	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 283	Fecha: 18-10-2022
		Página 05 de 07

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, a través 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 y contraseña) de la plataforma de entretenimiento Netflix, para luego dar clic en <Iniciar sesión>.

Paso Nº 03

Una vez hecho clic en <Asegure su cuenta>, aparece una pantalla solicitando que requiere actualizar los datos personales de la víctima:

- Nombre 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).
- Dirección y código postal.
- Número de teléfono móvil.

Paso Nº 02

Sitio web fraudulento de Netflix, donde solicita a la víctima, actualizar dirección de facturación y método de pago.

Paso Nº 04

Luego, aparece otra ventana que requiere la información de los datos de la tarjeta de crédito o débito.

Paso Nº 04

Después de registrarse la víctima, es redirigido al sitio web oficial de la Plataforma de entretenimiento de Netflix; sin embargo, los ciberdelincuentes obtuvieron los datos brindado por la víctima.

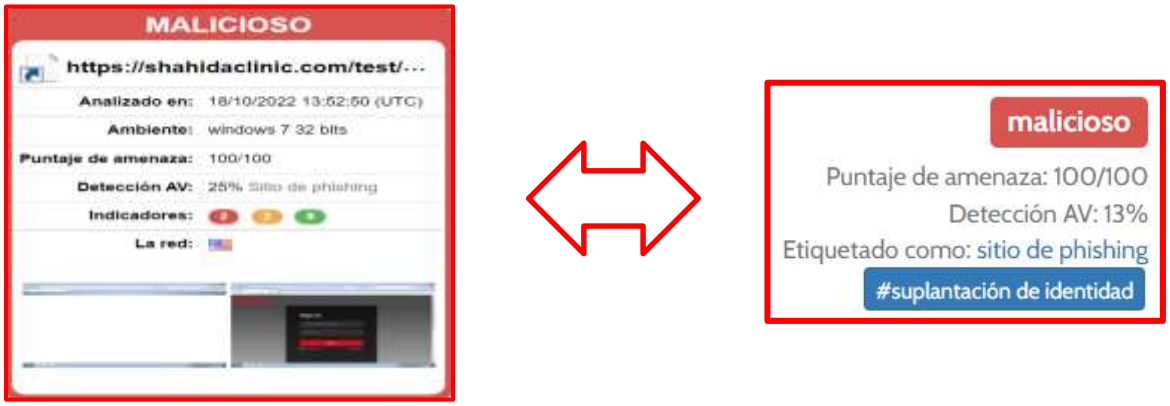
3. *Se procedió analizar la URL fraudulenta, obteniendo como resultado que VIENTITRES (23) proveedores de seguridad informática alertan como* ***SUPLANTACIÓN DE IDENTIDAD - PHISHING.***

alphaMountain.ai	Suplantación de identidad	Anti-AVL	Malicioso
Avira	Suplantación de identidad	Bitdefender	Suplantación de identidad
Veredicto de Comodo Valkyrie	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
CASO	Suplantación de identidad	Buscador de amenazas de Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	G-datos	Suplantación de identidad
Navegación segura de Google	Suplantación de identidad	kaspersky	Suplantación de identidad

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

- ✓ URL : hxxps://shahidaclinic[.]com/test/wp-content/Netflix/23f09b21324d1ed3cd722109bd55d6e7
- ✓ Dominio : shahidaclinic[.]com
- ✓ SHA-256 : 1b36b45754a3a9c16ddfc5aa318c8e4aa3a838fe4f40793cb771b6a15053f926
- ✓ IP : 192[.]254[.]232[.]43
- ✓ Servidor : Nginx/1.21.6

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.
- Ante cualquier sospecha de haber caído en el engaño del Phishing, accede a tu cuenta y cambia la contraseña.

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