseña).

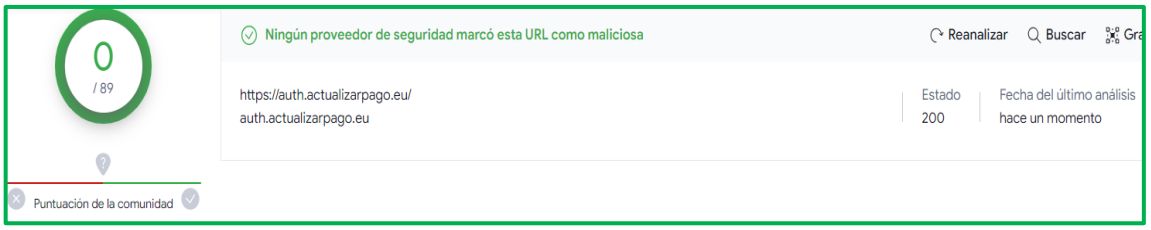
Imagen 2
Una vez ingresado las credenciales de acceso en el sitio web fraudulento, el atacante solicita a la víctima que configure la tarjeta de crédito o débito.

Imagen 3
Luego de completar los datos bancarios de la tarjeta, le informa que se le ha enviado un mensaje de texto con una contraseña.

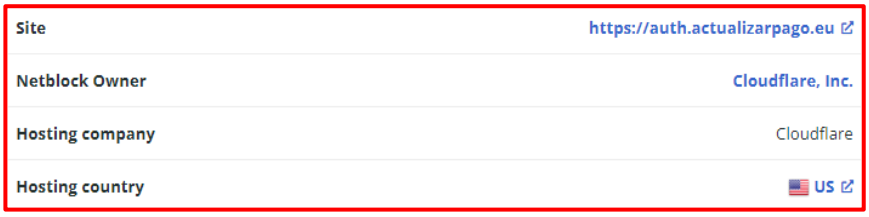
Imagen 4
Al completar con lo requerido es redirigido al sitio oficial web de NETFLIX, aparentando un error de autenticación.

A. INDICADORES DE COMPROMISO:

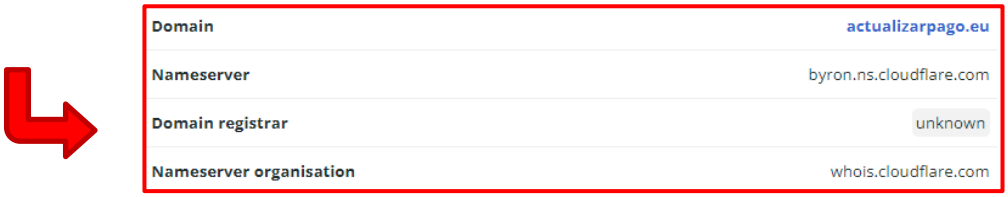
Hasta la formulación del presente documento, proveedores de seguridad informática NO HAN ALERTADO como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



- **URL:** hxxps://auth[.]actualizarpago[.]eu/



- **Dominio:** actualizarpago[.]eu



- **IP:** 104[.]21[.]46[.]76

- **SHA-256:** f2ac71d861166d6e2602e0d042821b9200a9fb0b3131d1f39be421bc6980bf64
- **Servidor:** Cloudflare
- **Tipo de Contexto:** Text/Html

B. ¿Qué es el Phishing?

Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

C. Apreciación de la información:

La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso de la plataforma de entretenimiento y una plataforma de Streaming.

La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial del banco BBVA.
- 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