

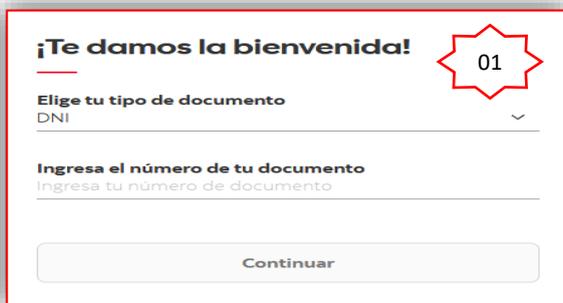
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°223		Fecha: 21-09-2023
			Página: 9 de 11
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria Scotiabank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
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:



¡Te damos la bienvenida!

Elige tu tipo de documento
DNI

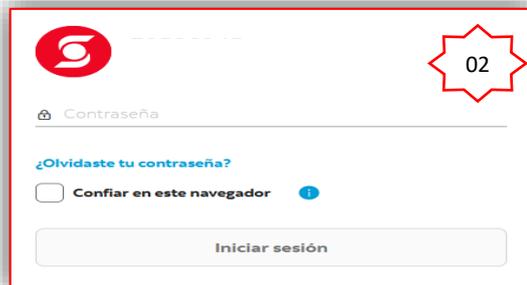
Ingresa el número de tu documento
Ingresa tu número de documento

Continuar

01

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 número de documento.

Paso N.º 02
Luego de continuar, solicita a las víctimas ingresar la contraseña de la cuenta bancaria.



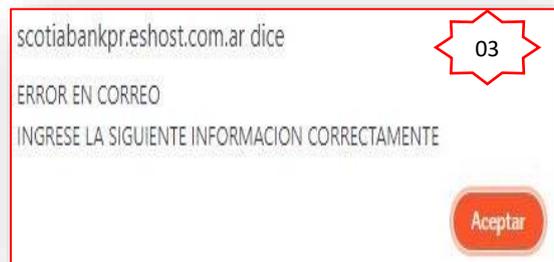
Contraseña

¿Olvidaste tu contraseña?

Confiar en este navegador

Iniciar sesión

02



scotiabankpr.eshost.com.ar dice

ERROR EN CORREO

INGRESE LA SIGUIENTE INFORMACION CORRECTAMENTE

Aceptar

03

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.

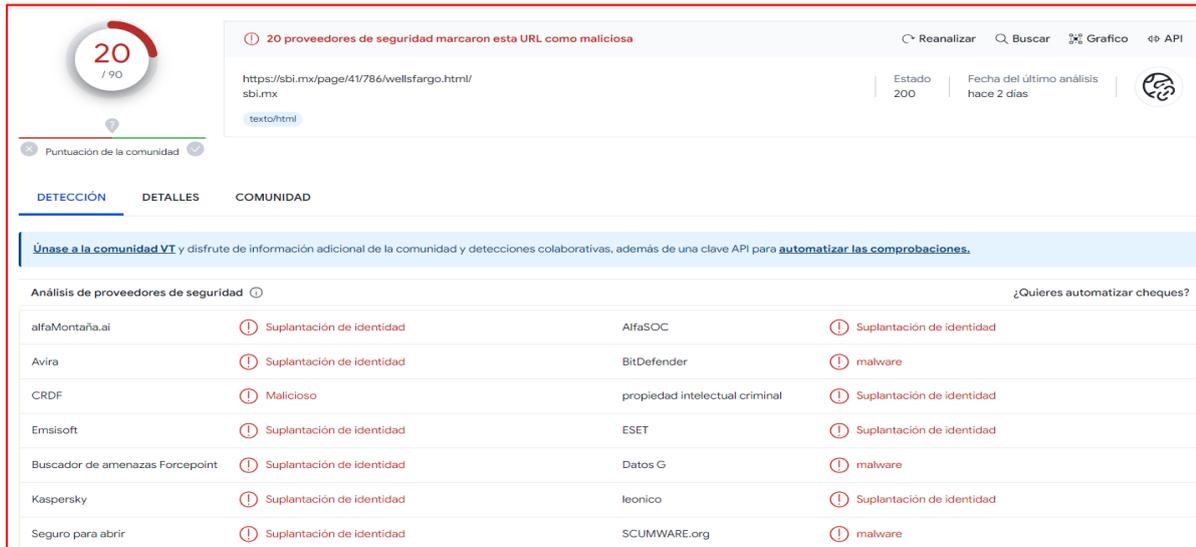


Scotiabank Perú

Para estar más cerca y mejor conectados, te brindamos la siguiente información

04

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



20 proveedores de seguridad marcaron esta URL como maliciosa

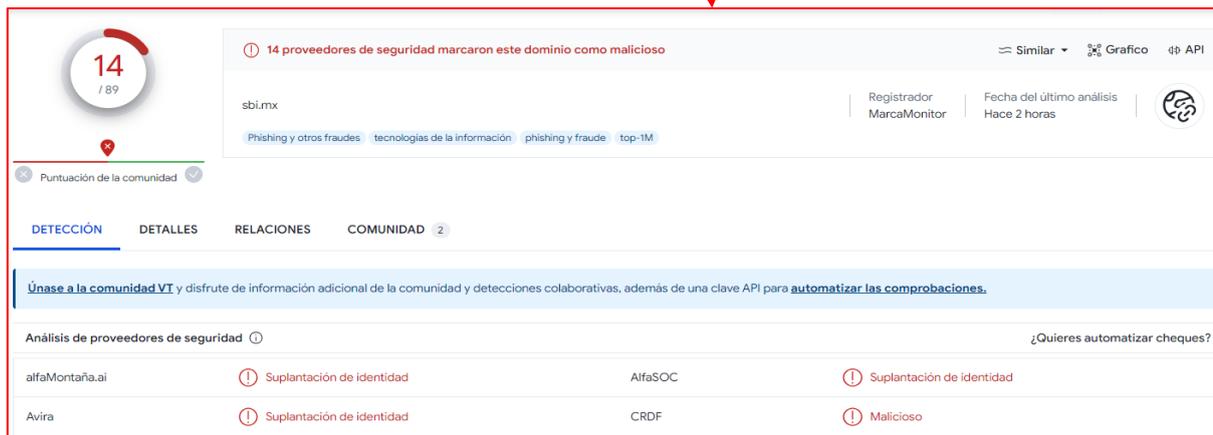
Estado: 200 | Fecha del último análisis: hace 2 días

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

Proveedor	Detección
AlfaMontaña.ai	Suplantación de identidad
AlfaSOC	Suplantación de identidad
Avira	Suplantación de identidad
BitDefender	malware
CRDF	Malicioso
propiedad intelectual criminal	Suplantación de identidad
Emsisoft	Suplantación de identidad
ESET	Suplantación de identidad
Buscador de amenazas Forcepoint	Suplantación de identidad
Datos G	malware
Kaspersky	Suplantación de identidad
leonico	Suplantación de identidad
Seguro para abrir	Suplantación de identidad
SCUMWARE.org	malware

INDICADORES DE COMPROMISO (IoC)

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



14 proveedores de seguridad marcaron este dominio como malicioso

Registrador: MarcaMonitor | Fecha del último análisis: Hace 2 horas

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

Proveedor	Detección
AlfaMontaña.ai	Suplantación de identidad
AlfaSOC	Suplantación de identidad
Avira	Suplantación de identidad
CRDF	Malicioso

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.