	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°223	Fecha: 21-09-2023
		Página: 9 de 11

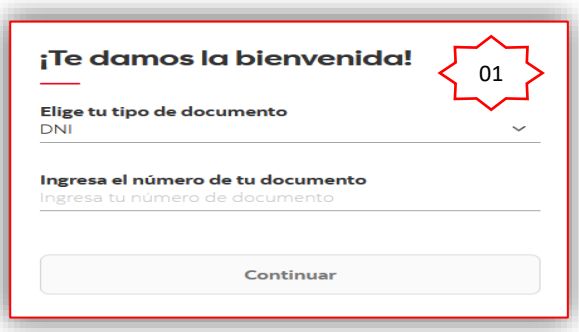
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria Scotiabank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

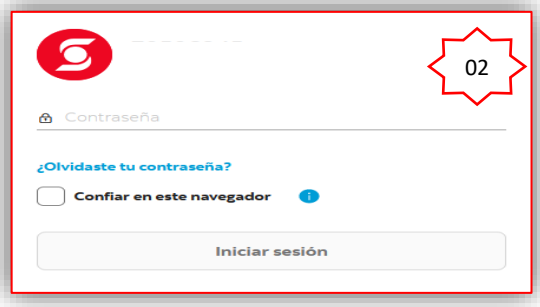
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web del Banco Scotiabank (Banca por internet), por medio de la creación de un sitio web falso que simula el oficial, con el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. **DETALLES:**



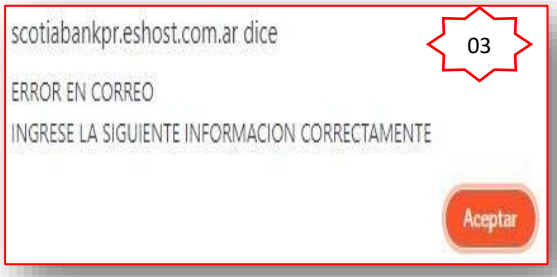
Paso N.º 01

El atacante mediante la creación de un sitio web fraudulento del banco Scotiabank, solicita a las posibles víctimas a ingresar el tipo de documento y numero de documento.



Paso N.º 02

Luego de continuar, solicita a las víctimas ingresar la contraseña de la cuenta bancaria.



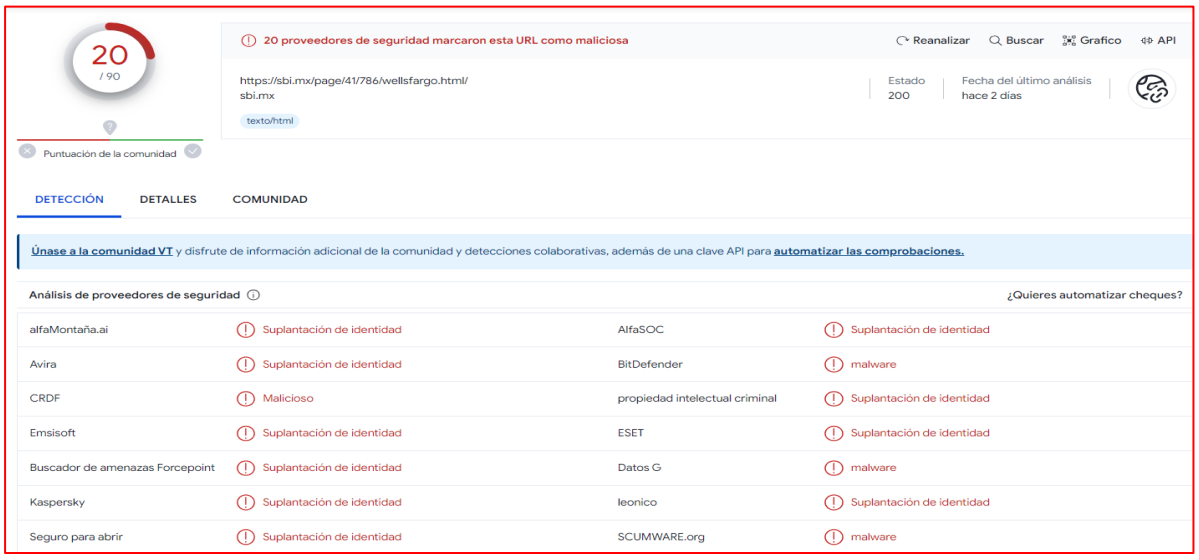
Paso N.º 03

Después, sale una ventana emergente, en la cual informa a la víctima que ha ocurrido error al colocar el correo.

Paso N.º 04

Finalmente, al completar lo requerido por el atacante, es redirigido automáticamente al sitio web oficial del banco Scotiabank, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **Phishing (suplantación de identidad):**



- **INDICADORES DE COMPROMISO (IoC)**

  - **URL** : hxxps://sbi[.]mx/page/41/786/wellsfargo[.]html
  - **Dominio** : sbi.mx
  - **IP** : 64[.]251[.]8[.]144

3. 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.
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.