	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 063	Fecha: 14-03-2023
		Página 10 de 12

Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva campaña de Phishing que suplanta 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 avanzados ataques cibernéticos, por medio de envíos masivos de correos electrónicos fraudulentos, o también conocidos como Phishing, simulado ser la plataforma de entretenimiento de Netflix, en el contenido del mensaje se indica lo siguiente: ***"Actualiza tu cuenta para seguir disfrutando Netflix, ingresando en el enlace adjunto <<ACTUALIZAR CUENTA AHORA>>",*** con el objetivo robar credenciales de acceso, datos personales y datos bancarios.

2. Detalles del proceso de Phishing:

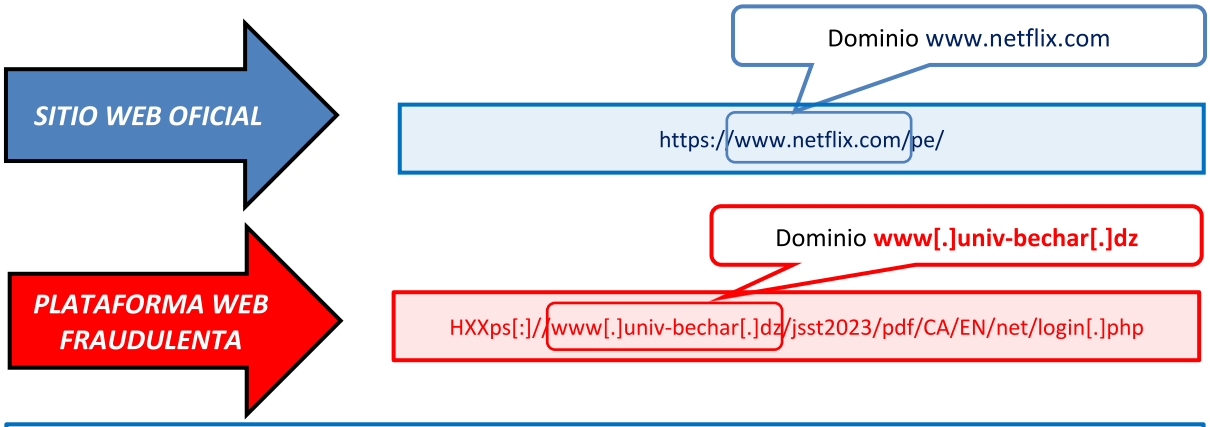
Imagen 1. Correo que llega a la víctima instando hacer clic en el enlace **<<ACTUALIZAR CUENTA AHORA>>**

Imagen 2. Una vez hecho clic, en ***<<ACTUALIZAR CUENTA AHORA>>***, es redirigido a una web falsa similar al oficial de Netflix, donde solicita ingresar las credenciales de acceso.

Imagen 3. Al hacer clic, en **<<iniciar sesión>>**, es dirigida a esta pagina que solicita ingresar los datos de la tarjeta de crédito o débito.

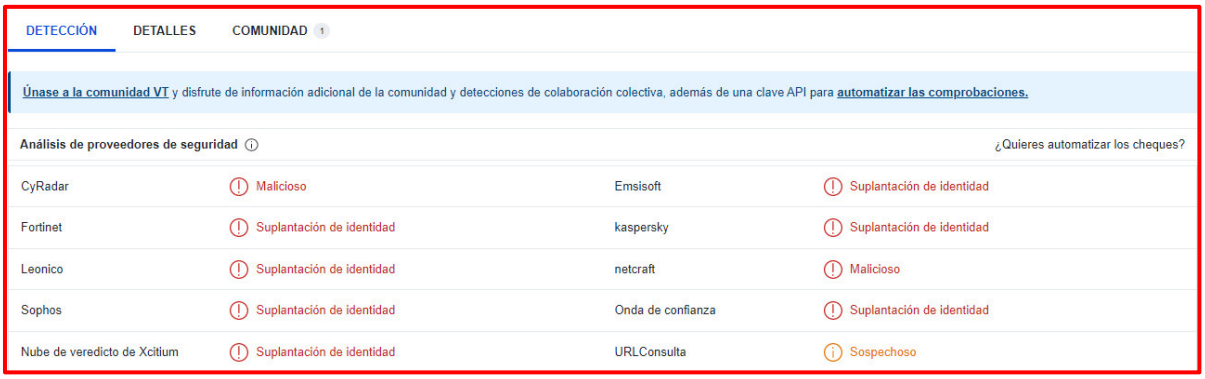
Imagen 4. Luego de haber actualizado la membresía, es redirigido al sitio web oficial de Netflix, aludiendo un aparente error; sin embargo, los datos fueron capturados.

3. Comparación del sitio web oficial y sitio web fraudulento de Netflix:



- Existe diferencia en el dominio de sitio web fraudulento, no coincide con el oficial.
- El sitio web fraudulento posee el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),** lo que hace convincente a la víctima al momento de ingresar a la web falsa.

4. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**:



DETECCIÓN | DETALLES | COMUNIDAD 1

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones de colaboración colectiva, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad			¿Quieres automatizar los cheques?
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
Fortinet	Suplantación de identidad	kaspersky	Suplantación de identidad
Leonico	Suplantación de identidad	netcraft	Malicioso
Sophos	Suplantación de identidad	Onda de confianza	Suplantación de identidad
Nube de veredicto de Xcitium	Suplantación de identidad	URLConsulta	Sospechoso

- Indicadores de compromiso:
  - URL: hXXps[:]//www[.]univ-bechar[.]dz/jsst2023/pdf/CA/EN/net/login[.]php
  - Dominio: www[.]univ-bechar[.]dz
  - SHA-256: af38021011f0e0ea1af160b7301df2a5e9fd7164a360e97cfd6fdeea6fc5c335
  - Dirección IP: 193[.]194[.]79[.]226
  - Código: 200
  - Longitud: 8.97KB

5. Recomendaciones:

- Verificar detalladamente la URL, que corresponda al sitio web oficial de Netflix.
- Ingresar desde fuentes oficiales.
- 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.

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