	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 065	**Fecha: 16-03-2023**
		Página 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la 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.

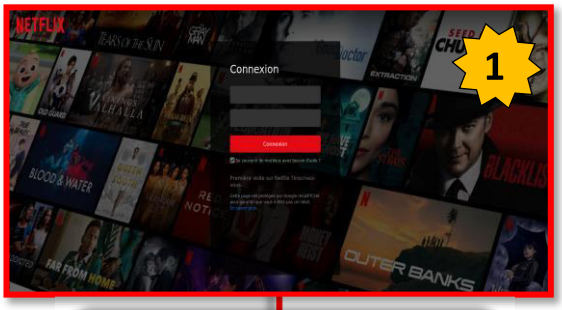


Imagen 1: Sitio web fraudulento, donde solicita acceder a la plataforma a través de las credenciales de acceso (correo electrónico y contraseña).

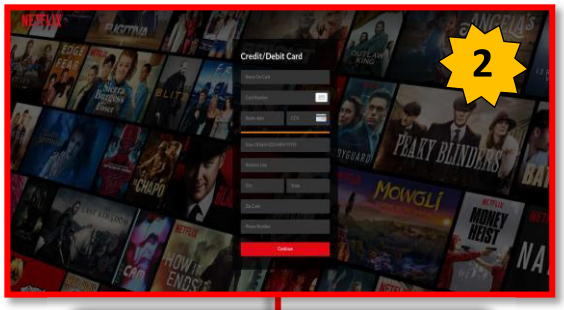


Imagen 2: Una vez ingresado las credenciales de acceso redirige a una ventana en donde solicita ingresar datos bancarios de la tarjeta.

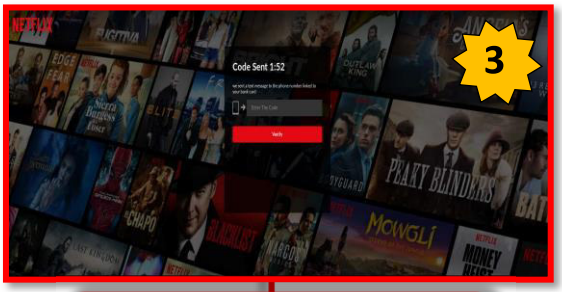


Imagen 3: Redirige a una ventana donde solicita un código al que se le envía al número de teléfono proporcionado.

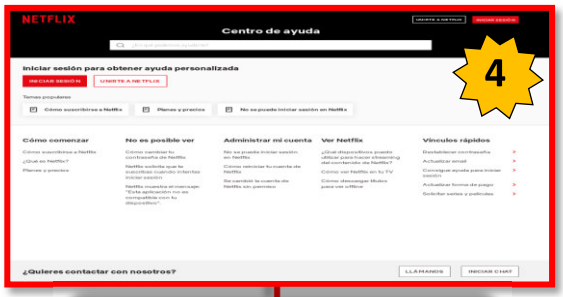
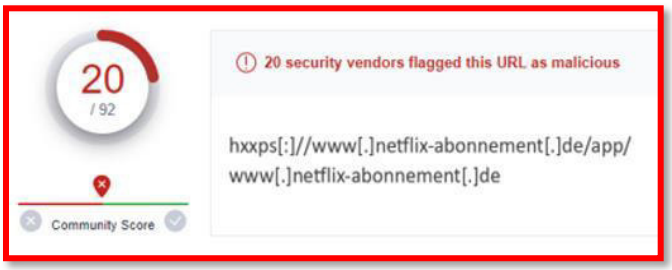


Imagen 4: Por último, redirige automáticamente a un supuesto sitio web de NETFLIX.

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

- **INDICADORES DE COMPROMISO:**
  - ✓ **URL:** hxxps[:]//www[.]netflix-abonnement[.]de/app/
  - ✓ **Dominio:** www[.]netflix-abonnement[.]de
  - ✓ **IP:** 193[.]42[.]32[.]83
  - ✓ **Código:** 200
  - ✓ **Longitud:** 6.62KB
  - ✓ **SHA-256**: a7fdab3c01efc46d09210757db090d2f2fb3f34cd1dd36043bc72060771efcb3



Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Malware	Cluster25	Phishing
CyRadar	Malicious	Emsisoft	Phishing
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing	G-Data	Malware
Google Safebrowsing	Phishing	Kaspersky	Phishing
Lionic	Phishing	Netcraft	Malicious
Phishtank	Phishing	Seclookup	Malicious
Segasec	Phishing	Sophos	Phishing
VIPRE	Malicious	Webroot	Malicious

- **OTRAS DETECCIONES:**