	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 062		Fecha: 13-03-2023
			Página 6 de 10
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva campaña de phishing que suplanta la identidad del sitio web "INTERBANK		
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, a través de los diferentes navegadores web, suplantando el sitio oficial de la financiera "INTERBANK", con el objetivo de acceder u obtener datos personales y/o bancarios; para luego utilizarlas por los ciberdelincuentes para cumplir con sus falsos propósitos.

2. **Imagen:** Proceso del ataque Phishing:

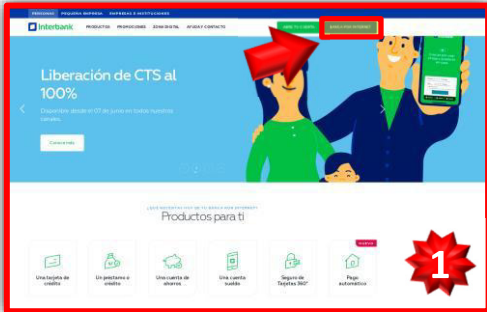


Imagen 1: Cuenta con los diferentes ítems similares que el sitio web original de la entidad financiera "Interbank" presenta.

Imagen 2: Al hacer clic en la opción "BANCA POR INTERNET", solicita ingresar el número de la tarjeta, DNI y la clave web.



Imagen 3: Se muestra una ventana aparentemente de la entidad financiera "INTERBANK", aludiendo como si estuviese cargando dicha página.

3. **Comparación del sitio web oficial del Banco Interbank, con el fraudulento:**

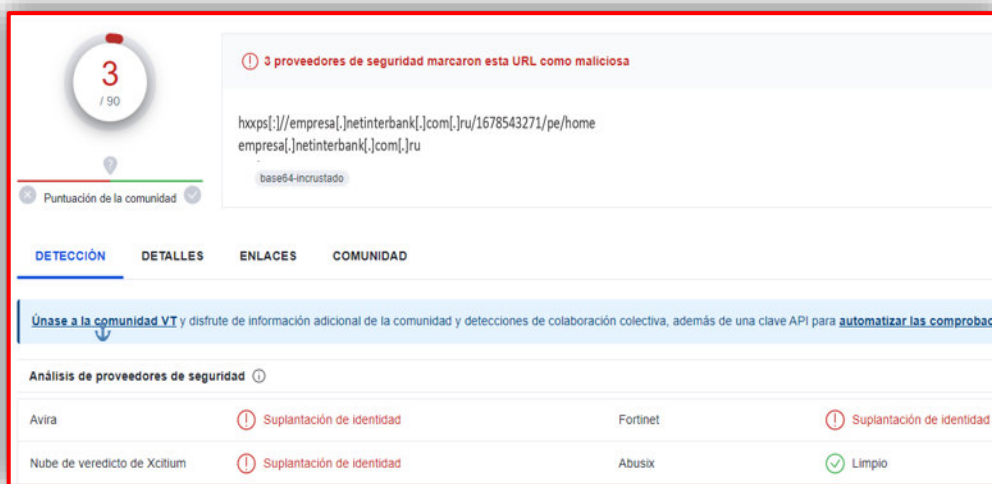
SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
URL: https://bancaporinternet.interbank.pe/login	URL: https://empresa[.]netinterbank[.]com[.]ru/1678543271/pe/banc4porinternet/login
	

- Existe similitud entre ambas páginas, en imagen, fondo y escritura la diferencia se encuentra en la URL.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- El dominio (empresa.netinterbank.com.ru) del sitio web fraudulento se encuentra reportado como PHISHING.
- La URL falsa está mal escrita y los caracteres ambiguos.

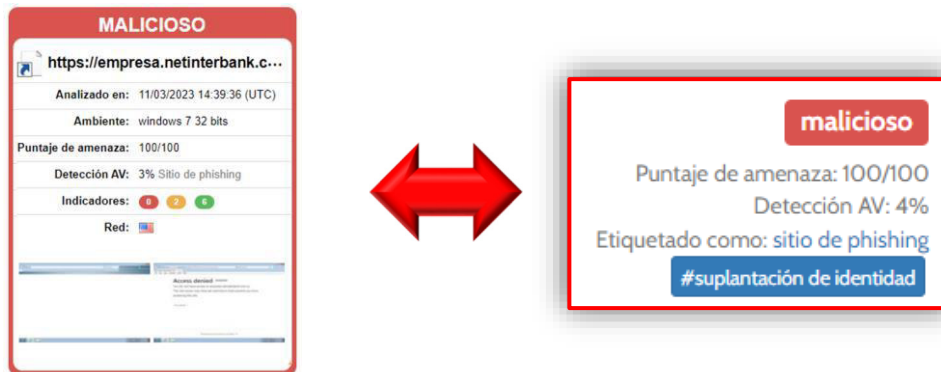
4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**:

• **INDICADORES DE COMPROMISO:**

- ✓ **URL:** hxxps[:]//empresa[.]netinterbank[.]com[.]ru/1678543271/pe/banc4porinternet/login
- ✓ **Dominio:** empresa[.]netinterbank[.]com[.]ru
- ✓ **IP:** 172[.]67[.]140[.]22
- ✓ **Código:** 403
- ✓ **Longitud:** 5.58KB
- ✓ **SHA-256:** 401cb7fad9c9813de6b4607176ef6435872ae4b3904b7680786799dabff1372



• **OTRAS DETECCIONES:**



5. **ALGUNAS RECOMENDACIONES:**

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta