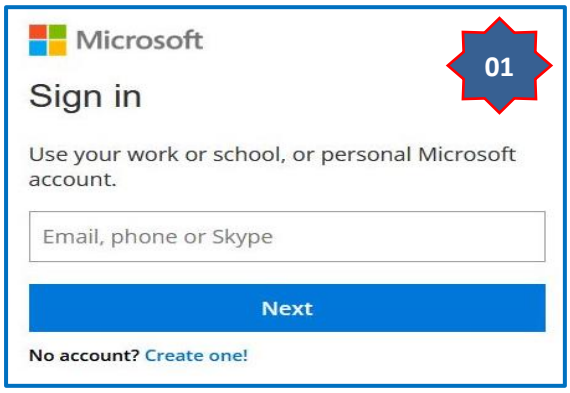
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 084	Fecha: 10-04-2023
		Página 5 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de la identidad de la Red Social Facebook		
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 actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica.

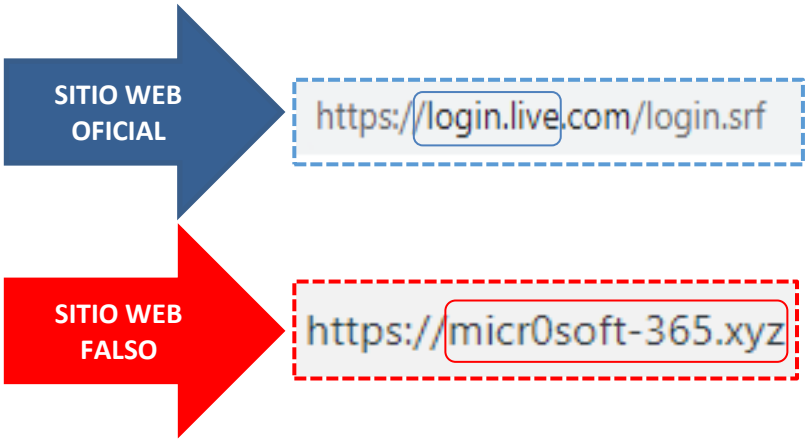
2. **Detalles del proceso de Phishing**



El atacante solicita a la victima que registre el correo electrónico de su trabajo, escuela o cuenta personal, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

Al registrar el correo, requiere la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Iniciar sesión>; sin embargo, después de unos segundos redirige al servicio del correo electrónico de la compañía Microsoft.

3. **Comparación del sitio web oficial y fraudulento.**



- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee el protocolo de seguridad de red (https), pero al ingresar es un sitio web fraudulenta.

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

5. Indicadores de compromiso (IoC)

- ✓ URL : hxxps://easydec[.]iinkedin[.]li/
- ✓ Dominio : iinkedin[.]li
- ✓ Server : Apache/2.4.41(Ubuntu)
- ✓ SHA-256 : c4a6ef1daacb9e61d10956d02e079e52e31a5216c0e97320d248e60ed1715caa
- ✓ IP : 185[.]237[.]25[.]26

6. Otras detecciones:

7. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).

- 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, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

8. Algunas Recomendaciones:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Realizar las actualizaciones correspondientes desde fuentes originales.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 084	**Fecha: 10-04-2023**
		Página 8 de 11

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

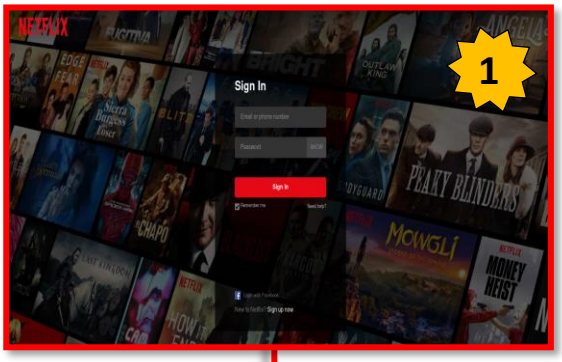


Imagen 1: Sitio web fraudulento, donde solicita acceder a la plataforma a través de las credenciales de acceso (correo electrónico y contraseña).

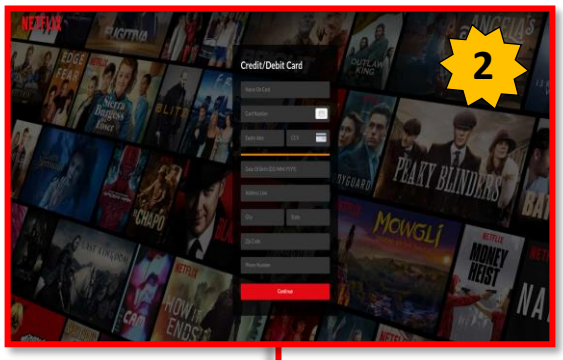


Imagen 2: Una vez ingresado las credenciales de acceso redirige a una ventana en donde solicita ingresar datos bancarios de la tarjeta.

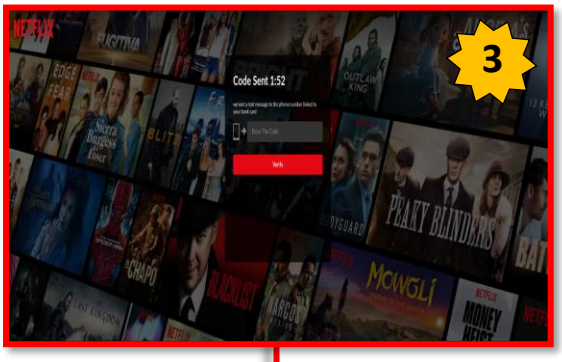


Imagen 3: Redirige a una ventana donde solicita un código al que se le envía al número de teléfono proporcionado.

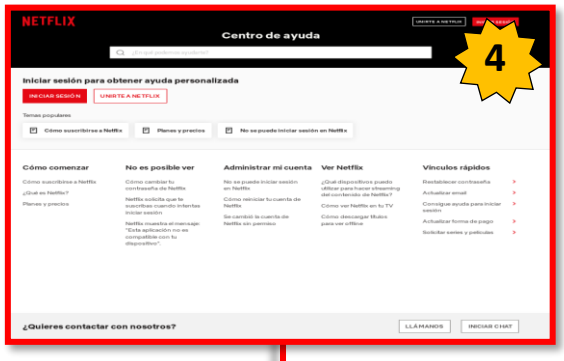


Imagen 4: Por último, redirige automáticamente a un supuesto sitio web de NETFLIX.

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://netflix-clone-project-1ypg452ly-muhammad32130o1[.]vercel.app/login
  - ✓ **Dominio:** netflix-clone-project-1ypg452ly-muhammad32130[.]vercel[.]app
  - ✓ **IP:** 76[.]76[.]21[.]164
  - ✓ **Código:** 200
  - ✓ **Longitud:** 1.33KB
  - ✓ **SHA-256**: b4f44396c1ac8c7e738ebd91363717b090c95848a83964814d8671e4ceee6159

Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Phishing	CRDF	Malicious
CyRadar	Malicious	Emsisoft	Phishing
ESET	Phishing	G-Data	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	Segasec	Phishing
Sophos	Phishing	Webroot	Malicious

- **OTRAS DETECCIONES:**

4. Apreciación de la información

- Netflix, es un servicio de Streaming 'transmisión' de vídeo a través de Internet que permite ver una amplia variedad de series, películas, documentales y películas en cualquier dispositivo con acceso a internet; mediante el pago de una tarifa fija mensual.

5. Algunas Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Ser escépticos (desconfiado) frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

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